Centro Universitário Processus

PORTARIA Nº 282, DE 14 DE ABRIL DE 2022

CENTRO UNIVERSITÁRIO PROCESSUS
Prática Extensionista

PROJETO/AÇÃO (2025.1)

1. Identificação do Objeto

Atividade Extensionista:

PROGRAMA ( ) PROJETO (X) CURSO ( ) OFICINA ( )

EVENTO ( ) PRESTAÇÃO DE SERVIÇOS ( ) AÇÃO DE EXTENSÃO SOCIAL ( )

Área Temática: Direito Digital e Penal

Linha de Extensão: Atividade Extensionista de Direito Digital

Local de implementação (Instituição parceira/conveniada): Defensoria pública de Brasília no DIA DA MULHER – 02/06/2025.

Título: Crimes cibernéticos e a atuação do direito penal digital.

2. Identificação dos Autor(es) e Articulador(es)

Curso: Direito**.**

Coordenador de Curso: Adalberto Nogueira Aleixo
Articulador(es)/Orientador(es): Prof. Alberto Carvalho Amaral
Aluno(a)/Equipe:

Nome Completo	Curso / Matrícula	Telefone
Ana Gabriele Neves de Souza	2213180000065	(61) 98665-9670
Ana Karen de Deus Silva Botelho	2513180000066	(61) 991592001
Arthur da Cunha Mendes	2413180000173	(61) 99814-8317
Barbara Rodrigues de Oliveira Bonifacio	2423180000130	(61) 984531779
Bruna Sorrechia Ferreira	2517200000016	(61) 98328-8109
Christine Costa dos Santos	24131180000178	(61) 99410-9685
Leonardo Alves Carvalho	2323180000004	(61) 98480-6338
Nivânia de Almeida Silva	2320010000114	(61) 98249-6509
Rodrigo de Freitas Gomes	23200100000102	(61) 98420-0290
Samara de Souza Magalhães	231318000045	(61) 98297-6555

3. Desenvolvimento

Apresentação: O Direito Penal Digital desempenha um papel fundamental na regulação e punição dos crimes cibernéticos, que são infrações cometidas por meio de sistemas informáticos e redes conectadas. Esses crimes incluem práticas como *hacking*, *phishing*, ataques *DDoS*, fraudes, roubo de identidade, *cyberbullying* e assédio virtual. A legislação brasileira avançou com a Lei dos Crimes Cibernéticos (12.737/2012), que tipifica a invasão de dispositivos e a violação de dados, e a Lei 12.735/12, que estabelece normas para infrações digitais.

Entretanto, o Direito Penal Digital enfrenta desafios significativos, como a natureza transnacional da internet, que dificulta a aplicação das leis nacionais, e a necessidade de atualização constante para acompanhar a evolução tecnológica. A harmonização das normas e o fortalecimento da cooperação internacional são essenciais para combater eficazmente esses delitos.

A investigação de crimes cibernéticos no Brasil pode ser conduzida pela Polícia Civil, Polícia Federal ou pelo Ministério Público, reforçando a necessidade de capacitação técnica e colaboração entre órgãos públicos e privados para garantir a eficácia da persecução penal.

Fundamentação Teórica:

1. CRIMES CIBERNÉTICOS E A ATUAÇÃO DO DIREITO PENAL DIGITAL

1.1. Identificação dos Principais Crimes Cibernéticos e seus Impactos na Sociedade Brasileira

A crescente digitalização das relações sociais, econômicas e institucionais trouxe inúmeros benefícios, mas também intensificou a ocorrência de crimes cibernéticos. No Brasil, a legislação tem buscado acompanhar essa realidade por meio de normas específicas, como a Lei nº 12.737/2012 (Lei dos Crimes Cibernéticos), o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e a Lei nº 14.155/2021, que alterou o Código Penal para tratar de fraudes cometidas com uso de tecnologia da informação. Esses diplomas legais formam o núcleo do Direito Penal Digital brasileiro e têm como objetivo a proteção de direitos fundamentais no ambiente virtual, como a privacidade, a segurança da informação e a integridade digital.

Entre os crimes cibernéticos mais recorrentes tipificados no ordenamento jurídico brasileiro, destacam-se: a invasão de dispositivo informático (art. 154-A do Código Penal), que trata do acesso não autorizado a sistemas alheios; a fraude eletrônica, descrita no art. 171, § 2º-A do Código Penal, inserido pela Lei nº 14.155/2021, que consiste em enganar a vítima por meio eletrônico para obter vantagem ilícita, geralmente por redes sociais, aplicativos de mensagens ou e-mails falsos; e o vazamento de dados pessoais, muitas vezes utilizado em práticas de estelionato, chantagem e manipulação de identidade.

Outro crime recorrente é a divulgação de imagens íntimas sem consentimento, tipificada na Lei nº 13.718/2018, com pena de reclusão de um a cinco anos. Esse delito está frequentemente relacionado à chamada "pornografia de vingança", gerando

graves consequências emocionais às vítimas, como depressão, humilhação e isolamento social, além de violar diretamente sua dignidade.

A disseminação de *fake news* e o discurso de ódio nas redes também são fenômenos que vêm preocupando especialistas e autoridades. Apesar de não possuírem uma tipificação penal específica, essas condutas podem ser enquadradas nos crimes de calúnia, difamação, injúria e incitação ao crime. Tais práticas são especialmente nocivas em períodos eleitorais, podendo influenciar negativamente a opinião pública e fomentar polarizações violentas.

A pedofilia na internet representa um dos crimes mais graves nesse contexto. O Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) prevê, em seus artigos 241-A e 241-B, punições para posse, divulgação e armazenamento de conteúdo pornográfico envolvendo crianças ou adolescentes, com penas que variam de um a oito anos de reclusão, além de multa.

Essas condutas produzem impactos profundos na sociedade. No plano individual, causam prejuízos financeiros, danos psicológicos, violação de privacidade e constrangimento público. No plano coletivo, abalam a confiança nos meios digitais, comprometem o ambiente econômico e sobrecarregam o sistema de justiça criminal, cuja atuação é frequentemente dificultada pela transnacionalidade dos delitos, pelo uso de criptografia e pelo anonimato virtual.

Diante disso, é essencial a atuação coordenada das autoridades investigativas, como a Polícia Civil, a Polícia Federal e o Ministério Público, além da constante atualização da legislação, investimento em tecnologia, educação digital da população e cooperação internacional. Essas ações são fundamentais para prevenir, investigar e punir de maneira eficaz os crimes cibernéticos e garantir a segurança dos cidadãos no ambiente digital.

