Coordenação:
HIGOR VINICIUS NOGUEIRA JORGE

DIREITO PENAL
sob a Perspectiva da Investigação Criminal Tecnológica

CRIMES CONTRA
A VIDA,
CRIMES CONTRA
O PATRIMÔNIO e
CRIMES CONTRA
A DIGNIDADE SEXUAL

4.ª edição
Revista, Atualizada e Ampliada

2026

EDITORA JusPODIVM
www.editorajuspodivm.com.br

Autores:
ANTÔNIO CARLOS CÂNDIDO ARAÚJO
BRENO EDUARDO CAMPOS ALVES
CAIO NOGUEIRA DOMINGUES DA FONSECA
DÁRIO TACIANO DE FREITAS JÚNIOR
DENIZE DOS SANTOS ORTIZ
ÉRICA MARCELINA CRUZ
FELIX MAGNO VON DÖLLINGER
FELLIPE CRIVELARO AYRES PEREIRA
FERNANDO HUGO MIRANDA TELES
FLÁVIO ROLIM PINHEIRO RESENDE
IASLEY ALMEIDA
FRANCISCO PETRARCA IELO NETO
FRANCISCO SANNINI
GILBERTO GOMES ROCHA
GUSTAVO WORCKI SATO
HIGOR VINICIUS NOGUEIRA JORGE
JANIO KONNO JÚNIOR
JOAQUIM LEITÃO JÚNIOR
JOSÉ ANTONIO BRANCO
KAMILLA CORREA BARCELOS
KLEBER LEANDRO TOLEDO RODRIGUES
LEONARDO D'ALMEIDA COUTO BARRETO
LIGIA BARBIERI MANTOVANI
LUÍS GONZAGA DA SILVA NETO
MARCELO VEIGA VIEIRA
MARIA HELENA DO NASCIMENTO
MARIA LUÍSA DALLA BERNARDINA RIGOLIN
MARIANA ALVES MACHADO NASCIMENTO
MAURO ARGACHOFF
PAULO FURTADO
PEDRO HENRIQUE NEVES COUTINHO DA SILVA
RENAN GUSTAVO DA SILVA REBECHI
RICARDO ANTONIO PORTO MATAZO
RICARDO MAGNO TEIXEIRA FONSECA
RICHARD GANTUS ENCINAS
ROGER FRANCHINI
SÉRGIO HUSSEIN MOURAD TENÓRIO
SERGIO LUCAS ADLER GUEDES DE OLIVEIRA
VALÉRIA ISABEL DOS SANTOS
VANESSA VITÓRIA OLIVEIRA
VITOR FREITAS ANDRADE VIEIRA
VIVIANNE MARQUES TORRES JARDIM
VYTAUTAS FABIANO SILVA ZUMAS
WILLIAM GARCEZ

5

OS CRIMES PATRIMONIAIS E O *E-COMMERCE*: A VULNERABILIDADE DO CONSUMIDOR NO AMBIENTE DIGITAL

Ligia Barbieri Mantovani

Sumário: 1. Considerações iniciais – **2.** Aspectos básicos de investigação no ambiente cibernético: **2.1.** A cadeia de custódia da prova e a preservação cautelar de dados e registros; **2.2.** Facebook e Instagram – **3.** Principais crimes patrimoniais no âmbito do comércio digital: **3.1.** Furto digital; **3.2.** Dano digital; **3.3.** Golpe do boleto falso; **3.4.** Falso e-mail de sites de vendas on-line; **3.5.** Site de comércio eletrônico fraudulento; **3.6.** Anúncio duplicado – **4.** Vulnerabilidade do consumidor no âmbito do *e-commerce*: uso seguro da internet e a prevenção contra fraudes e golpes – **5.** Conclusão – **6.** Referências.

1. CONSIDERAÇÕES INICIAIS

A internet está inserida na vida da maior parte da população na prática de diversas atividades rotineiras. A evolução dos meios tecnológicos proporcionou maior facilidade nas atividades cotidianas das pessoas, especialmente para a realização de negócios jurídicos digitais, dentre os quais destaca-se a compra e venda, culminando no aumento expressivo de crimes praticados no meio virtual.

