

CRIMES INFORMÁTICOS NO BRASIL

Os principais delitos praticados no ambiente digital, sua tipificação penal, as penas aplicáveis e como o cidadão pode se proteger e denunciar.

Por Wilson Furtado Roberto

O que são crimes informáticos?

Crimes informáticos (ou crimes cibernéticos) são condutas ilícitas praticadas por meio de sistemas informáticos, dispositivos eletrônicos ou da internet, ou que têm esses sistemas como alvo.

01

Crimes informáticos próprios

A tecnologia é o próprio alvo do delito. Só existem no meio digital. Ex.: invasão de dispositivo informático (art. 154-A do CP) e ataques a sistemas.

02

Crimes informáticos impróprios

Delitos clássicos cometidos com auxílio da tecnologia. Ex.: estelionato, furto mediante fraude, crimes contra a honra e ameaça praticados pela internet.

PANORAMA

Um crime em plena expansão

Dados da 19ª edição do Anuário Brasileiro de Segurança Pública (FBSP, 2025), referentes ao ano de 2024:

2,2 mi

casos de estelionato registrados
no Brasil em 2024 – cerca de 4
golpes por minuto

+408%

crescimento dos registros
de estelionato entre 2018 e
2024

281 mil

estelionatos por meio eletrônico
em 2024, alta de 17% sobre 2023

Os números reais tendem a ser ainda maiores: nem todos os estados destacam o meio eletrônico nos registros, e muitas vítimas não formalizam ocorrência.

Evolução da legislação brasileira

2008

Endurece o ECA contra a pornografia infantil na internet (arts. 241-A a 241-E).

2012

"Lei Carolina Dieckmann": cria o crime de invasão de dispositivo informático (art. 154-A do CP).

2014

Marco Civil da Internet: direitos, deveres e guarda de registros de conexão e acesso.

2018

LGPD: proteção de dados pessoais e sanções para tratamento irregular.

2021

Leis 14.132 e 14.155

Stalking e endurecimento das penas da fraude eletrônica e da invasão de dispositivo.

2024-25

Leis 14.811, 15.123 e 15.211

Cyberbullying, agravamento para uso de IA contra a mulher e ECA Digital.

MARCO LEGAL

Lei Carolina Dieckmann (Lei 12.737/2012)

Aprovada após o vazamento de fotos íntimas da atriz que lhe deu o apelido, foi a primeira lei brasileira a tipificar especificamente os delitos informáticos. Inseriu no Código Penal o crime de invasão de dispositivo informático (art. 154-A) e equiparou o cartão de crédito ou débito a documento particular para fins de falsificação (art. 298, parágrafo único).

COMO OCORRE NA PRÁTICA

Invasão de celulares, computadores e contas para obter dados
Instalação de vulnerabilidades para obter vantagem ilícita

TIPIFICAÇÃO

Art. 154-A do Código Penal,

com redação da Lei 14.155/2021

PENA

Reclusão de 1 a 4 anos e multa, com aumento se houver prejuízo econômico ou obtenção de conteúdo privado

CRIMES EM ESPÉCIE

Invasão de dispositivo informático

Consiste em invadir dispositivo informático de uso alheio, conectado ou não à internet, com o fim de obter, adulterar ou destruir dados sem autorização do usuário, ou instalar vulnerabilidades para obter vantagem ilícita. A Lei 14.155/2021 endureceu as penas e retirou a exigência de violação de mecanismo de segurança – basta a ausência de autorização.

COMO OCORRE NA PRÁTICA

Acesso indevido a e-mails, redes sociais e nuvem
Obtenção de senhas, conversas e segredos comerciais

TIPIFICAÇÃO

Art. 154-A do Código Penal

PENA

Reclusão de 1 a 4 anos e multa;
de 2 a 5 anos se da invasão resultar obtenção de conteúdo privado ou segredos

CRIMES EM ESPÉCIE

Fraude eletrônica (estelionato digital)

É o estelionato cometido com informações fornecidas pela vítima ou por terceiro induzido a erro por redes sociais, e-mails ou outros meios fraudulentos análogos - a forma mais comum de crime digital no Brasil. Criada pela Lei 14.155/2021, a qualificadora do art. 171, § 2º-A, reconhece a maior gravidade do golpe praticado a distância e em escala.

