AS REDES SOCIAIS COMO MEIO DE PROPAGAÇÃO DOS CRIMES DIGITAIS FINANCEIROS

Clara Oliveira de Paula Avelino
Edivaldo Leite da Silva Junior
Felipe Marinho dos Santos
Gabriella Morais Marques de Oliveira
Helen Cristina da Costa Dias
Ingrid Innaiah da Silva Rocha Soares de Souza
Luany Maria Alves
Maria da Glória da Silva Rocha
Tatianne Francilla Maia Oliveira
Vantuil Alves de Oliveira[1]

Resumo

A presente pesquisa acadêmica foi realizada com o objetivo de embasar a atividade extensionista a ser realizada no âmbito da disciplina Direito Digital, sob a orientação do Prof. Dr. Henrique Savonitti Miranda. Ao tratar o tema "As redes sociais como meio de propagação dos crimes digitais financeiros", pretende-se apresentar a relação de causa e efeito entre ambos e propor soluções preventivas capazes de inibir práticas que causam prejuízos à população. Vivemos em um mundo tecnológico onde as pessoas se conectam através da internet e dispositivos informáticos. Dessa forma, torna-se necessária a adoção de comportamentos adequados no uso da internet e das redes sociais, com o objetivo de reduzir a possibilidade de se tornar vítima dos crimes digitais, especialmente os de natureza financeira. Estudos de mercado que revelam que, atualmente, o *cybercrime* movimenta mais dinheiro que o tráfico de drogas. Considerando os riscos envolvidos, o tema proposto é de grande relevância, pois visa promover a conscientização do público, auxiliando na prevenção dos crimes digitais financeiros praticados no ambiente virtual.

1. Introdução

A internet é uma vasta rede que conecta computadores ao redor do mundo, possibilitando a comunicação entre eles. Sua origem remonta ao ano de 1966, época em que seu uso era específico das Forças Armadas dos Estados Unidos, com a

[1] Graduandos em *Direito* pelo Centro Universitário Processus.

finalidade de garantir o funcionamento contínuo da rede, mesmo em emergências. O sistema se fundamentava na ideia de eliminar comandos centrais, atribuindo a cada ponto da rede a mesma importância. Essa evolução resultou em uma dependência crescente da eficiência e segurança da tecnologia da informação, que passou a ser amplamente utilizada nas relações comerciais, nas administrações públicas e na sociedade em geral. No âmbito comercial, grande parte das transações financeiras ocorre via computador; da mesma forma, muitas empresas armazenam seus arquivos de informações confidenciais e valiosas de forma eletrônica.

Crespo (2011, p. 13) pontua três alterações percebidas desde o final do século XX até os dias atuais: (i) a formação da sociedade da informação; (ii) o desenvolvimento da sociedade de risco**;** e (iii) a configuração de uma sociedade global e digital. Segundo ele, a transição da sociedade industrial para a sociedade da informação é considerada por alguns estudiosos como uma "segunda revolução industrial", pois, enquanto a primeira substituiu o trabalho humano pelo uso de máquinas, a segunda busca substituir a atividade intelectual humana por máquinas.

Atualmente, a internet tornou-se um instrumento fundamental na vida das pessoas. Uma pesquisa de 2020, realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC), demonstrou que o percentual de domicílios com acesso à Internet chegou a 83%, ou seja, estima-se que aproximadamente 152 milhões de brasileiros utilizavam a rede, representando 81% da população com dez anos ou mais.[2]

Em contrapartida, com o aumento de usuários no meio virtual, cresce também o número de agentes criminosos que realizam golpes, principalmente os de natureza financeira, utilizando-se, em grande parte, de técnicas de engenharia social. Mitnick e Simon (2003, p.6) afirmam que, na engenharia social, o criminoso utiliza persuasão e influência para enganar as pessoas, obtendo, assim, informações confidenciais das vítimas em benefício próprio.