Os crimes praticados no ambiente digital[1], normalmente, demandam complexa investigação policial, notadamente porque seus vestígios[2] possuem

1. As primeiras referências aos crimes praticados no ambiente virtual remontam à década de 1960, destacando-se o manuseio de dados, a espionagem e o uso ilegal de sistemas de computadores. Cf. BOITEUX, Luciana. Crimes informáticos: reflexões sobre a política criminal inseridas no contexto infracional atual. Revista Brasileira de Ciências Criminais – Instituto Brasileiro de Ciências Criminais – número 47 – Editora Revista dos Tribunais: ano 12: março – abril de 2004. p. 156.
2. Vestígio é a marca, objeto ou sinal presente no local de um crime e que pode ter relação com o fato investigado. Vestígio é tudo que é encontrado no local de um crime, o material bruto que precisa ser interpretado. Depois de analisado pelo perito, se ficar constatado que o vestígio possui, de fato, relação com o crime, transformar-se-á em evidência.

características específicas que dificultam sobremaneira as apurações de materialidade e autoria, do que é exemplo a volatilidade, já que os dados disponíveis no meio virtual podem ser facilmente modificados, editados, ocultados apagados ou perdidos.

Diante dessa fragilidade de elementos, faz-se necessária a correta e adequada coleta de dados que proporcionará elementos probatórios mínimos de investigação criminal.

A propagação do uso da internet certamente foi alavancada pela globalização e pela comodidade dos usuários, que viram nessa ferramenta a possibilidade de acesso a diversas atividades e conhecimento de informações sem sair de seu conforto.

Com o avanço tecnológico, o comércio digital passou a ocupar lugar de destaque nas transações comerciais. A praticidade de comprar e vender produtos e mercadorias, contratar serviços, fazer transações, efetuar pagamentos bancários, aquisição de ingressos e acesso a cursos atraiu não somente consumidores, mas também oportunistas, que viram nesse cenário a chance de obter vantagem patrimonial por meio do cometimento de crimes.

Os crimes virtuais são resultados de uma propagação desregrada do uso internet pelas pessoas que se empolgam com as facilidades do meio digital e esquecem-se de se certificar minimante de protocolos básicos de segurança.

Em razão da vulnerabilidade dos consumidores, crimes patrimoniais cometidos no meio digital estão ocorrendo de forma cada vez mais frequente, por meio de golpes praticados no comércio digital, a exemplo dos chamados golpes do *boleto falso*, *do e-mail duplicado* e *do site falso*.

A eficiente coleta de elemento de informação será fundamental para a comprovação da materialidade, para identificação da autoria e para a recuperação de eventual prejuízo financeiro.

O presente texto será desenvolvido no intuito de apontar alguns dos principais golpes criminosos praticados no meio virtual, especialmente na plataforma do *e-commerce*, indicando técnicas de coleta e preservação de dados que assegurem a eficiência da investigação e alertar, por fim, os consumidores quanto às vulnerabilidades a que estão expostos no ambiente digital.

2. ASPECTOS BÁSICOS DE INVESTIGAÇÃO NO AMBIENTE CIBERNÉTICO

A globalização proporcionou à população maior acesso à internet no dia a dia. Ocorre que o uso desregrado e a falta de conhecimento técnico da

população, abriram portas aos criminosos que viram neste cenário oportunidade para prática de crimes. A fim de regulamentar o uso da internet no Brasil, foi editada a Lei do Marco Civil (LMC) – Lei nº 12.965, de 23 de abril de 2014, a qual atribuiu responsabilidades aos cidadãos, ao governo e às organizações. Essa lei:

> [...] estabelece normas para a proteção da privacidade, seja em relação à guarda e ao tratamento de registros, dados pessoais ou comunicações por sites ou empresas que prestem serviços de acesso à internet, seja em relação à forma como essas informações devem ser disponibilizadas (MPMG, 2019, p. 07).

Para definir o que seja o crime virtual apontam-se conceitos de alguns estudiosos no assunto.

Segundo Augusto Rossini:

> [...] o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade (ROSSINI, 2004, p. 110)

A investigação de crimes ocorridos no âmbito digital é complexa e abrange técnicas específicas de coleta de dados para garantir o sucesso de uma investigação.

O domínio de alguns conceitos relacionados ao meio virtual é imprescindível para possibilitar a correta coleta de dados que eficientemente auxilie na comprovação da materialidade, na identificação da autoria de um crime cibernético e na futura recuperação patrimonial às vítimas. Os crimes virtuais ocorrem por meio de conexões ou acessos feitos por criminosos à Rede Mundial de Computadores que deixam rastros armazenados em dispositivos próprios.