1.2. Exame das Normas Legais Aplicáveis ao Direito Penal Digital: Marco Civil da Internet, Lei Geral de Proteção de Dados e Lei dos Crimes Cibernéticos

A consolidação do ambiente digital como espaço de convivência, negócios e circulação de informações impôs novos desafios ao ordenamento jurídico brasileiro, sobretudo no campo penal. Diante disso, o Direito Penal Digital emergiu como um ramo necessário e dinâmico, voltado à repressão de condutas ilícitas praticadas por meios eletrônicos e à proteção de bens jurídicos afetados pelas novas tecnologias. Neste contexto, destacam-se três pilares normativos fundamentais: o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e a Lei dos Crimes Cibernéticos (Lei nº 12.737/2012), que juntos formam o núcleo normativo da regulação penal no ciberespaço.

O Marco Civil da Internet, ainda que não configure uma norma penal em essência, desempenha papel fundamental na delimitação de direitos e deveres dos usuários e provedores. Entre seus principais dispositivos, destaca-se o reconhecimento da privacidade, da inviolabilidade das comunicações e da proteção de dados pessoais como garantias fundamentais dos usuários (art. 7º). Tais dispositivos norteiam a interpretação penal em casos de interceptação ilegal de comunicações e invasão de dispositivos informáticos. Além disso, o Marco Civil impõe a responsabilidade dos provedores de aplicações apenas quando houver descumprimento de ordem judicial

para remoção de conteúdo ilícito, o que é especialmente relevante nos crimes contra a honra praticados online.

A Lei Geral de Proteção de Dados (LGPD) complementa o Marco Civil ao estabelecer um regime específico para o tratamento de dados pessoais. Embora seu foco principal seja de natureza civil e administrativa, a LGPD introduziu a figura penal do tratamento de dados pessoais mediante fraude (art. 168-A do Código Penal), com pena de reclusão de um a quatro anos. Além disso, o uso indevido de dados pode ser considerado elemento típico de outros crimes, como invasão de dispositivo informático, furto mediante fraude eletrônica e crimes contra a honra. A LGPD também reforça a exigência de consentimento do titular para coleta e uso de dados, sendo esse ponto crucial para definir a licitude ou ilicitude da conduta em casos penais.

Já a Lei dos Crimes Cibernéticos (Lei nº 12.737/2012) representou um marco no enfrentamento de delitos digitais no Brasil. Popularmente conhecida como Lei Carolina Dieckmann, essa norma inseriu no Código Penal o crime de invasão de dispositivo informático (art. 154-A), estabelecendo penas mais severas para condutas que resultem na obtenção de dados sigilosos, controle remoto do sistema ou divulgação de informações obtidas ilicitamente. Também ampliou a proteção penal ao tipificar a interrupção ou perturbação de serviços informáticos (art. 154-B) e equiparar documentos eletrônicos aos documentos físicos para fins de falsificação. Com o advento da Lei nº 14.155/2021, tais crimes passaram a ter penas mais severas quando praticados com uso de meio eletrônico, demonstrando o reconhecimento do agravamento da lesividade dessas condutas.

Apesar dos avanços legislativos, o Direito Penal Digital brasileiro ainda enfrenta desafios relevantes na aplicação prática dessas normas. A natureza transnacional da internet, a rápida evolução tecnológica e a complexidade técnica de certas investigações dificultam a responsabilização dos autores dos crimes. Além disso, a atuação eficaz das autoridades exige capacitação permanente, infraestrutura tecnológica adequada e cooperação internacional, especialmente em casos de pornografia infantil, fraudes bancárias ou ciberterrorismo[1].

Em síntese, as normas analisadas fornecem uma base importante para a atuação do Direito Penal no ambiente digital, assegurando a proteção da privacidade, da integridade informacional e da dignidade das vítimas. No entanto, é imprescindível que tais dispositivos sejam constantemente revisitados, aprimorados e integrados com políticas públicas voltadas à educação digital, prevenção de delitos e fortalecimento das instituições investigativas. Somente assim será possível consolidar um ordenamento jurídico penal verdadeiramente eficaz diante dos desafios do século XXI.

1.3. O Papel das Autoridades Investigativas na Apuração e Repressão dos Crimes Cibernéticos: Uma Análise da Atuação da Polícia Civil, Polícia Federal e Ministério Público

O combate aos crimes cibernéticos no Brasil exige uma atuação coordenada e especializada das autoridades investigativas, uma vez que tais delitos são marcados pela volatilidade, pelo anonimato e, frequentemente, pela transnacionalidade das ações criminosas. Neste cenário, destacam-se três atores centrais: a Polícia Civil, a

[1] Ciberterrorismo é o uso de ataques cibernéticos para atingir um governo ou população com fins políticos ou religiosos. O objetivo é causar danos graves, medo ou coagir as vítimas.

Polícia Federal e o Ministério Público, cujas atribuições, embora distintas, são complementares e essenciais para a eficácia da persecução penal no âmbito digital.

A Polícia Civil, responsável pela esfera estadual da investigação criminal, atua principalmente na repressão a crimes de menor complexidade, mas de elevado impacto social, como fraudes bancárias, estelionato eletrônico, invasão de dispositivos, cyberbullying e divulgação de imagens íntimas sem consentimento. Apesar de suas limitações técnicas em algumas regiões do país, tem desempenhado papel relevante em operações locais, como a Operação Hacker Invicto, deflagrada no Distrito Federal, que resultou na prisão de uma quadrilha especializada em golpes via PIX. Essa atuação demonstra a importância da capacitação das delegacias especializadas e do investimento em tecnologia investigativa.

Por sua vez, a Polícia Federal assume a responsabilidade por delitos de maior gravidade e alcance nacional ou internacional, tais como *ransomware*[2], tráfico de dados, pornografia infantil online, fraudes contra instituições públicas e crimes contra a segurança nacional. Com unidades especializadas, como a Divisão de Repressão a Crimes Cibernéticos (DRCC), a PF tem ampliado sua capacidade de atuação, especialmente por meio de parcerias com agências estrangeiras. Um exemplo emblemático foi a Operação Trojan Shield, conduzida em cooperação com o FBI e a *Europol*, que desarticulou uma rede global de fraudes bancárias, movimentando cerca de R$ 500 milhões. Tais operações evidenciam o papel estratégico da PF na repressão de crimes cibernéticos complexos e transfronteiriços.

O Ministério Público, por sua vez, exerce a função de fiscal da lei e detém a titularidade da ação penal pública. Sua atuação vai além da proposição da denúncia, estendendo-se à supervisão das investigações, proposição de acordos de colaboração premiada, representação por medidas cautelares e atuação em processos que envolvam dados sigilosos e privacidade digital. Destaca-se, nesse sentido, a Operação *Dark Web*, que contou com a atuação conjunta do MP e da Polícia Federal, resultando na desarticulação de fóruns criminosos e na apreensão de criptomoedas[3] utilizadas em transações ilícitas. Ademais, o Ministério Público também tem papel relevante na responsabilização de empresas que não adotam medidas de segurança adequadas para proteção de dados, conforme exigido pela LGPD.