De maneira abrangente, os delitos cibernéticos têm gerado uma crescente preocupação entre os usuários, entes governamentais e organizações empresariais que são alvos frequentes de atividades maliciosas. Conforme mencionado no relatório

[2] DOMICÍLIOS, Tic. Cresce o uso de Internet durante a pandemia e número de usuários no Brasil chega a 152 milhões, é o que aponta pesquisa do Cetic.br, 2021. Disponível em: https://cetic.br/pt/noticia/cresce-o-uso-de-internet-durante-a-pandemia-e-numero-de-usuariosno-brasil-chega-a-152-milhoes-eo-que-aponta-pesquisa-do-cetic-br. Acesso em: 16 out. 2024.

de 2022, publicado pela empresa de segurança cibernética Kaspersky, o Brasil registrou mais de 76 mil ocorrências de fraudes eletrônicas (TEAM, 2022, Online), evidenciando a gravidade e a urgência de implementação estratégias eficazes de cibersegurança e de conscientização digital.

Esta pesquisa acadêmica tem como objetivo reunir informações que embasem a conscientização do público e o auxiliem na prevenção dos crimes digitais financeiros, frente à necessidade do uso da tecnologia na vida atual.

Para atingir esse objetivo, a pesquisa foi dividida em três partes, além de introdução e da conclusão. A primeira parte traz uma visão geral e aborda as peculiaridades dos crimes cibernéticos. A segunda parte explora os impactos e a legislação aplicável aos crimes cibernéticos. A terceira apresenta informações sobre como prevenir-se dos crimes cibernéticos financeiros.

Dessa forma, busca-se contribuir para o avanço na prevenção dos crimes digitais financeiros, oferecendo embasamento ao público, ainda que sem esgotar o tema ora proposto.

2. Desenvolvimento do tema pesquisado

2.1. Conceito de crimes cibernéticos (crimes digitais).

Inicialmente, cabe destacar que, doutrinariamente, não existe uma nomenclatura consolidada para definir os crimes cibernéticos, pois diversos termos são empregados para descrevê-los, como crimes digitais, crimes informáticos, crimes virtuais, e-crimes, cibercrimes, crimes eletrônicos. Silva (2015, p.39) observa que a falta de um consenso entre os doutrinadores sobre a denominação desses crimes resulta em uma multiplicidade de termos para o mesmo conceito.

Nesta pesquisa, utilizaremos o termo “crime cibernético”, por considerá-lo abrangente e adequado para englobar atividades criminosas executadas em rede ou por meio de qualquer sistema informático. Nesse contexto, Castro (2003, p.41) define crimes de informática como práticas delitivas realizadas através de dispositivos informáticos, bem como condutas ilegais contra equipamentos tecnológicos, sistemas de informação ou banco de dados.

Entre as diversas classificações utilizadas na literatura para esses crimes, destaca-se divisão em crimes cibernéticos próprios e impróprios. Conforme Oliveira (2009, p.33),

um crime cibernético próprio é aquele que só pode ser realizado no ciberespaço, ou seja, para caracterizar crime cibernético próprio, é necessário que o crime seja cometido no ambiente virtual. Esses estão previstos nos artigos 313-A (publicação de dados falsos em sistema de informações), 313-B (modificar ou alterar sem autorização sistema de informações), 154-A (invadir dispositivo informático) do Código Penal Brasileiro (BRASIL, 1940), e no artigo 241- A do Estatuto da Criança e do Adolescente – ECA (BRASIL, 1990), que trata da oferta, troca, disponibilização, transmissão, distribuição, publicação ou divulgação de materiais pornográficos envolvendo crianças ou adolescentes.

Já os crimes cibernéticos impróprios são aqueles em que sistemas informáticos são utilizados apenas como um meio para a prática do delito, o qual pode ser realizado com ou sem os meios tecnológicos. Entre os crimes cibernéticos impróprios estão crimes contra a honra, ameaça, estelionato, furto mediante fraude, racismo, falsa identidade, tráfico de drogas (WENDT; JORGE, 2013, p.20).

Entre os doutrinadores brasileiros, destaca-se ainda a classificação proposta por Ivete Senise Ferreira e Vicente Greco Filho, que categoriza os crimes digitais em: a) condutas criminosas praticadas em sistema informático; b) comportamentos criminosos realizados contra outros bens jurídicos.

