



Estelionato Eletrônico no Direito Digital

Alana Nagashima de Lima

Bianca e Silva Caires

Carlos Eduardo da Silva Costa Junior

Filipe Borges Marra

Lucas Felipe Machado Silva

Miguel Nardi Coral

Samara Adriele Fernandes Martins Matos

Sarah Emanuelle de Souza Silva

Tayná Cesar Justino de Mello

Vivian Carvalho Santos



Introdução

O estelionato no direito digital envolve o uso de meios eletrônicos e digitais para enganar ou obter vantagem ilícita de terceiros, utilizando-se de fraudes em plataformas online, redes sociais, e-mails ou aplicativos. Com o avanço da tecnologia e o aumento das transações online, crimes dessa natureza têm se tornado cada vez mais comuns, exigindo novas formas de combate e prevenção.

Definição e Características

Estelionato eletrônico se caracteriza por atos fraudulentos que visam obter vantagem ilícita em operações financeiras ou comerciais realizadas por meio de sistemas eletrônicos. Essa prática envolve o uso de táticas de persuasão e manipulação para induzir vítimas a realizarem transações fraudulentas.

1

Engano

A base do estelionato eletrônico é o engodo da vítima, levando-a a acreditar em informações falsas ou a realizar ações que lhe causam prejuízo.

2

Uso de Tecnologias

O crime se vale de computadores, smartphones, internet e outras tecnologias para alcançar suas vítimas e perpetrar seus atos ilícitos.

3

Objetivo Financeiro

A motivação principal é obter lucro financeiro, seja por meio de transferências bancárias, compras fraudulentas ou acesso a dados confidenciais.



Modalidades de Estelionato Eletrônico

O estelionato eletrônico assume diversas formas, cada uma com suas características e métodos de execução.

Phishing

Envio de e-mails falsos para induzir vítimas a fornecer dados confidenciais, como senhas e dados bancários.

Golpes em Sites Falsos

Criar sites falsos que imitam páginas legítimas para coletar dados pessoais e financeiros de usuários.

Ataques de Engenharia Social

Manipular vítimas por meio de táticas psicológicas para convencê-las a realizar ações que as prejudicam.

Legislação Aplicável no Direito Digital

O combate ao estelionato eletrônico exige a aplicação de leis específicas que criminalizam essas práticas e garantem a proteção aos usuários do ambiente digital.

Código Penal Brasileiro e Lei 14.155/2021

Arts. 171 e § 2-A e B: estelionato, incluindo modalidades eletrônicas.

Marco Civil da Internet (Lei nº 12.965/2014)

Princípios e regras para o uso da internet, incluindo a proteção de dados pessoais e a responsabilização por danos.

Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado

Danos Causados pelo Estelionato Eletrônico

As consequências do estelionato eletrônico podem ser graves para indivíduos e empresas, causando prejuízos financeiros, psicológicos e sociais.

1

Prejuízo Financeiro

Perda de dinheiro por meio de transferências fraudulentas, compras não autorizadas ou roubo de dados bancários.

2

Dano Moral

Abalo psicológico e emocional causado pela violação da privacidade, perda de confiança e sensação de impotência.

3

Danos à Reputação

Mancha na reputação de indivíduos e empresas, especialmente em casos de vazamento de dados e crimes que envolvem a imagem.



Prevenção e Combate ao Estelionato Eletrônico

Combater o estelionato eletrônico exige ações preventivas e punitivas, envolvendo autoridades, empresas e usuários.



Sensibilização e Educação

Campanhas de conscientização para o público sobre os riscos do estelionato eletrônico e medidas de segurança.



Investigação e Repressão

Ações policiais para identificar, prender e responsabilizar criminosos, além do uso de inteligência para rastrear atividades suspeitas.



Tecnologia de Segurança

Uso de softwares de segurança, antivírus, firewalls e autenticação de dois fatores para proteger dispositivos e dados.



Cooperação Internacional

Troca de informações entre países para rastrear atividades criminosas transnacionais e fortalecer a aplicação da lei.



Responsabilização Civil e Criminal

Os autores de estelionato eletrônico podem ser responsabilizados civil e criminalmente, com penas e medidas judiciais aplicáveis aos crimes cometidos.

1

Responsabilidade Civil

Indenização por danos causados às vítimas, incluindo prejuízos materiais e morais, podendo ser aplicada de forma individual ou coletiva.

2

Responsabilidade Criminal

Penas de prisão e multas, além de medidas cautelares como a proibição de acesso à internet, dependendo da gravidade do crime.

3

Procedimentos Legais

Investigação policial, ação penal, processo judicial, sentença e cumprimento de pena, com possibilidade de recursos e revisão judicial.



Conclusão e Considerações Finais

O estelionato eletrônico representa um desafio crescente para o direito digital, exigindo atenção constante e ações eficazes para combater esse tipo de crime e proteger os cidadãos no mundo virtual.

Segurança Digital

A prevenção é fundamental para evitar ser vítima de estelionato. Mantenha seus dispositivos e dados seguros, utilizando senhas fortes e atualizando softwares.

Conscientização

Fique atento a tentativas de fraude, desconfiando de e-mails suspeitos, ligações inesperadas e ofertas irresistíveis. Informe-se sobre os riscos e medidas de segurança.

Combate à Impunidade

É importante denunciar crimes cibernéticos às autoridades competentes. A colaboração entre usuários, empresas e órgãos de segurança é crucial para combater o estelionato eletrônico.