A atuação articulada desses órgãos é indispensável para garantir uma resposta eficaz ao crime digital. Os crimes cibernéticos, por sua natureza complexa, exigem integração entre instituições, celeridade processual, acesso a ferramentas tecnológicas avançadas e colaboração internacional, principalmente quando os criminosos operam a partir de servidores no exterior ou utilizam criptografia de ponta para ocultar seus rastros. Além disso, é essencial o fortalecimento de canais de denúncia e a conscientização da população, permitindo que condutas ilícitas sejam identificadas e comunicadas com maior agilidade.

Portanto, a Polícia Civil, a Polícia Federal e o Ministério Público desempenham papéis distintos, mas igualmente cruciais na prevenção, investigação e repressão dos crimes cibernéticos. O fortalecimento dessas instituições — por meio de investimentos

[2] *Ransomware* é um tipo de *malware* que criptografa ou bloqueia dados, exigindo um pagamento para restaurar o acesso. É um crime cibernético que visa extorquir dinheiro das vítimas.

[3] Ativos virtuais (chamados popularmente de moedas virtuais, criptomoedas ou moedas criptográficas) não são emitidos nem garantidos pelo Banco Central (BC). Não têm as características de uma moeda, ou seja, de meio de troca, de reserva de valor e de unidade de conta, mas, sim, as características de ativo.

estruturais, capacitação contínua e maior interoperabilidade entre seus sistemas — é condição indispensável para garantir a segurança digital da população, assegurar os direitos fundamentais no ambiente virtual e promover justiça.

1.4. Crimes cibernéticos no âmbito do Distrito Federal

Com base nas informações disponíveis, a Polícia Civil do Distrito Federal (PCDF), por meio da Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC), tem adotado diversas medidas para combater os crimes cibernéticos. A seguir, destacam-se as principais ações implementadas:

1. **Operações Policiais Especializadas**: A DRCC realiza operações específicas para desarticular organizações criminosas envolvidas em fraudes eletrônicas e outros delitos cibernéticos. Por exemplo, a Operação IB2K visou desmantelar uma quadrilha que desviava valores de contas de clientes via internet, resultando em prejuízos significativos para instituições financeiras.

2. **Cooperação Internacional**: A PCDF participa de operações conjuntas com agências internacionais para combater crimes cibernéticos transnacionais. A Operação *Darkode* é um exemplo, onde houve colaboração com o FBI e a *Europol* para desmantelar um fórum virtual de hackers que operava em mais de dezoito países, incluindo o Brasil.

3. **Capacitação Contínua dos Servidores**: A PCDF investe na formação e atualização de seus profissionais por meio de cursos especializados. Destacam-se treinamentos em ferramentas de análise de dados, como o programa i2 – *iBase* e *Analyst's* Notebook, que auxiliam na investigação criminal.

4. **Uso de Tecnologias Avançadas**: A adoção de sistemas como o SITTEL (Sistema de Tratamento e Intercâmbio de Informações) permite à PCDF aprimorar a coleta e análise de dados, fortalecendo as investigações cibernéticas.

5. **Educação e Conscientização Pública**: A PCDF promove campanhas educativas para alertar a população sobre os riscos e formas de prevenção contra crimes cibernéticos, incentivando a denúncia e a adoção de práticas seguras no ambiente digital.

Essas medidas refletem o compromisso do Distrito Federal em fortalecer a segurança cibernética e proteger os cidadãos contra as ameaças digitais emergentes. A seguir, destacam-se algumas das principais ações realizadas pela Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC) da Polícia Civil do Distrito Federal (PCDF):

1. **Operação Dígito 8 (2024)**: Desarticulou um esquema de fraudes em pagamentos de guias de arrecadação via QR *Code* PIX, causando um prejuízo de R$ 21 milhões a uma instituição financeira. Os criminosos adulteravam códigos de barras para desviar valores significativos.

2. **Operação *Infamis* – 2ª Fase (2024)**: Em parceria com a Polícia Civil da Bahia, neutralizou o núcleo cibernético de uma quadrilha especializada em furtos bancários, que causou prejuízos estimados em R$ 600 mil a 26 vítimas no Distrito Federal.

3. **Operação *Downloader* – 4ª Fase (2022)**: Visou combater a pornografia infantojuvenil, resultando na prisão de um indivíduo em Planaltina por armazenamento de material pornográfico envolvendo crianças e adolescentes.

4. **Operação Mantigueira (2023)**: Desmantelou um grupo que praticava extorsão pela internet, utilizando aplicativos de relacionamento para obter fotos íntimas das vítimas e exigir pagamentos via PIX para não as divulgar.

5. **Operação Testa de Ferro (2020)**: Investigou uma associação criminosa envolvida em transações bancárias fraudulentas, que resultaram em prejuízos de aproximadamente R$ 800 mil. Os criminosos acessavam contas bancárias das vítimas e realizavam transferências para ocultar a origem dos valores.

6. **Operação *XCoderX* (2020)**: Investigou um esquema interestadual de subtração de valores de contas bancárias, afetando pelo menos 37 vítimas no Distrito Federal e outras em diversos estados. Foram cumpridos 50 mandados judiciais em seis estados brasileiros.

7. **Operação Poderoso Chefão (2020)**: Resultou na condenação de 32 integrantes de uma organização criminosa especializada em furtos de contas bancárias, com penas que somam 257 anos de prisão. A operação foi realizada em conjunto com o Ministério Público do Distrito Federal e Territórios (MPDFT).

Essas operações evidenciam o comprometimento da DRCC/PCDF em enfrentar os desafios impostos pelos crimes cibernéticos, utilizando estratégias investigativas avançadas e cooperação interinstitucional para proteger a sociedade contra ameaças digitais.

2. CONCLUSÃO

Diante da crescente complexidade e sofisticação dos crimes praticados no ambiente digital, o Direito Penal brasileiro tem buscado se adaptar às novas demandas sociais e tecnológicas por meio de um arcabouço normativo específico. A análise do Marco Civil da Internet, da Lei Geral de Proteção de Dados e da Lei dos Crimes Cibernéticos revela importantes avanços legislativos na proteção da privacidade, segurança da informação e repressão a condutas ilícitas, como fraudes eletrônicas, invasões de dispositivos, divulgação de imagens íntimas e crimes contra a honra.

Contudo, os desafios permanecem expressivos. A natureza transnacional dos delitos, a constante evolução tecnológica e a insuficiência estrutural de algumas instituições dificultam a plena efetividade das normas vigentes. Nesse cenário, torna-se indispensável o fortalecimento da atuação das autoridades investigativas, como a Polícia Civil, a Polícia Federal e o Ministério Público, cuja atuação articulada tem se mostrado essencial para a identificação, repressão e responsabilização dos infratores.