Esses rastros são chamados de registros ou *logs*, os quais contêm informações relevantes para investigação. Em regra, as empresas que guardam esses registros ou *logs* não podem repassar as informações armazenadas a terceiros, já que sigilosas. Todavia, é possível que a polícia judiciária, em sua atividade típica de investigação criminal, tenha acesso a essas informações, a fim de elucidar crimes cibernéticos.

Assim, faz-se necessário o conhecimento de alguns termos técnicos para melhor compreensão do texto:

a) **Terminal:** é o computador ou qualquer dispositivo que se conecte à *Internet* (ex.: tablet, smartphone, smart Tv, servidor);

b) **Protocolo de *Internet* – *Internet Protocol* (IP):** é um número que identifica um terminal quando é conectado à Internet utilizando-se para isso dos provedores de conexão (ex.: Vivo, NET, Oi etc.). Há diversas versões de IP; as versões de IP mais utilizadas e atualizadas segundo a doutrina são as denominadas IPV6 e IPV4. No caso do IPV4, é possível o uso por vários clientes ao mesmo;

c) **Provedor de conexão (provedor de acesso):** é a empresa que presta serviço de conexão à *Internet* (ex.: Vivo, Net, Tim);

d) **Registro de conexão (*log* de conexão ou de acesso):** informações referentes à data e hora de início e término de uma conexão à *Internet*, tempo de duração e o endereço IP usado pelo terminal.

Cabe à Autoridade Policial, ao realizar uma investigação de crime ocorrido no meio virtual, solicitar aos provedores de aplicações de internet (Google, Microsoft, Facebook, Instagram etc.) qual o número do IP (*Internet Protocol*) utilizado pelo indivíduo para a prática criminosa e a respectiva porta lógica de origem. Porta lógica de origem está vinculada ao IP e refere-se à tecnologia que permite identificar de forma individualizada qual dos indivíduos usou o terminal sob análise, no caso de haver diversos acessos simultâneos.

A fragilidade desses elementos que compõem o conjunto probatório exige que a coleta seja feita de forma adequada e no menor tempo possível, sob pena de se perderem, o que poderá comprometer toda a investigação.

Assim, ao se deparar com a ocorrência de um crime praticado no meio digital, a primeira coisa que deverá ser feita é o registro policial pela vítima da situação criminosa, essencial para identificar qual foi o meio utilizado pelo autor para prática do crime (site de comércio, aplicativo de mensagem, rede social), bem como a coleta do maior número de informações possível sobre esse meio, como: a cópia do URL do anúncio fraudulento; a cópia do boleto falso; número de telefone e link do URL.

A partir da identificação pela Autoridade Policial de qual foi o meio utilizado para prática do crime, será possível, então, delinear qual a melhor técnica investigativa a seguir.

2.1. A cadeia de custódia da prova e a preservação cautelar de dados e registros

Uma das providências investigativas de maior importância é a preservação cautelar dos registros, evitando que informações importantes sejam apagadas, perdidas ou bloqueadas. A preservação, em caráter cautelar, garante um conjunto probatório mais robusto.

Para que haja a preservação dos registros será necessário identificar qual é o provedor de conexão (Claro, Tim, Vivo) vinculado ao IP *(Internet Protocol)* registrado no momento em que o crime foi praticado. Essa identificação pode ser feita facilmente através de diversas ferradas, sendo uma delas através do site Registro.Br (<https://registro.br/>) que disponibiliza consulta de forma simplificada.

Após a identificação, comunica-se, via ofício, ao provedor de conexão a situação, sendo que cabe àquela empresa realizar a guarda dos registros do usuário investigado durante os prazos estipulados na Lei do Marco Civil, Lei nº 12.965/2014.

A Lei do Marco Civil dispõe que os provedores de conexão armazenarão os registros dos usuários pelo período de 01 (um) ano (LMC, art. 13) e os provedores de aplicações de internet pelo prazo de 06 (seis) meses (LMC, art. 15).

Nota-se que os prazos legais de guarda de dados são curtos, razão pela qual é possível que o Delegado de Polícia solicite a dilação dos mesmos.

Essa previsão de aumento de prazo está expressa na Lei do Marco Civil, a qual garantiu a possibilidade de que o Delegado de Polícia solicite, cautelarmente e via ofício, que os registros sejam armazenados por maior tempo considerando a complexidade de cada caso concreto.

Trata-se da chamada Requisição Cautelar de Guarda de Registros Eletrônicos, a cargo da Autoridade Policial titular das investigações (arts. 13, § 2º, e 15, § 2º da Lei nº 12.965/2014).