COMO OCORRE NA PRÁTICA

Falsas lojas virtuais, boletos adulterados e anúncios falsos

Pena aumentada se o crime usa servidor fora do Brasil ou vítima idoso ou vulnerável

TIPIFICAÇÃO

**Art. 171, § 2º-A, do Código Penal
(Lei 14.155/2021)**

PENA

Reclusão de 4 a 8 anos e multa -
sanção superior à do estelionato
simples



Furto mediante fraude eletrônica

Ocorre quando a subtração de valores se dá por meio de dispositivo eletrônico ou informático, com ou sem violação de mecanismo de segurança, ou com uso de programa malicioso – caso típico das transferências bancárias não autorizadas. No furto, o criminoso subtrai os valores diretamente; no estelionato, a própria vítima, enganada, realiza o pagamento.

COMO OCORRE NA PRÁTICA

- Transferências feitas por invasores no app bancário
- Uso de malware para capturar senhas e esvaziar contas

TIPIFICAÇÃO

Art. 155, § 4º-B, do Código Penal
(Lei 14.155/2021)

PENA

Reclusão de 4 a 8 anos e multa, com aumentos se houver servidor no exterior ou vítima idosa

Phishing: a isca digital

Técnica em que o criminoso "pesca" dados da vítima por mensagens falsas que imitam bancos, lojas, órgãos públicos ou empresas conhecidas, levando-a a clicar em links maliciosos ou informar senhas e códigos. Não há tipo penal autônomo: conforme o resultado, configura estelionato qualificado, furto mediante fraude ou invasão de dispositivo.

COMO OCORRE NA PRÁTICA

- E-mails e SMS com links falsos
- ("smishing") Páginas clonadas de bancos e do gov.br

§

TIPIFICAÇÃO

Enquadramento conforme a conduta: arts. 171, § 2º-A; 155, § 4º-B; ou 154-A do CP

PENA

Até 8 anos de reclusão na modalidade de fraude eletrônica

Golpes envolvendo o Pix

A instantaneidade do Pix tornou-o o meio preferido dos estelionatários: o valor transferido é pulverizado em "contas-laranja" em minutos. O Banco Central instituiu o MED (Mecanismo Especial de Devolução), que permite o bloqueio cautelar de valores quando a fraude é comunicada rapidamente ao banco.

COMO OCORRE NA PRÁTICA

- Falso comprovante de pagamento e QR Code
- adulterado Golpe da "mão fantasma" com acesso remoto ao celular

§

TIPIFICAÇÃO

Em regra, art. 171, § 2º-A (fraude eletrônica) ou art. 155, § 4º-B do CP

PENA

Reclusão de 4 a 8 anos e multa;
comunicação imediata ao banco
pode viabilizar o MED

GOLPES EM DESTAQUE

Golpe do WhatsApp clonado e do perfil falso

No golpe da clonagem, o criminoso obtém o código de verificação da vítima e assume sua conta, pedindo dinheiro aos contatos. No golpe do perfil falso, usa a foto e o nome da vítima em um número novo, simulando "troca de chip". Além do estelionato contra os contatos, pode configurar invasão de dispositivo informático e uso indevido de imagem, com reflexos cíveis indenizatórios.

COMO OCORRE NA PRÁTICA

Pedidos urgentes de Pix a familiares e amigos

Prevenção: ativar a confirmação em duas etapas no aplicativo

TIPIFICAÇÃO

Art. 171, § 2º-A, e art. 154-A do CP, conforme a conduta

PENA

Reclusão de 4 a 8 anos e multa
na modalidade de fraude eletrônica

GOLPES EM DESTAQUE

Golpe da falsa central de atendimento

A vítima recebe ligação de suposto funcionário do banco informando uma transação suspeita. Em tom de urgência, o falso atendente induz a vítima a fornecer senhas, instalar aplicativos de acesso remoto ou "transferir o dinheiro para uma conta segura". Variante frequente é o golpe do falso motoboy, em que o cartão da vítima é retirado em casa sob o pretexto de perícia.