Essa classificação, mais simples em comparação com as anteriores, é de fácil assimilação e aplicação (FERREIRA, 2000, p.139)

2.2. Crimes cibernéticos nas redes sociais.

Com o avanço da tecnologia e o uso cada vez mais frequente das redes sociais onde os usuários passam muitas horas conectados, como *Facebook, Instagram, Kwai, LinkedIn, Messenger, TikTok, WhatsApp, Youtube,* essas plataformas digitais tornaram-se ambientes propícios para a prática de crimes. Nesse contexto, Wendt e Jorge (2013, p.12) afirmam que, embora a internet funcione como um canal de globalização, transformando a forma como nos comunicamos no trabalho, nas pesquisas, nos estudos, nos relacionamentos interpessoais, ela também pode ser utilizada para práticas delitivas, incluindo fraudes financeiros.

Quando criminosos enganam as vítimas por meio de mensagens, contato telefônico ou redes sociais, com a finalidade de obter informações confidenciais, como senhas de acesso a bancos ou número de cartão, inicia-se uma fraude eletrônica (TJDFT,

2021, Online). Um exemplo recente desses ataques foi registrado por Rodrigues (2022), que relata os ciberataques que geraram um prejuízo de R$ 16 milhões às prefeituras de São Paulo e Minas Gerais em outubro de 2022. Segundo a Polícia Civil de São Paulo, os suspeitos utilizavam sites falsos para obter credenciais de acesso e, assim, acessar as redes das vítimas.

A atenção dos usuários ao utilizarem meios virtuais é indispensável tanto para a sua própria proteção quanto para evitar ações que se caracterizem crimes virtuais. Outro aspecto relevante é a adoção de práticas de compliance pelas organizações, com o objetivo de integrar a segurança da informação ao ambiente corporativo. A aplicação de protocolos de autenticação em duas etapas, criptografia de dados e auditorias internas de segurança são práticas que reduzem os riscos de crimes financeiros. De acordo com Lopes e Silva (2022), empresas que investem em uma cultura de segurança digital tendem a apresentar menores índices de vulnerabilidade a ataques cibernéticos, protegendo tanto seus ativos quanto os de seus clientes.

2.3. Ações que caracterizam invasão da privacidade.

A intimidade e a privacidade são direitos constitucionais assegurados pelo artigo 5º, inciso X, da Constituição Federal (BRASIL, 2023). Contudo, os crimes cibernéticos que envolvem a invasão desses direitos tornaram-se uma preocupação crescente na era digital. Com o avanço tecnológico, as oportunidades de violação da privacidade por meio de dispositivos informáticos aumentaram. Esse tipo de delito envolve ações que visam invadir, coletar, manipular e divulgar informações confidenciais das pessoas sem o consentimento delas, geralmente com o intuito de obter ganhos financeiros.

Um exemplo conhecido de crime cibernético ocorreu em 2011, quando a atriz Carolina Dieckmann foi vítima de um ataque em que invadiram seu computador, subtraíram e divulgaram suas fotos íntimas na internet. Esse episódio levou à criação da Lei nº 12.737 de 2012, conhecida como Lei Carolina Dieckmann, que incluiu no Código Penal Brasileiro o artigo 154-A, tipificando a invasão de dispositivos informáticos (BRASIL, 1940).

No Direito Penal, a proteção dos bens jurídicos envolve o direito ao sigilo de dados, à intimidade e à vida privada. Esses direitos impõem a necessidade de inviolabilidade do domicílio e das comunicações, com proteção penal específica (NUCCI, 2017, p.

26). A configuração do crime cibernético ocorre quando há invasão de um dispositivo informático sem autorização do proprietário. O legislador, no §3º do artigo 154-A do Código Penal Brasileiro, incluiu uma qualificadora para invasões que afetam a privacidade da vítima, aumentando a pena para reclusão de seis meses a dois anos, além de multa (CAPEZ, 2016). O §4º do mesmo artigo também estabelece uma causa de aumento de pena de um a dois terços quando há divulgação, comercialização ou transmissão a terceiros dos dados ou informações obtidas (BRASIL, 1940).