2.2. Facebook e Instagram

O aumento do uso das redes sociais pela população exigiu significativas medidas protetivas a fim de salvaguardar os usuários. A preservação de dados está presente nas plataformas do Facebook e Instagram, tendo em vista o aumento exponencial de crimes praticados nas redes sociais. No Facebook, a preservação de dados é realizada através da ferramenta Facebook Records.

Trata-se de uma plataforma digital presente na página do Facebook indicada como *´Law Enforcement Online Request`*, ou seja, Sistema de Solicitação Online do Cumprimento da Lei[3].

A utilização desta plataforma de solicitação é restrita aos órgãos oficiais, já que o usuário deverá indicar informações cadastrais como nome completo, título e organização a qual está vinculado, além de possuir um e-mail institucional através do qual será disponibilizado o acesso ao ambiente virtual e o link da plataforma *´Law Enforcement Online Request`* por um prazo específico para coleta de elementos investigativos.

Após o *login* na plataforma pode o agente realizar uma solicitação de preservação de dados requerendo que as informações sigilosas sejam armazenadas pelo prazo definido pelo próprio Facebook.

Esse procedimento assegura que o conjunto probatório seja resguardado, de forma que, mesmo que o titular da conta alvo da investigação apague as publicações, os dados continuarão disponíveis e acessíveis ao agente que fez a solicitação.

Há diversas outras técnicas de coleta de dados para os casos de crimes praticados no ambiente cibernético, das quais se destaca a identificação dos titulares de números de linhas telefônicas utilizadas para prática de crimes.

A utilização dessas técnicas visa a salvaguardar as informações contidas no ambiente digital, reforçando o conjunto probatório de elementos investigativos para elucidação de crimes e identificação de autores criminosos.

3. PRINCIPAIS CRIMES PATRIMONIAIS NO ÂMBITO DO COMÉRCIO DIGITAL

O cenário de uso expressivo da internet pelas pessoas em suas atividades cotidianas atraiu criminosos que encontraram na Rede Mundial de Computadores a oportunidade de obter vantagens ilícitas.

Normalmente, os criminosos virtuais são pessoas com conhecimentos tecnológicos. Algumas vezes, o autor utiliza-se de conhecimentos técnicos para explorar as vulnerabilidades do sistema e identificar quais as fragilidades da rede; outras vezes, vale-se de ardil para ludibriar e enganar as vítimas convencendo-as a fornecer informações sensíveis, executar operações, acessar páginas falsas, clicar em links maliciosos.

3. Disponível em: <https://www.facebook.com/records/login/>. Acesso em 20 dez. 2020.

3.1. Furto digital

Um dos crimes contra o patrimônio mais comuns cometidos no ambiente virtual é o furto, no caso, furto digital.

No crime de furto digital, o autor realiza a captação de dados do usuário, manipulando informações sensíveis como senhas ou dados de cartão de crédito, a fim de obter vantagem financeira da maneira que lhe for mais oportuno.

Normalmente, a captação das informações é feita por mensagem enviada à vítima, pela qual o(s) autor(es) do delito se faz(em) passar por uma instituição bancária ou órgão público, solicitando informações pessoais ou a confirmação de dados pessoais. De posse das informações desejadas, os criminosos repassam os dados sensíveis ao *hacker*, o qual, por sua vez, invade a conta bancária ou página de acesso da vítima realizando saques, transações e/ou transferências, compras ou vendas.

A identificação destes autores envolvidos no furto virtual é complexa, já que normalmente o processo é ramificado com participação de diversas pessoas que se utilizam de nomes falsos, dados pessoais alterados e contas *fakes*.

3.2. Dano digital

O dano digital ocorre quando o criminoso propaga algum vírus ou código malicioso que danifica ou destrói arquivos, informações ou dados da vítima.

Neste caso, o criminoso conhecedor das vulnerabilidades de um sistema de informática realiza a disseminação de um vírus na Rede Mundial de Computadores resultando em danos em software, arquivos ou dados contidos no computador da vítima, podendo até em casos extremos danificar algum hardware.

3.3. Golpe do boleto falso

Esse golpe se perfaz mediante envio de um boleto falso à vítima por SMS, aplicativo de mensagens ou e-mail.

A materialização do golpe praticado via e-mail normalmente ocorre assim: inicialmente, a vítima realiza alguma compra ou contrata algum serviço na internet, cujo pagamento ocorre via boleto. A vítima então recebe por e-mail o boleto (correto) para pagamento enviado pela empresa.