Além da aplicação da legislação, é necessário investir na capacitação técnica das instituições, na cooperação internacional e na educação digital da população, de modo a prevenir novas formas de criminalidade e garantir a proteção dos direitos fundamentais no ambiente virtual. A continuidade do aprimoramento normativo e a consolidação de práticas investigativas eficazes representam caminhos promissores para o fortalecimento do Direito Penal Digital no Brasil.

Assim, conclui-se que, embora o país possua instrumentos legais relevantes, o enfrentamento efetivo dos crimes cibernéticos depende de uma atuação integrada entre legislação, instituições e sociedade, aliada à constante atualização frente às novas dinâmicas do ciberespaço.

Tema Geral: Crimes Cibernéticos

Tema Específico do Grupo: Crimes cibernéticos e a atuação do direito penal digital.

Problema verificado: *Em que medida o Direito Penal Digital brasileiro é eficaz na repressão e prevenção dos crimes cibernéticos, considerando os desafios operacionais e normativos enfrentados pelas autoridades?* Cogitou-se a seguinte hipótese: A atual legislação brasileira sobre crimes cibernéticos, apesar dos avanços proporcionados pelo Marco Civil da Internet, pela Lei dos Crimes Cibernéticos e pela Lei Geral de Proteção de Dados, ainda apresenta limitações na sua aplicação prática, especialmente devido à rápida evolução tecnológica, à natureza transnacional dos delitos digitais e à falta de capacitação técnica das autoridades responsáveis.

Objetivo Geral: analisar o papel do Direito Penal Digital na regulação e repressão dos crimes cibernéticos no Brasil, considerando os desafios da aplicação da legislação vigente diante da evolução tecnológica e da natureza transnacional da internet.

Objetivo específico:

1. Identificar os principais crimes cibernéticos tipificados na legislação brasileira e seus impactos na sociedade;

2. Examinar as normas legais aplicáveis ao Direito Penal Digital, incluindo o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a Lei dos Crimes Cibernéticos;

3. Avaliar o papel das autoridades investigativas, como Polícia Civil, Polícia Federal e Ministério Público, na apuração e repressão de crimes cibernéticos; e

4. Crimes cibernéticos no âmbito do Distrito Federal.

Justificativa: A crescente digitalização das relações sociais, econômicas e institucionais trouxe benefícios significativos, mas também aumentou a ocorrência de crimes cibernéticos, que representam desafios para o Direito Penal Digital. A invasão de dispositivos, fraudes eletrônicas, roubo de identidade e assédio virtual são exemplos de práticas que afetam a segurança dos indivíduos e das instituições, exigindo um arcabouço legal eficiente para sua prevenção e repressão.

No Brasil, a legislação avançou com normas como a Lei dos Crimes Cibernéticos (Lei nº 12.737/2012), o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). No entanto, a rápida evolução da tecnologia e a natureza transnacional dos delitos digitais criam desafios à aplicação efetiva dessas normas. Além disso, a necessidade de cooperação entre órgãos nacionais e internacionais, bem como a capacitação técnica das autoridades, são aspectos fundamentais para garantir a eficácia da persecução penal.

Diante desse cenário, este estudo se justifica pela importância de compreender as lacunas e os desafios do Direito Penal Digital, buscando contribuir para o aprimoramento das estratégias de combate aos crimes cibernéticos. A análise da legislação vigente e das dificuldades enfrentadas pelas autoridades permitirá identificar possíveis soluções para fortalecer a segurança jurídica e a proteção dos direitos no ambiente digital.

Metas: Analisar a eficácia do Direito Penal Digital na regulação e repressão dos crimes cibernéticos no Brasil, identificando desafios jurídicos e operacionais e a atuação das autoridades responsáveis pela investigação e persecução penal desses delitos.

Hipótese: A atual legislação brasileira sobre crimes cibernéticos, apesar dos avanços proporcionados pelo Marco Civil da Internet, pela Lei dos Crimes Cibernéticos e pela Lei Geral de Proteção de Dados, ainda apresenta limitações na sua aplicação prática, especialmente devido à rápida evolução tecnológica, à natureza transnacional dos delitos digitais e à falta de capacitação técnica das autoridades responsáveis. Dessa forma, o aprimoramento normativo e a ampliação da cooperação internacional podem ser fundamentais para aumentar a eficácia do Direito Penal Digital na repressão e prevenção desses crimes.

Resultados esperados: Espera-se que este estudo possa contribuir com o operador do Direito devido à crescente demanda por conhecimento técnico-jurídico frente aos desafios do cibercrime[4] e à necessidade de atuação efetiva diante da complexidade dos delitos virtuais, bem como para a ciência visando ampliar o referencial teórico sobre a efetividade do Direito Penal Digital, contribuindo para o aperfeiçoamento normativo e investigativo frente às novas tecnologias e que possa agregar à sociedade pelo fato de promover a conscientização sobre os riscos no ambiente digital e subsidiar a formulação de políticas públicas voltadas à proteção de direitos fundamentais, como a privacidade e a segurança da informação.

Metodologia: Este estudo foi desenvolvido por meio de pesquisa bibliográfica, com o objetivo de analisar o Direito Penal Digital e sua aplicação na repressão aos crimes cibernéticos no Brasil. A pesquisa se baseia em fontes doutrinárias, legislações vigentes e artigos científicos que tratam do tema, permitindo uma abordagem teórica aprofundada sobre os desafios e as possíveis soluções para a persecução penal desses delitos.

A metodologia adotada seguiu uma abordagem qualitativa, com a análise de normas como o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e a Lei dos Crimes Cibernéticos (Lei nº 12.737/2012), além de obras de especialistas em Direito Digital e Penal. A revisão bibliográfica possibilitará a compreensão do cenário atual, identificando lacunas na legislação e dificuldades enfrentadas pelas autoridades na investigação e punição dos crimes cibernéticos. Dessa forma, o estudo buscará apresentar um diagnóstico do tema e propor medidas para aprimorar a eficácia do Direito Penal Digital.

Cronograma de execução:

DATA DE INÍCIO: 28\03\2025

[4] Cibercrime é um crime cometido por meio da internet, utilizando computadores ou dispositivos conectados em rede. Também é conhecido como crime informático ou crime virtual.

DATA DE TÉRMINO: 04\07\2025

Evento	Período	Observação
Visitação na Defensoria	28\03\2025	visitar o lugar da apresentação.
Elaboração do Projeto	29/03/2025 a 29/05/2025	
Apresentação ao professor orientador	30/05/2025	
Apresentação na defensoria	02\06\2025	Dia da Mulher na Defensoria Pública
Relatório Final	04/07/2025	

Referência Bibliográfica:

BRASIL. ***Constituição da República Federativa do Brasil de 1988***. Diário Oficial da União: seção 1, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 abr. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 8 abr. 2025.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. **Estatuto da Criança e do Adolescente. Diário Oficial da União**: seção 1, Brasília, DF, 16 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 8 abr. 2025.