2.4. Propagação dos crimes cibernéticos nas redes sociais.

A seguir, apresentam-se as práticas mais comuns de crimes cibernéticos por meio das redes sociais.

2.4.1. *Cyberbullying* (assédio virtual).

Segundo Ferraz (2021), cyberbullying consiste em uma agressão física ou psicológica praticada em ambiente virtual, estando associado aos crimes de calúnia, difamação e injúria previstos no Código Penal. Com o crescimento das redes sociais, essa prática tem se tornado cada vez mais frequente, sendo importante ressaltar que esse tipo de violência pode causar danos irreparáveis à vítima, já que as informações se espalham rapidamente no meio online.

2.4.1.1. Atos que podem ser considerados assédio virtual.

Registra-se que não há um tipo penal específico para o assédio virtual. Todavia, conforme versa o artigo 147-C, do Decreto-Lei nº 2.848/1940, comportamentos que atentem contra a intimidade, a honra, a privacidade e a dignidade sexual de terceiros estão sujeitas a punição pelo Estado, dado que esses bens jurídicos são protegidos pelo direito penal (BRASIL, 1940). Algumas condutas que podem configurar assédio virtual incluem:[3]

- enviar fotos íntimas de terceiros sem permissão;
- enviar mensagens com conotação sexual;
- propagar discursos de ódio contra um indivíduo ou determinado grupo de pessoas;

[3] MOREIRA, Paulo Roberto Silvério. O que é assédio virtual. Migalhas, 2022. Disponível em: https://www.migalhas.com.br/depeso/366628/o-que-e-assedio-virtual. Acesso em: 10 set. 2024.

- divulgar dados de terceiros sem autorização;
- fazer comentários pejorativos em nome de terceiros nas redes sociais;
- instigar à violência;
- espalhar rumores ou boatos que prejudiquem a honra de terceiros.

2.4.1.2. Principais crimes e contravenções penais que o assédio virtual pode caracterizar

- **Calúnia**: caracteriza-se como crime de calúnia a acusação falsa contra alguém, atribuindo-lhe a prática de um crime a terceiro. Assim, divulgar publicações nas redes sociais que imputem a alguém a prática de um fato criminoso, quanto tal fato não é verdadeiro, em tese configura crime de calúnia, conforme o artigo 138 do Código Penal Brasileiro (BRASIL, 1940).
- **Difamação**: descrita no artigo 139 do Código Penal Brasileiro, ocorre difamação no ambiente online quando alguém compartilha informações que ofendem a reputação de outrem (BRASIL, 1940).
- **Injúria**: a injúria envolve a ofensa à imagem e autoestima da vítima. Por exemplo, insultos enviados pela internet podem caracterizar injuria, conforme o artigo 140 do Código Penal Brasileiro (BRASIL, 1940).
- **Invasão de dispositivo informático**: popularmente conhecida como Lei Carolina Dieckmann, a Lei 12.737/2012, que incluiu o artigo 154-A no Código Penal Brasileiro, tipifica a invasão de dispositivos informáticos sem autorização, visando a obtenção, modificação ou destruição de informações. O objetivo da norma é proteger a privacidade e liberdade individual dos cidadãos (BRASIL, 1940).

2.4.2. Disseminação por *malwares* (códigos maliciosos).

Links maliciosos e arquivos infectados podem ser compartilhados por meio de mensagens diretas, postagens ou comentários em redes sociais. Quando clicados, esses links ou arquivos podem instalar malware nos dispositivos das vítimas, comprometendo sua segurança e permitindo que os criminosos acessem dados pessoais ou controlem os dispositivos remotamente. O termo malware, ou software malicioso, refere-se a um conjunto de programas que causam danos aos usuários, geralmente sem que estes tenham consciência do que estão executando (STEINBERG; GAIO, 2021, p.103).