Todavia, antes que a mesma efetue o pagamento é enviado um novo e-mail com outro boleto, normalmente com valor inferior ao primeiro, e contendo alguma justificativa como desconto ou vantagem concedido ao cliente. A vítima então efetua o pagamento do boleto recebido por último cujo valor é menor e somente descobre que foi alvo de um golpe quando a empresa passa a efetuar cobranças em razão da falta de pagamento do boleto bancário.

Nota-se que a vítima efetua o pagamento do boleto sem tomar as cautelas necessárias de conferência dos dados do boleto. Os boletos falsos normalmente possuem o formato bastante semelhante ao dos originais, mas com algumas pequenas alterações no código de barras, o que fará com que o valor pago seja direcionado à conta bancária do criminoso ou de "laranjas", ou divergência quase imperceptíveis nos dados referentes ao nome, número da conta bancária e agência da empresa.

Esse golpe pode ocorrer em qualquer transação cuja forma de pagamento seja através de boleto, tanto em redes sociais quanto sites falsos.

3.4. Falso e-mail de sites de vendas on-line

Esse golpe ocorre com frequência em plataformas digitais de compra e venda de mercadorias.

Consiste no fato de que uma pessoa (vítima) anuncia um produto em site de vendas (*v.g.*: OLX; Mercado Livre; Enjoei; Estante Virtual e Uzlet). O criminoso, a fim de obter informações sensíveis sobre o vendedor (vítima) utiliza-se da caixa de perguntas para simular suposto interesse no produto e questiona qual o e-mail e o número do telefone do vendedor para negociação.

O vendedor (vítima), acreditando em um potencial comprador repassa a informação sensível. Após, o criminoso envia um e-mail para o endereço indicado pelo vendedor fazendo-se passar pela empresa e noticiando a venda do produto com frases como "Você vendeu!" ou "Está com sorte! Seu produto foi vendido!", além de enviar orientações para que a vítima faça o envio do produto e do código de rastreamento. Esse endereço de e-mail é muito parecido com o e-mail original da empresa, normalmente trocando apenas uma letra, palavra, número ou item a fim de que a fraude seja despercebida.

Não raras vezes, o criminoso faz diversos contatos com a vítima, solicitando-lhe o envio imediato do produto com o código de rastreio, o que é de pronto atendido pelo anunciante.

Assim que a mercadoria é entregue ao criminoso, ele bloqueia ou apaga todos os possíveis contatos ou formas de interação, impedindo que a vítima o localize para questionamentos.

O anunciante (vítima) somente tomará ciência do golpe no momento em que deixar de receber o pagamento quando fizer contato com a empresa digital que informará que se tratava de uma fraude.

3.5. Site de comércio eletrônico fraudulento

Outro golpe recorrente no âmbito do comércio eletrônico é o do site fraudulento. Neste tipo de golpe, o criminoso cria um site falso praticamente igual ao original, com as mesmas cores, tipo de escrita, exposição de produtos e mercadorias e formatação.

A vítima pensando tratar-se do site original efetua compras de maneira online realizando o pagamento conforme as opções ofertadas pelo site. Ocorre que o produto ou mercadoria não é entregue.

A Cartilha de Segurança para a Internet da CERT.br (2017) esclarece que o criminoso "costuma utilizar artifícios como: enviar spam, fazer propaganda via links patrocinados, anunciar descontos em sites de compras coletivas e ofertar produtos muito procurados e com preços abaixo dos praticados pelo mercado."

Os golpistas cada vez mais audaciosos utilizam-se de nomes de grandes empresas reconhecidas pela população na intenção de passar maior credibilidade ao site fraudulento.

3.6. Anúncio duplicado

Outra prática criminosa que tem feito milhares de vítimas em sites de compra e venda de mercadorias como, por exemplo, OLX, Mercado Livre, Enjoei e Uzelet, é o golpe do anúncio duplicado.

O golpe do anúncio duplicado normalmente está vinculado à compra e venda de veículos. Neste caso, o criminoso captura as informações do vendedor que estão expostas no próprio anúncio como o número do telefone da vítima. Após faz contato com o vendedor manifestando interesse em adquirir o produto e solicitando então que o mesmo retire o anúncio do site para que nenhuma outra pessoa efetue a compra.