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**. *Diário Oficial da União: seção 1*, Brasília, DF, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 11 abr. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** *Diário Oficial da União: seção 1*, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 abr. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera o Marco Civil da Internet.** *Diário Oficial da União: seção 1*, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 abr. 2025.

BRASIL. Lei nº 14.155, de 27 de maio de 2021**. Altera o Código Penal para dispor sobre os crimes de violação de dispositivo informático, furto mediante fraude e estelionato praticados com uso de tecnologia da informação.** *Diário Oficial da União: seção 1*, Brasília, DF, 28 maio 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 11 abr. 2025.

BLUM, Ricardo. ***Marco Civil da Internet comentado***. 2. ed. São Paulo: Thomson Reuters Brasil, 2016.

CORREIO BRAZILIENSE. **Esquema de lavagem de dinheiro que lucrou R$ 21 mi é alvo da PCDF**. Correio Braziliense, Brasília, 23 jan. 2024. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2024/01/6788746-esquema-de-lavagem-de-dinheiro-que-lucrou-rs-21-mi-e-alvo-da-pcdf.html. Acesso em: 11 abr. 2025.

CORREIO BRAZILIENSE. **Membros de organização criminosa são condenados a 257 anos de prisão.** Correio Braziliense, Brasília, 20 dez. 2021. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2021/12/4971309-membros-de-organizacao-criminosa-sao-condenados-a-257-anos-de-prisao.html. Acesso em: 11 abr. 2025.

DONEDA, Danilo; GAETA, Tiago; TEIXEIRA, Ricardo (Coords.). ***Lei Geral de Proteção de Dados comentada*.** São Paulo: Thomson Reuters Brasil, 2019.

JORNAL DE BRASÍLIA. **PCDF desmantela organização criminosa especializada em crimes cibernéticos.** Jornal de Brasília, Brasília, 12 mar. 2024. Disponível em: https://jornaldebrasilia.com.br/brasilia/pcdf-desmantela-organizacao-criminosa-especializada-em-crimes-ciberneticos/. Acesso em: 11 abr. 2025.

JORNAL DE BRASÍLIA. **PCDF deflagra quarta fase de operação de combate à pornografia infantojuvenil. Jornal de Brasília**, Brasília, 21 nov. 2022. Disponível em: https://jornaldebrasilia.com.br/nahorah/pcdf-deflagra-quarta-fase-de-operacao-de-combate-a-pornografia-infantojuvenil/. Acesso em: 11 abr. 2025.

JORNAL DE BRASÍLIA. **PCDF combate crime de extorsão pela internet.** Jornal de Brasília, Brasília, 10 maio 2023. Disponível em: https://jornaldebrasilia.com.br/brasilia/pcdf-combate-crime-de-extorsao-pela-internet/. Acesso em: 11 abr. 2025.

METRÓPOLES. **Fraude bancária: PCDF mira em grupo que desviou R$ 800 mil de contas. Metrópoles, Brasília, 30 nov. 2020**. Disponível em: https://www.metropoles.com/distrito-federal/fraude-bancaria-pcdf-mira-em-grupo-que-desviou-r-800-mil-de-contas. Acesso em: 11 abr. 2025.

NUCCI, Guilherme de Souza. ***Crimes cibernéticos***. 4. ed. Rio de Janeiro: Forense, 2022.

OLIVEIRA, Rafael Augusto Quaresma de. ***Proteção de dados pessoais e o direito penal***. São Paulo: Tirant lo Blanch, 2020.

PINHEIRO, Rafael. ***Direito penal digital: desafios e perspectivas***. Rio de Janeiro: Lumen Juris, 2020.

TAVARES, André Ramos; LENZA, Pedro. ***Direito digital***. 7. ed. São Paulo: Saraiva Educação, 2023.

YOSHIDA, Consuelo Yatsuda Moromizato. ***Direito penal informático***. 6. ed. São Paulo: Saraiva Educação, 2020.

Anexos

Anexo I – Principais Golpes Praticados Contra a Comunidade
Anexo II – Alerta para Golpe do Whatsapp por meio de Outras Linhas Telefônica
Anexo III – Golpe do Leilão Falso pela Internet

Anexo I – Principais Golpes Praticados Contra a Comunidade

Golpe do perfil falso no WhatsApp

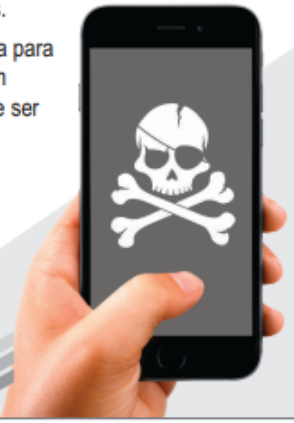
Como acontece o golpe:
Os criminosos vinculam a fotografia da vítima, normalmente retirada do próprio WhatsApp ou de redes sociais, a um número telefônico. Se passando por ela, eles solicitam dinheiro e/ou outras vantagens para os conhecidos da vítima.

O que fazer caso tenha sido vítima:
Denunciar o perfil falso no aplicativo WhatsApp usando o suporte@whatsapp.com ou clicar no número que enviou a mensagem e, no campo "dados do contato" clicar em denunciar.

Como se prevenir:
Fique atento às mensagens de solicitação de dinheiro por conhecidos.

Desconfie se a fotografia do perfil do WhatsApp estiver vinculada a uma linha de telefônica que não esteja cadastrada nos seus contatos.

Se a conta bancária informada para depósito de valores estiver em nome de terceiro, a chance de ser fraude é ainda maior.



Golpe de investimentos

Como acontece o golpe:

Os criminosos usam pessoas jurídicas com aparente credibilidade para oferecer investimentos pessoais com ganhos e taxas de juros acima dos comumente praticados no mercado. Eles alegam que atuam no mercado de ações ou que possuem algum produto de grande valia.

As vítimas fazem aportes de dinheiro, em diversos níveis e momentos distintos, e com esses valores os criminosos pagam investimentos daqueles que entraram antes, apresentando uma suposta credibilidade no modelo de negócio.

Assim, os primeiros investidores, animados com seus ganhos, acabam trazendo outros que também fazem aportes. Dessa forma, fazem girar o sistema financeiro criado pelos criminosos, até o momento em que estes "quebram" o esquema, desviando milhares de reais dos investidores.

Não se trata da conhecida "pirâmide financeira", pois não há o recrutamento voluntário progressivo que caracteriza esta modalidade de sistema como forma de auferir ganhos. O golpe de investimento independe de qualquer recrutamento a ser feito pelo investidor.