Os impactos do malware são vastos e podem resultar na perda de dados, riscos financeiros, interrupção de serviços, comprometimento de dispositivos, além de outros danos significativos para indivíduos e empresas.[4] Cada tipo de malware possui características específicas que o identificam e o diferenciam dos demais, incluindo a forma de retenção, a maneira de instalação e os meios utilizados para propagar ações maliciosas executadas nos computadores infectados. As formas mais comuns de propagação incluem: executar de maneira automática mídias removíveis, como pendrives; direcionar a sites falsos ou corrompidos; e abrir arquivos infectados. [5]

2.4.2.1. Como se proteger dos *malwares.*[6]

- **Mantenha programas atualizados**: atualize regularmente antivírus e antispyware por meio das opções disponibilizadas pelos fabricantes.
- **Remova programas desnecessários**: desinstale software que não é mais utilizado.
- **Utilize programas originais**: sempre prefira software original e licenciado.
- **Crie um disco de emergência**: utilize-o se suspeitar que o antimalware instalado está corrompido ou se o computador estiver lento, gravando ou lendo o disco rígido com frequência.
- **Verifique logs de segurança**: analise frequentemente os registros gerados pelo seu firewall, sistema operacional e antimalware para identificar possíveis problemas de segurança.
- **Seja cauteloso ao clicar em links**: avalie a origem dos links e quem os enviou antes de clicar.
- **Desabilite a autoexecução de anexos**: configure seu leitor de e-mails para não executar automaticamente arquivos anexados.
- **Desabilite a execução automática de mídias removíveis**: evite a execução automática ao conectar dispositivos como pendrives.

  Realize backups regulares: Mantenha cópias de segurança dos seus dados.

2.4.3. Engenharia social.

[4] CERT.BR. Cartilha de segurança para internet. 2012. Versão 4.0. Disponível em: https://cartilha.cert.br/malware. Acesso em: 10 set. 2024.
[5] CERT.BR. Cartilha de segurança para internet. 2012. Versão 4.0. Disponível em: https://cartilha.cert.br/malware. Acesso em: 10 set. 2024.
[6] CERT.BR. Cartilha de segurança para internet. 2012. Versão 4.0. Disponível em: https://cartilha.cert.br/malware. Acesso em: 10 set. 2024.

Conforme Fontes (2017, p.119), a Engenharia Social é o meio de interação enganosa utilizada por golpistas, envolvendo um conjunto de técnicas persuasivas que visam a obtenção de informações confidenciais de indivíduos ou empresa. De acordo com Tieso e Santos (2020, p.3), os tipos de ataques de engenharia social podem ser classificados da seguinte forma:

> *Phishing*
> É comumente empregada por *hackers e crackers* e consiste em um método comum de acesso fraudulento a informações. Geralmente o ataque é aplicado a diversas pessoas, sistemas de informação ou empresas. Sua finalidade é fazer com que os destinatários acreditem em mensagens falsas enviadas por redes sociais, e-mail, plataformas. Na maioria das vezes acompanhadas de anexos que modificam senhas ou atualizações de cadastros, verificação de informações pessoais.
>
> *Spear Phishing*
> Esta é uma variação do *Phishing* um pouco mais maliciosa e atual. Foca em organizações e empresas, normalmente enviando e-mails e comunicações eletrônicas que parecem ser fontes confiáveis. Contudo, o destinatário é encaminhado para um site falso, onde são clonadas as informações pessoais.
>
> *Vishing*
> De acordo com Kaspersky (2022), a técnica combina voz e *phishing,* onde utiliza-se o telefone para fraudar. Muitas vezes essas ligações são camufladas de telemarketing ou representantes de empresas, para enganar os usuários com ofertas tentadoras e informações enganosas.

2.4.3.1 Como evitar ataques de engenharia social no meio virtual.[7]

- **Não clique em anexos e links**: Evite abrir anexos e clicar em links enviados por e-mail, redes sociais ou mensagens de texto.
- **Limite informações pessoais**: Reduza a quantidade de informações disponíveis em suas redes sociais.

  Use senhas seguras: Proteja seus dispositivos (computadores, celulares, tablets) com senhas fortes.