O criminoso, durante a negociação com o proprietário, coleta informações importantes sobre o produto e, após, cria um anúncio falso colocando

o mesmo produto à venda (com aquelas características que coletou através de informações obtidas com o vendedor), porém com valor inferior. Com mais uma vítima interessada no veículo, o golpista ilude a primeira vítima (vendedor original) dizendo que irá revender o carro para um terceiro que, no caso, é a segunda vítima. À segunda vítima autoriza que conheça pessoalmente o produto antes de concluir a compra, mas argumenta que quem irá comparecer ao local para atendê-la é um terceiro. O golpista, muito ardiloso, orienta as duas vítimas para que não conversem sobre valores entre si.

Após o encontro, o comprador transfere o valor combinado, mas para a conta bancária do golpista – intermediador da venda sem que as outras duas pessoas (vendedor original e vítima) soubessem da fraude.

As duas vítimas (vendedor original e vítima) somente terão ciência que foram alvo de um golpe no momento marcado para entrega do produto quando o vendedor não terá recebido o pagamento e o comprador terá repassado a quantia para a conta bancária do golpista.

4. VULNERABILIDADE DO CONSUMIDOR NO ÂMBITO DO *E-COMMERCE*: USO SEGURO DA INTERNET E A PREVENÇÃO CONTRA FRAUDES E GOLPES

O uso desregrado e descuidado da internet fragiliza os consumidores, que ficam expostos às práticas ilegais, passando-se de usuários a vítimas potenciais.

Diante dessa vulnerabilidade, o Código de Defesa do Consumir, Lei nº 8.078/90, disciplinou as relações de consumo, definindo os direitos e responsabilidades dos consumidores e dos fornecedores, estabelecendo mecanismos para reparação de danos, regulamentando situações consumeristas e estabelecendo crimes e punições.

O Decreto nº 7.962/2013, que regulamentou o Código de Defesa do Consumidor, detalhou a disciplina da contratação em casos de comércio eletrônico (*E-commerce*) e ampliou a esfera de proteção do consumidor.

Um dos principais direitos do consumidor estabelecido no CDC e alvo de regulamentação pelo referido decreto é o direito ao arrependimento. Conforme o art. 49 do Código Consumerista, o consumidor pode desistir do contrato, no prazo de 7 dias a contar de sua assinatura ou do recebimento do produto ou serviço, sempre que o negócio jurídico for realizado fora do estabelecimento comercial, especialmente por telefone ou a domicílio. Uma vez exercido o direito, os valores eventualmente pagos, a

qualquer título, durante o prazo de reflexão, serão devolvidos, de imediato, monetariamente atualizados.

Especificamente, o direito de arrependimento do consumidor em casos de comércio eletrônico consagrado pelo art. 1º, III, do Decreto nº 7.962/2013, diploma que estabeleceu ao fornecedor, em seu art. 5º, o dever de informar, de maneira clara e ostensiva, os meios adequados e eficazes para seu exercício pelo consumidor. O direito ao arrependimento poderá ser exercido pela mesma ferramenta utilizada para a contração, implicando em rescisão de contratos acessórios e sem ônus para o consumidor (art. 5º, §§ 1º e 2º). Efetivado o direito de arrependimento, será realizada a comunicação à instituição financeira ou à administradora do cartão de crédito ou similar para que tome as medidas necessárias no sentido de que a transação não seja lançada na fatura do consumidor ou efetivado o estorno do valor (art. 5º, § 3º).

Além do direito de arrependimento, o Decreto nº 7.962/2013 dispõe sobre aspectos relacionados à obrigatoriedade de informações claras a respeito do produto, serviço e do fornecedor digital, bem como atendimento facilitado ao consumidor no ambiente eletrônico.

Diante de tantas vulnerabilidades a que estão expostos os consumidores virtuais, é necessário apontar condutas simples de prevenção que certamente diminuirão as chances de cair em golpes. Conferir *sites* que apresentem formatação estranha e erros excessivos de gramática na escrita, sem indicação das formas de contato com a empresa, pesquisar eventuais reclamações sobre a empresa postadas em páginas públicas, conferir de forma detalhada boletos enviados e desconfiar de descontos e vantagens.

A adoção de mecanismos de segurança minimiza os riscos aos quais os consumidores são expostos na internet. Alguns desses mecanismos, como o uso de contas e senhas como ferramenta de autenticação para controlar o acesso a sites, dominar a política de segurança de determinada página quanto a senhas "fortes" e privacidade, criptografia para proteção de informações sensíveis, backup de dados, contratação de antivírus ou outros programas que impeçam a entrada de códigos maliciosos, são essenciais para segurança dos e-consumidores.

5. CONCLUSÃO

Considerando o acima exposto, restou constatado que a internet inevitavelmente já está inserida na vida cotidiana das pessoas desde as mais simples atividades.