Golpe de investimentos

Como se prevenir :

Sempre suspeitar de ofertas de investimentos com ganhos acima daqueles praticados pelo mercado bancário regular, ainda que apresentados por empresas com aparente credibilidade, ou por pessoas conhecidas e familiares, que podem estar na base do sistema e por isso receberam algum "rendimento", os fazendo crer na rentabilidade do negócio.

Verificar se existe autorização do Banco Central e fiscalização do Conselho de Valores Mobiliários.

Lembre-se, esse esquema a qualquer momento pode ser interrompido e quebrado, deixando inúmeras vítimas.

Golpe do motoboy de banco

Como acontece o golpe:

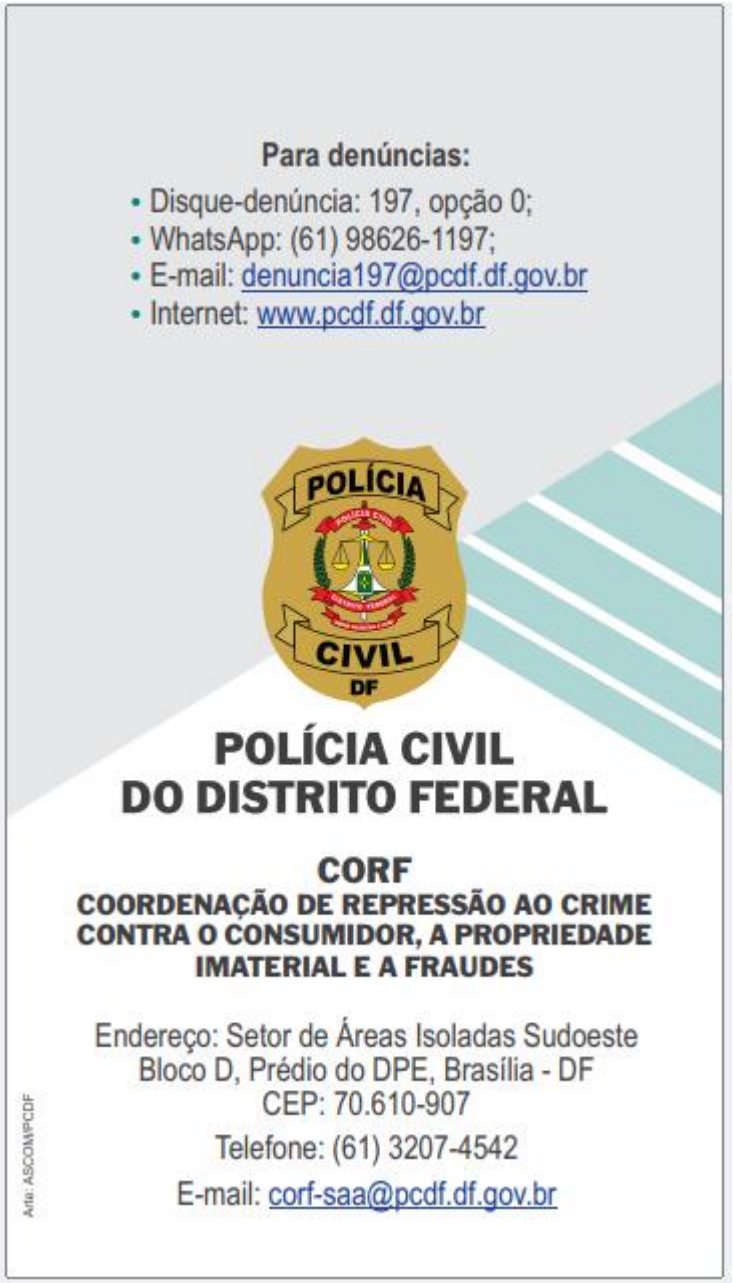
A vítima recebe ligação telefônica supostamente da área de segurança do banco e é questionada sobre uma compra realizada com seu cartão de crédito. Diante da resposta negativa, o interlocutor confirma alguns dados pessoais, informa que o cartão de crédito foi clonado, mas que já está cancelado. Explica que, para comodidade do cliente, um funcionário da agência, devidamente identificado com crachá, irá comparecer à residência da vítima para pegar o cartão de crédito cancelado e também uma declaração de não reconhecimento de compra. Na posse do cartão, o criminoso realiza saques e diversas compras em nome da vítima.

Como se prevenir:

Suspeite de ligações telefônicas que questionem compras realizadas com o cartão de crédito.

Não forneça por telefone dados pessoais tais como endereço e senha de cartão bancário.

Os bancos não dispõem de serviço delivery, ou seja, não enviam funcionários a residências de clientes para pegar documentos e cartões.


Para denúncias:
• Disque-denúncia: 197, opção 0;
• WhatsApp: (61) 98626-1197;
• E-mail: denuncia197@pcdf.df.gov.br
• Internet: www.pcdf.df.gov.br
POLÍCIA
CIVIL
DF
POLÍCIA CIVIL
DO DISTRITO FEDERAL
CORF
COORDENAÇÃO DE REPRESSÃO AO CRIME CONTRA O CONSUMIDOR, A PROPRIEDADE IMATERIAL E A FRAUDES
Endereço: Setor de Áreas Isoladas Sudoeste
Bloco D, Prédio do DPE, Brasília - DF
CEP: 70.610-907
Telefone: (61) 3207-4542
E-mail: corf-saa@pcdf.df.gov.br
Arte: ASCOM/PCDF

Anexo II – Alerta para Golpe do Whatsapp por meio de Outras Linhas Telefônica

Golpe do WhatsApp por meio de outra linha telefônica

Com o objetivo de obter vantagem indevida, criminosos estão utilizando a seguinte estratégia para enganar usuários do aplicativo WhatsApp:

1. Inicialmente, o criminoso obtém o número de telefone e outros dados de um usuário do WhatsApp, principalmente a partir de serviços da internet que comercializam dados pessoais paras fins de comércio eletrônico (e-commerce);