[7] CERT.BR. Cartilha de segurança para internet. 2012. Versão 4.0. Disponível em: https://cartilha.cert.br/malware. Acesso em: 10 set. 2024.

2.4.4. Estelionato virtual.

Para Roque (2007, p.25), um crime cibernético é toda conduta definida em lei como crime, em que um dispositivo informático é utilizado para prática do delito. O crime de estelionato evoluiu para ambientes virtuais devido aos avanços tecnológicos e à melhoria dos dispositivos que facilitam a vida cotidiana. O estelionato virtual é tipificado no artigo 171 do Código Penal Brasileiro, sendo classificado como fraude eletrônica no § 2º-A do mesmo artigo, onde a principal diferença em relação ao estelionato tradicional é o *modus operandi* do criminoso (BRASIL, 1940).

2.4.4.1. Tipos de ataques que causam danos.[8]

> **Ataques de negação de serviço DoS (*Denial of Service*) e ataques distribuídos de negação de serviço DDoS (*Distributed Denial of Services*).** O objetivo desses ataques é tornar um determinado serviço indisponível.
>
> ***BoTNets e Zoombies*.** Basicamente, os *hackers* infectam inicialmente milhares de computadores na Internet criando uma rede de *zoombies* conhecida como *BoTNet*. Esses computadores podem ser controlados e acessados remotamente pelas máquinas dos *hackers*. Hoje, existe uma série de *BotNets* na Internet, e uma das redes mais conhecidas é a Zeus, que tem milhares de computadores infectados conectados a ela. Os *hackers* que controlam essas *BotNets* normalmente vendem serviços de uso da rede para realizar ataques, armazenar conteúdo e enviar spams.
>
> No controle de uma BotNet, um hacker pode facilmente disparar um ataque de Negação de Serviços Distribuídos (DDoS) enviando um comando para que todas as milhares de máquinas acessem, com o número máximo de conexões possível, alguma máquina-alvo do ataque, normalmente um servidor de alguma corporação.

2.4.4.2. Como evitar ataques de estelionato no meio virtual.

[8] MORAES, Alexandre Fernandes de. Cibersegurança é a nova geração de Firewalls. Rio de Janeiro: Expressa, 2021. *E-book.* p.10.

Izel (2023) aponta que, com o aumento dos casos, é importante que a população esteja ciente dos golpes. A Polícia Civil do DF recomenda as seguintes precauções: não acessar links suspeitos ou desconhecidos, ser atento com imagens e informações publicadas nas redes sociais, além de não fazer pagamentos em contas de pessoas físicas sem antes averiguar se são realmente vinculadas às empresas ou instituições que dizem ser.

A autora enfatiza que, em casos de delitos relacionados a serviços ao consumidor, o Procon-DF oferece orientações importantes. É fundamental que o consumidor verifique a reputação tanto do site quanto da empresa antes de realizar qualquer transação. Além disso, em situações que envolvem boletos ou compras fraudulentas, a recomendação é entrar em contato imediatamente com o fornecedor, utilizando o telefone ou o site oficial da empresa. Todos os casos de fraude devem ser registrados na Polícia Civil do DF (PCDF) para a elaboração do boletim de ocorrência. Nos casos que envolvem serviços ao consumidor, é crucial que a vítima registre também uma reclamação no Procon, vinculado à Secretaria de Justiça e Cidadania (Sejus-DF) (IZEL, 2023).

2.5. Principais características das redes sociais.

Atualmente, as redes sociais desempenham um papel fundamental na comunicação e interação entre pessoas. Elas oferecem diversas funções que facilitam a conexão e o compartilhamento de conteúdo. Segundo dados coletados por We Are Social e Meltwater, em 2024, o Brasil terá 187,9 milhões de usuários da internet, representando 86,6% da população. Esse número é superior à média da América do Sul, que é de 82,5%. As redes sociais são acessadas por 98,9% dos usuários conectados no país, evidenciando sua importância na vida digital dos brasileiros.[9]

Kietzmann (2011, pp.241-251) aponta sete características típicas das redes sociais:

- **Identidade**: os usuários registram os seus dados pessoais;
- **Conversações**: forma com a qual as pessoas se comunicam reciprocamente;
- **Compartilhamento**: os usuários trocam, enviam e recebem conteúdo;

[9] NEGÓCIOS SC. Santa Catarina, 26 de março de 2024. O uso da internet, redes sociais e mídia no Brasil em 2024. Disponível em: https://www.negociossc.com.br/blog/o-uso-da-internet-redes-sociais-e-midia-no-brasil-em-2024. Acesso em: 7 set. 2024.