Diante desse fato inconteste e das vulnerabilidades a que ficam indubitavelmente expostos os consumidores, há que se tomar todas as medidas preventivas com o objetivo de evitar ser vítima de golpes virtuais.

Desconfiar sempre de postagens que oferecem descontos de forma aleatória é o um dos meios de segurança do consumidor. Demonstrou-se que, na maioria das vezes, o golpe praticado por criminosos no ambiente virtual está vinculado com o interesse do consumidor de obter alguma vantagem, normalmente econômica.

Indispensável lembrar que, por trás de qualquer ato praticado na rede digital, há pessoas manipulando e alimentando esse sistema virtual, razão pela qual adotar medidas de segurança de criptografia, autenticação de acesso por contas e senhas e adoção de políticas de privacidades são fundamentais para proteção do consumidor.

A Rede Mundial de Computadores propicia a prática de crimes, já que neste ambiente digital os criminosos ficam, ao menos naquele momento, invisíveis. O crescimento alarmante de crimes cometidos neste cenário estimulou a criação de delegacias de polícia especializadas em crimes cibernéticos, as quais têm conseguido elucidar diversos crimes virtuais, prendendo criminosos e desarticulando grupos organizados estruturalmente organizados para prática de crimes virtuais.

6. REFERÊNCIAS

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei.12965.htm>. Acesso em: 16 de dez. 2020.

BRASIL. **Decreto-lei nº 7.962, de 15 de março de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm>. Acesso em: 19 dez. 2020.

BOITEUX, Luciana. Crimes informáticos: reflexões sobre a política criminal inseridas no contexto infracional atual. Revista Brasileira de Ciências Criminais – Instituto Brasileiro de Ciências Criminais – número 47 – Editora Revista dos Tribunais: ano 12: março – abril de 2004.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de Segurança na Internet:** Fascículo Dispositivos Móveis. Disponível em: <https://cartilha.cert.br/fasciculos/internet-banking/fasciulo-internet-banking.pdf>. Acesso em: 18 dez. 2020.

GOMES, Luiz Flávio; BIANCHINI, Alice. **Globalização e direito penal.** In: ESCRITOS em homenagem a Alberto da Silva Franco. São Paulo: Revista dos Tribunais, 2003. p. 264-287.

MALLMITH, Décio. Corpo de delito, vestígio, evidência e indício. Rio Grande do Sul. 07 de maio de 2007. Disponível em: <http://peritocriminal.net/mambo/index2.php?option=com content&dopdf=1&id=136>. Acesso em: 07 jul. 2019.

MINISTÉRIO PÚBLICO DE MINAS GERAIS. **Navegar com Segurança:** por uma internet mais segura, ética e responsável. 4 ed. Belo Horizonte: MPMG, 2019.

PINHEIRO, Reginaldo César. **Os cybercrimes na esfera jurídica brasileira**. In: Revista Eletrônica Jus Navigandi. Site: http://jus.com.br/revista/texto/1830/os-cybercrimes-na-esfera-juridica-brasileira Acesso em 21 dez. 2020.

PINHEIRO, Patrícia Peck. **Direito digital**. 4°. Ed. São Paulo: Saraiva, 2010.p.300 e 301.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. **Jus Navigandi**, Teresina, a. 6, n. 58, ago. 2002. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=3186>. Acesso em: 21 dez. 2020.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica, 2004.

____. **Cartilha de Segurança na Internet:** Fascículo Privacidade. Disponível em: <https://cartilha.cert.br/fasciculos/privacidade/fasciculo-privacidade.pdf>. Acesso em: 18 dez. 2020.

____. **Cartilha de Segurança na Internet:** Fascículo Senhas. Disponível em: <https://cartilha.cert.br/fasciculos/senhas/fasciculo-senhas.pdf>. Acesso em: 18 dez. 2020.

____. **Cartilha de Segurança na Internet**: Fascículo Comércio Eletrônico. Disponível em: <https://cartilha.cert.br/fasciculos/comercio-eletronico/fasciculo-comercio-eletronico.pdf>. Acesso em: 18 dez. 2020.

____. **Cartilha de Segurança na Internet:** Fascículo Redes Sociais. Disponível em: <https://cartilha.cert.br/fasciculos/redes-sociais/fasciculo-redes-sociais.pdf>. Acesso em: 18 dez. 2020.