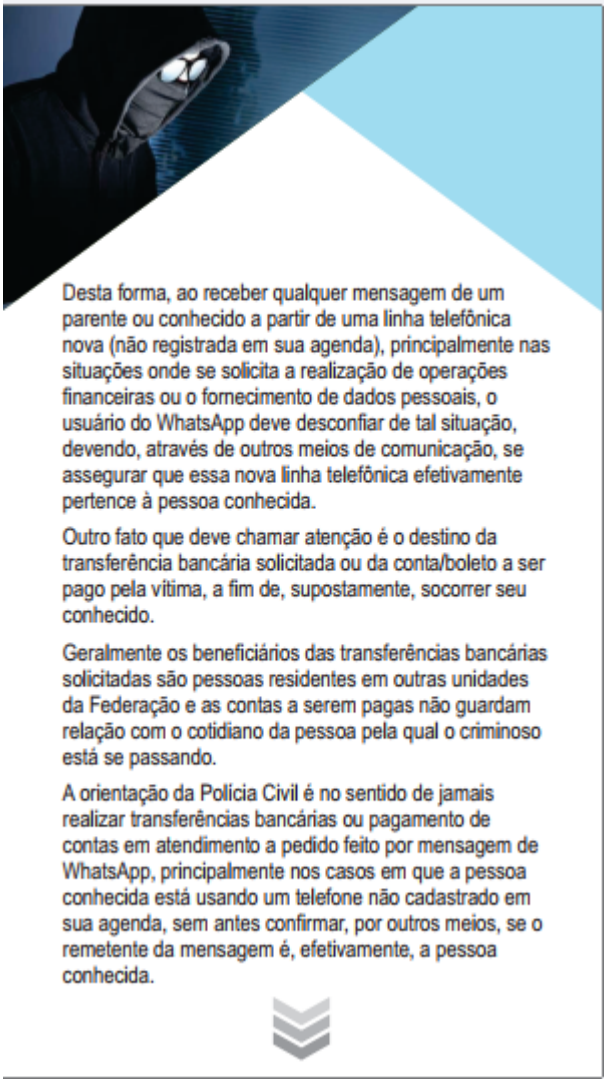
2. Após, o criminoso inicia uma pesquisa para identificar o nome e o telefone de parentes ou pessoas próximas da vítima, através de consultas em sites clandestinos de fornecimento de dados ou consultas em serviços semelhantes da Deep Web.

3. Ao identificar nomes e telefones de pessoas próximas de uma potencial vítima, o criminoso copia a imagem/fotografia que aparece no WhatsApp da pessoa pela qual pretende se passar e, utilizando uma linha telefônica qualquer, cria uma nova conta no aplicativo de mensagens usando a imagem/foto original da vítima ou outra obtida em redes sociais.

4. O passo final do golpe consiste em mandar uma mensagem para o parente ou pessoa próxima da vítima, se passando por ela, a fim de narrar algum tipo de situação emergencial que demande a transferência de dinheiro ou o pagamento de alguma conta como forma de sanar/minorar tal imprevisto.

5. Nos casos em que a vítima indaga ao criminoso sobre a nova linha telefônica utilizada no WhatsApp, até então desconhecido, o estelionatário informa, se passando por tal pessoa, que teria trocado sua linha telefônica antiga para uma nova.


WhatsApp
+55 61 9999-9999
Dicas
de segurança
Note que para realizar esse golpe, o criminoso tem de fazer uso de uma linha telefônica que não estará registrada na agenda do celular da pessoa que recebe a ligação;
Desta forma, ao receber qualquer mensagem de um parente ou conhecido a partir de uma linha telefônica nova (não registrada em sua agenda), principalmente nas situações onde se solicita a realização de operações financeiras ou o fornecimento de dados pessoais, o usuário do WhatsApp deve desconfiar de tal situação, devendo, através de outros meios de comunicação, se assegurar que essa nova linha telefônica efetivamente pertence à pessoa conhecida.


Desta forma, ao receber qualquer mensagem de um parente ou conhecido a partir de uma linha telefônica nova (não registrada em sua agenda), principalmente nas situações onde se solicita a realização de operações financeiras ou o fornecimento de dados pessoais, o usuário do WhatsApp deve desconfiar de tal situação, devendo, através de outros meios de comunicação, se assegurar que essa nova linha telefônica efetivamente pertence à pessoa conhecida.
Outro fato que deve chamar atenção é o destino da transferência bancária solicitada ou da conta/boleto a ser pago pela vítima, a fim de, supostamente, socorrer seu conhecido.
Geralmente os beneficiários das transferências bancárias solicitadas são pessoas residentes em outras unidades da Federação e as contas a serem pagas não guardam relação com o cotidiano da pessoa pela qual o criminoso está se passando.
A orientação da Polícia Civil é no sentido de jamais realizar transferências bancárias ou pagamento de contas em atendimento a pedido feito por mensagem de WhatsApp, principalmente nos casos em que a pessoa conhecida está usando um telefone não cadastrado em sua agenda, sem antes confirmar, por outros meios, se o remetente da mensagem é, efetivamente, a pessoa conhecida.

Procedimento no caso de consumação do golpe

Caso a pessoa que recebeu a mensagem do criminoso efetue a transferência bancária ou realize o pagamento do boleto solicitado, as seguintes providências deverão ser adotadas:

- Faça uma cópia de todas as mensagens trocadas com o criminoso que se passou pelo conhecido da vítima;
- Guarde o comprovante de transferência bancária contendo o nome do beneficiário e o boleto eventualmente pago a pedido do criminoso;
- Registre ocorrência de estelionato pela internet ou em uma das unidades da PCDF, apresentando os documentos anteriormente mencionados;
- Se o valor do prejuízo for maior do que 20 (vinte) salários mínimos, a ocorrência poderá ser registrada diretamente na Delegacia Especial de Repressão aos Crime Cibernéticos.

Para denúncias:

- Disque-denúncia: 197, opção 0;
- WhatsApp: (61) 98626-1197;
- E-mail: denuncia197@pcdf.df.gov.br
- Internet: www.pcdf.df.gov.br

POLÍCIA CIVIL DF

POLÍCIA CIVIL DO DISTRITO FEDERAL

DRCC
DELEGACIA ESPECIAL DE REPRESSÃO AOS CRIMES CIBERNÉTICOS

Endereço: Setor de Áreas Isoladas Sudoeste
Bloco D, Prédio do DPE, Brasília - DF
CEP: 70.610-200

Telefone: (61) 3207-4892

E-mail: drcc-atendimento@pcdf.df.gov.br

Arte: ASCOM/PCDF

Anexo III – Golpe do Leilão Falso pela Internet

Muitos sites falsos de leilão de veículos têm sido criados na internet por criminosos. Eles induzem a vítima a realizar lances e posteriormente a depositar o respectivo valor da arrematação em contas bancárias em nome de terceiros.

Conheça as principais dicas para identificar possíveis sites falsos:

SITES COM DOMÍNIOS ESTRANGEIROS:

Com o objetivo de evitar a utilização de domínios brasileiros ".com.br", cujo registo exige muito mais informações do que os domínios internacionais, a maioria dos criminosos que atuam em leilões falsos de veículos fazem uso de domínios "links" internacionais.

Após analisar diversos domínios de sites falsos de leilão de veículos, verificou-se que a maior parte deles termina da seguinte forma: ".com" ou ".com/br".