- **Presença**: coerência e ciência das pessoas sobre o acesso dos demais;
- **Relações**: a maneira com a qual os usuários se associam;
- **Reputação**: demonstra a possibilidade de os usuários conhecerem a fama por meio dos seus próprios conteúdos;
- **Grupos**: possibilidade de criação de comunidades pelos participantes.

3. Considerações Finais.

O dinheiro atrai o crime, e a cada dia circula mais dinheiro na rede. Atualmente, as instituições financeiras no Brasil são as principais vítimas das ameaças digitais, resultando em perdas financeiras significativas devido a fraudes eletrônicas. Muitas dessas fraudes ocorrem não apenas por falhas nos sistemas das instituições, mas também devido à falta de segurança nos equipamentos dos clientes, que muitas vezes não adotam medidas preventivas, como a instalação e atualização de antivírus.

Esta pesquisa acadêmica demonstrou que, embora a inovação tecnológica tenha trazido avanços significativos, também aumentou os riscos e perigos à sociedade, facilitando a propagação de crimes digitais, especialmente os financeiros.

A informação é uma ferramenta crucial na prevenção de ações criminosas no meio virtual, e é vital que a sociedade esteja ciente das vulnerabilidades, buscando conhecimento e auxílio para se proteger contragolpes e outros crimes financeiros.

É essencial conscientizar a população sobre os riscos associados ao uso de redes sociais e plataformas digitais. Medidas como o uso de senhas fortes, atualizações periódicas de programas e atenção redobrada ao acessar conteúdos suspeitos são fundamentais. A responsabilidade de cada usuário é crucial para a proteção individual e para evitar se envolver em crimes virtuais.

Atitudes proativas de usuários, empresas e governos são indispensáveis para prevenir crimes financeiros no ambiente virtual. O uso de legislação adequada, investimento em tecnologias de segurança e promoção de uma cultura digital consciente e segura são fundamentais para mitigar riscos e reforçar a proteção contra crimes que podem causar prejuízos financeiros a indivíduos e instituições.

Os autores desses crimes podem ser responsabilizados criminalmente por furto mediante fraude praticada via dispositivos eletrônicos ou informáticos, bem como por estelionato, que envolve o uso de informações fornecidas pela vítima através de redes

sociais, contatos telefônicos ou e-mails fraudulentos. As penas para esses crimes variam de quatro a oito anos de reclusão, além de multa.

Referências

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 out. 2024.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 14 out. 2024.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 14 out. 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 out. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 out. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 out. 2024.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília,DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 18 out. 2024.

CAPEZ, Fernando Prado. **Código Penal Comentado**. São Paulo: Saraiva, 2016.

CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. **Revista de Direito Eletrônico**. Petrópolis: IBDE, v. 1, n. 3, 2003.

CERT.BR. **Cartilha de segurança para internet**. 2012. Versão 4.0. Disponível em: https://cartilha.cert.br/malware. Acesso em: 10 set. 2024.

CRESPO, Marcelo Xavier de F. **Crimes digitais**. *E-book.* Rio de Janeiro: Saraiva Jur, 2011.

DA SILVA, Patrícia Santos; SILVA, Matheus Passos. **Direito e crime cibernético:** análise da competência em razão do lugar no julgamento de ações penais. Editora Vestnik, 2015.

DOMICÍLIOS, Tic. **Cresce o uso de Internet durante a pandemia e número de usuários no Brasil chega a 152 milhões**, é o que aponta pesquisa do Cetic. br, 2021. Disponível em: https://cetic. br/pt/noticia/cresce-o-uso-de-internet-durante-a-pandemia-e-numero-de-usuariosno-brasil-chega-a-152-milhoes-eo-que-aponta-pesquisa-do-cetic-br. Acesso em: 16 out. 2024.