6

O CABIMENTO DO ASSISTENTE NA INVESTIGAÇÃO

Caio Nogueira Domingues da Fonseca

Sumário: 1. Introdução – **2.** A vítima como assistente na investigação – mecanismos legais que autorizam sua participação na persecução penal: **2.1.** Como a vítima pode fornecer elementos de informação e de prova para auxiliar as investigações?; **2.2.** Casos práticos – **3.** Sigilo de dados: breve análise de quais dados podem ser fornecidos por requisição e quais são acobertados pelo sigilo – **4.** Medidas processuais que podem ser requeridas pelo assistente na investigação – **5.** Considerações finais – **6.** Obras citadas – Referências Jurisprudenciais.

1. INTRODUÇÃO

No primeiro semestre de 2020, a revista Época Negócios publicou reportagem informando a disparada dos golpes virtuais durante o período de isolamento social[1]. A reportagem fazia menção ao artigo publicado pela empresa Refinaria de Dados, onde era informado que no período entre março e maio de 2020, a busca por informações bancárias e pessoais de brasileiros na chamada *dark web* havia crescido 108%, colocando o Brasil em 9º lugar no ranking de países mais afetados por tentativas de fraudes[2].

Esse aumento exponencial das fraudes também foi motivo de alerta da Federação Brasileira de Bancos – Febraban. Segundo os dados fornecidos pela entidade, durante o período de isolamento social, o setor bancário registrou grande aumento das mais variadas modalidades de fraudes.

Apenas a título de exemplo, os ataques de *phishing*, que se inicia por meio de e-mails que carregam vírus, ou através mensagens SMS, que carregam links que direcionam a vítima para sites falsos das instituições bancárias, cresceram 80%[3] durante o período.

---

1. Disponível em: <https://epocanegocios.globo.com/Brasil/noticia/2020/06/epoca-negocios-golpes-virtuais-disparam-com-covid-19.html>. Acesso em: 07.12.2020.
2. Disponível em: < https://refinariadedados.com.br/estudos-originais/pesquisa-golpes-virtuais-disparam-durante-isolamento-social/>. Acesso em: 07.12.2020.
3. Disponível em: <https://portal.febraban.org.br/noticia/3522/pt-br/>. Acesso em 07.12.2020.

O fenômeno do aumento das fraudes ocorre em escala mundial, e está intimamente ligado à popularização dos meios de comunicação virtuais, bem com a sensação de anonimato e impunidade proporcionado pelo ambiente virtual. Soma-se a isso ainda a dificuldade que as empresas e autoridades de investigação tem em combater e prevenir esses crimes.

Segundo Gustavo Bueno e Higor Nogueira Jorge:

> "(...) a despeito de seus efeitos positivos para a humanidade, esta nova realidade despertou a prática de um novo fenômeno criminal, impulsionado pela sensação de anonimato e impunidade, pela potencialização dos danos aos bens jurídicos visados, pela facilidade do aprendizado de técnicas criminosas, e pelo favorecimento da cooperação entre indivíduos com propósitos desviantes.[4]"

As fraudes acabam por sujeitar empresas a riscos constantes de dano financeiro e reputacional, implicando em prejuízos que vão desde o pagamento de indenizações aos clientes vítimas de fraudes, a perda de confiança perante o mercado, aumentando ainda mais o efeito deletério causado pelos crimes.

Por essas razões, o combate e prevenção aos crimes patrimoniais decorrentes de fraudes, ganha importante relevância, e a utilização de técnicas modernas de investigação tecnológica precisam ser cada vez mais recorrentes e aprimoradas, seja pelos órgãos de investigação oficiais, seja pelas próprias empresas.

Nesta esteira, surge um personagem que pode auxiliar ativamente as investigações, a vítima, a quem chamaremos de assistente da investigação e que atua nomeando um defensor, normalmente advogado criminalista.

2. A VÍTIMA COMO ASSISTENTE NA INVESTIGAÇÃO – MECANISMOS LEGAIS QUE AUTORIZAM SUA PARTICIPAÇÃO NA PERSECUÇÃO PENAL

A vítima durante muito tempo teve sua atuação relegada no processo penal, sendo constantemente impedida de atuar durante a fase da investigação, seja ela realizada no inquérito policial ou no procedimento investigatório criminal.

4. JORGE, Higor Vinicuis Nogueira; BUENO, Gustavo. Investigação criminal tecnológica e direitos fundamentais das vítimas de crimes. Disponível em: <https://canalcienciascriminais.com.br/investigacao-criminal-tecnologica-e-direitos-fundamentais/>. Acesso em 08.12.2020.