É importante frisar que os sites ".com.br" são diferentes dos sites ".com/br", pois no segundo tipo, a expressão "/br" configura, apenas, um subdomínio inserido para dar impressão de que o domínio é brasileiro, quando na realidade não é.

Desta forma, ao se deparar com um site de leilão de veículos cujo domínio termine com ".com" ou ".com/br", o primeiro sinal que indica a possibilidade de fraude já pode ser identificado.

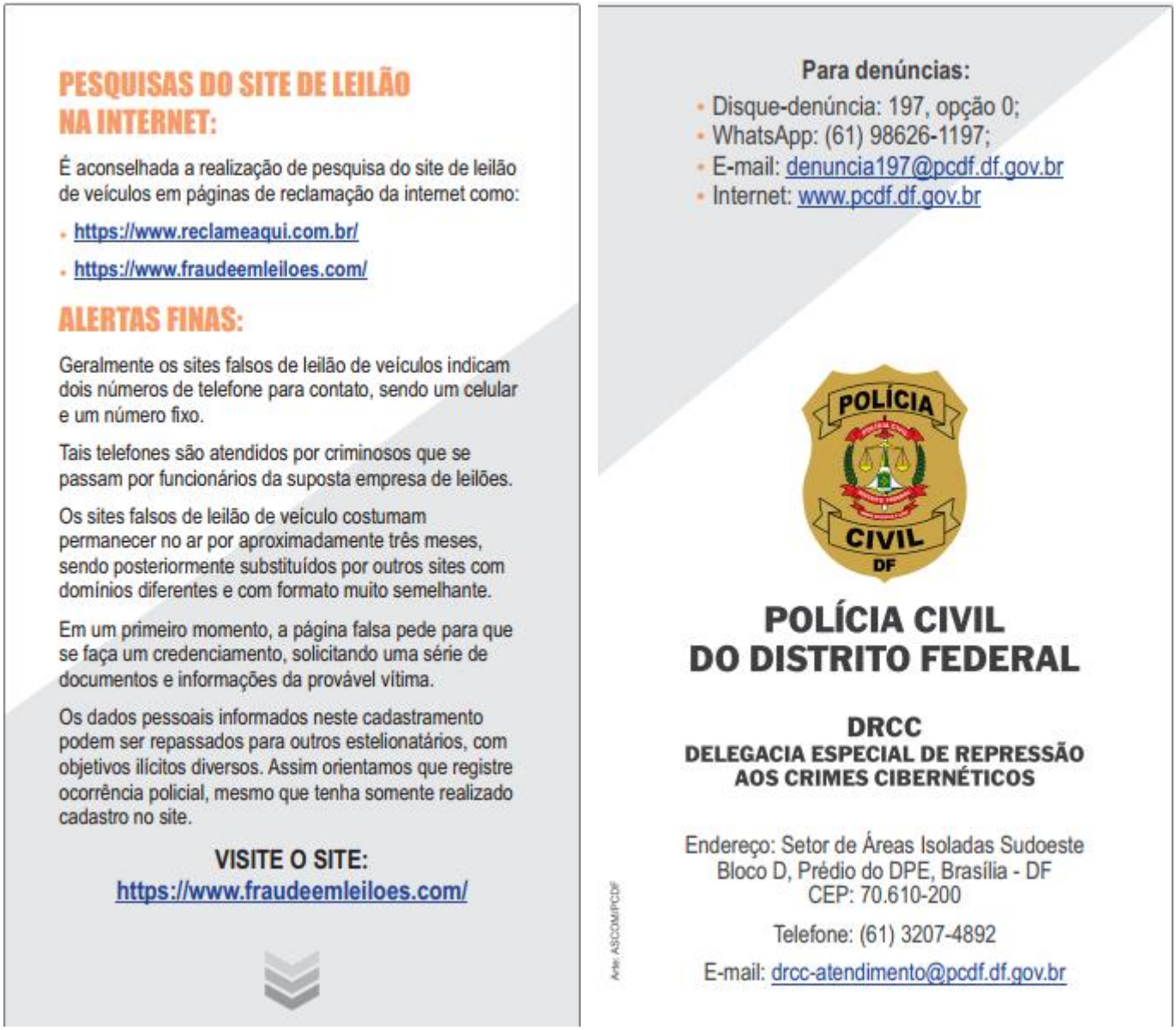
SITES CUJO DOMÍNIO FOI CRIADO HÁ POUCO TEMPO:

Caso decida participar de um site de leilão de veículos pela internet, cujo domínio é estrangeiro ".com" ou ".com/br", o interessado deve verificar sua data de criação.

Para obter tal informação, basta pesquisar o domínio do site de leilão na seguinte página da internet: http://whois.domaintools.com/

Como resultado de tal pesquisa será exibida a data de criação do domínio:

Quando a data de criação do domínio for igual ao inferior ao prazo de seis meses em relação às datas designadas para os leilões, haverá forte indício de que a criação do respectivo site se deu em período muito próximo, o que, igualmente, aponta para o segundo sinal da possibilidade de fraude.



PESQUISAS DO SITE DE LEILÃO NA INTERNET:

É aconselhada a realização de pesquisa do site de leilão de veículos em páginas de reclamação da internet como:

- https://www.reclameaqui.com.br/
- https://www.fraudeemleiloes.com/

ALERTAS FINAS:

Geralmente os sites falsos de leilão de veículos indicam dois números de telefone para contato, sendo um celular e um número fixo.

Tais telefones são atendidos por criminosos que se passam por funcionários da suposta empresa de leilões.

Os sites falsos de leilão de veículo costumam permanecer no ar por aproximadamente três meses, sendo posteriormente substituídos por outros sites com domínios diferentes e com formato muito semelhante.

Em um primeiro momento, a página falsa pede para que se faça um credenciamento, solicitando uma série de documentos e informações da provável vítima.

Os dados pessoais informados neste cadastramento podem ser repassados para outros estelionatários, com objetivos ilícitos diversos. Assim orientamos que registre ocorrência policial, mesmo que tenha somente realizado cadastro no site.

VISITE O SITE:
https://www.fraudeemleiloes.com/

Para denúncias:

- Disque-denúncia: 197, opção 0;
- WhatsApp: (61) 98626-1197;
- E-mail: denuncia197@pcdf.df.gov.br
- Internet: www.pcdf.df.gov.br

POLÍCIA CIVIL DF

POLÍCIA CIVIL DO DISTRITO FEDERAL

DRCC
DELEGACIA ESPECIAL DE REPRESSÃO AOS CRIMES CIBERNÉTICOS

Endereço: Setor de Áreas Isoladas Sudoeste
Bloco D, Prédio do DPE, Brasília - DF
CEP: 70.610-200

Telefone: (61) 3207-4892

E-mail: drcc-atendimento@pcdf.df.gov.br

Arte: ASCOM/PCDF