FEDERAL, Brasil Governo. Tribunal de Justiça do Distrito Federal e dos Territórios-TJDFT. **Direito Fácil**. Edição Semanal: Estelionato, 2021. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato-1#:~:text=A%20fraude%20eletr%C3%B4nica%20ocorre%20quando,cart%C3%A3o%20de%20cr%C3%A9dito%20ou%20d%C3%A9bito. Acesso em: 15 out. 2024.

FERRAZ, Artur. **Violência contra jovens nas redes sociais reacende debate sobre cyberbullying no Brasil**. Folha de Pernambuco, 2021. Disponível em: https://www.folhape.com.br/noticias/violencia-contra-jovens-nas-redes-sociaisreacende-debate-sobre/193767. Acesso em: 17 out. 2024.

FERREIRA, Ivete Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). **Direito e internet**: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

FONTES, Edison. **Segurança da Informação**.1ª edição. Editora Saraiva. 2017.

IZEL, Adriana. **Crimes virtuais causam danos financeiros e morais**. Agência Brasília, 2023. Disponível em: https://www.agenciabrasilia.df.gov.br/2023/10/01/crimes-virtuais-causa-danos-financeiros-e-morais-veja-como-se-proteger. Acesso em: 1 set. 2024.

KIETZMANN, Jan H. [et al]. Social media? Get serious! Understanding the functional building block of social media. *In:* **Business Horizons** [s.l.], v. 54, nº 3, 2011. Disponível em: https://www.sciencedirect.com/science/article/pii/S0007681311000061. Acesso em: 24 out. 2024.

LOPES, R.; SILVA, M. **Compliance Digital e Segurança da Informação**. São Paulo: Editora Jurídica. 2022.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**. São Paulo, 2003.

MORAES, Alexandre Fernandes de. **Cibersegurança e a nova geração de Firewalls**. Rio de Janeiro: Expressa, 2021.

MOREIRA, Paulo Roberto Silvério. O que é assédio virtual. **Migalhas**, 2022. Disponível em: https://www.migalhas.com.br/depeso/366628/o-que-e-assedio-virtual. Acesso em: 10 set. 2024.

NEGOCIOS SC. **O uso da internet, redes sociais e mídia no Brasil em 2024**. Santa Catarina, 26 de março de 2024. Disponível em: https://www.negociossc.com.br/blog/o-uso-da-internet-redes-sociais-e-midia-no-brasil-em-2024. Acesso em: 7 set. 2024.

NUCCI, Guilherme de Souza. **Código Penal comentado**. 17° Edição. Rio de Janeiro: Forense, 2017.

OLIVEIRA, Anderson Soares Furtado. **Crime por Meios Eletrônicos**. Brasília, DF: Universidade Gama Filho, 2009.

RODRIGUES, Leonardo Tulio. Especialista alerta para aumento de crimes nas redes sociais. **Central de Notícias Uninter**, 2022. Disponível em: https://www.uninter.com/noticias/especialista-alerta-para-aumento-de-crimes-nas-redes-sociais. Acesso em: 8 set. 2024.

ROQUE, S. M. **Criminalidade informática**: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007.

STEINBERG, Joseph; GAIO, Carolina**. Cibersegurança para leigos**. Rio de Janeiro: Alta Books, 2020.

TEAM, Kaspersky. **Brasil e a cibersegurança:** ainda somos o maior alvo de ataques na América Latina, 2022. Disponível em: https://www.kaspersky.com.br/blog/panorama-ameacas-latam- 2022/20311. Acesso em: 17 out. 2024.

TIESO, I. H. D. S.; ESPÍRITO SANTO, F. D. Ataques de Engenharia Social. **Revista Interface Tecnológica**, 2020. 206–218. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/947. Acesso em: 24 out. 2024.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos:** Ameaças e procedimentos de investigação. 2ª Edição. Brasport, 2013.