COMO OCORRE NA PRÁTICA

- Bancos nunca pedem senha, cartão ou transferência por telefone
- Desligue e retorne pelos canais oficiais do banco

TIPIFICAÇÃO

Art. 171, § 2º-A, do CP; eventual concurso com furto qualificado

PENA

Reclusão de 4 a 8 anos e multa, majorada se a vítima for idosa

GOLPES EM DESTAQUE

SIM swap: o sequestro da linha telefônica

O criminoso, com dados pessoais vazados e, por vezes, com auxílio de funcionário infiel da operadora, transfere a linha da vítima para outro chip. Com a linha em mãos, recebe os códigos SMS de verificação e assume contas bancárias, WhatsApp, e-mail e redes sociais – porta de entrada para fraudes em cadeia.

COMO OCORRE NA PRÁTICA

Sinal de alerta: celular subitamente sem sinal
Prefira autenticação por aplicativo em vez de SMS

TIPIFICAÇÃO

Arts. 154-A, 155, § 4º-B, e 171, § 2º-A, do CP, em concurso conforme o caso

PENA

Penas somadas podem superar 8 anos de reclusão, além da responsabilidade civil da operadora

GOLPES EM DESTAQUE

Ransomware: o sequestro de dados

Programa malicioso que criptografa os arquivos da vítima – pessoa física, empresa ou órgão público – e exige resgate, geralmente em criptomoedas, para devolver o acesso. No Brasil, a conduta é enquadrada como invasão de dispositivo informático qualificada e extorsão, podendo somar-se dano e interrupção de serviço quando atinge sistemas públicos.

COMO OCORRE NA PRÁTICA

Ataques a hospitais, tribunais e prefeituras
Backups íntegros e atualizações reduzem o impacto

TIPIFICAÇÃO

**Art. 154-A c/c art. 158 do CP
(extorsão); art. 266 quando interrompe serviço público**

PENA

Extorsão: reclusão de 4 a 10 anos
e multa, além das penas dos demais delitos

Crimes contra a honra na internet

Calúnia

Art. 138 do CP: imputar falsamente a alguém fato definido como crime. Pena: detenção de 6 meses a 2 anos e multa.

Difamação

Art. 139 do CP: imputar fato ofensivo à reputação. Pena: detenção de 3 meses a 1 ano e multa.

Injúria

Art. 140 do CP: ofender a dignidade ou o decoro. Injúria racial é crime equiparado ao racismo.

Atenção: a pena é triplicada se o crime for cometido via internet ou rede social (Art. 141, § 2º, do CP).

Perseguição (cyberstalking)

A Lei 14.132/2021 criou o crime de perseguição: perseguir alguém, reiteradamente e por qualquer meio – inclusive digital –, ameaçando sua integridade, restringindo sua locomoção ou invadindo sua liberdade e privacidade. Abrange monitoramento obsessivo em redes sociais, mensagens insistentes, criação de perfis falsos para vigiar a vítima e uso de rastreadores.

COMO OCORRE NA PRÁTICA

Pena aumentada contra mulher, criança, adolescente ou idoso. Cabem medidas protetivas de urgência (Lei Maria da Penha).

TIPIFICAÇÃO

Art. 147-A do Código Penal

PENA

Reclusão de 6 meses a 2 anos e multa, com aumento de metade nas hipóteses qualificadas

CRIMES EM ESPÉCIE

Bullying e cyberbullying

A Lei 14.811/2024 tipificou a intimidação sistemática (bullying): intimidar uma ou mais pessoas com violência física ou psicológica, de forma intencional e repetitiva, mediante humilhações ou discriminação. Quando praticada pela internet, redes sociais, aplicativos ou jogos on-line – o cyberbullying –, a conduta deixa de ser mera infração com pena de multa e passa a ser punida com reclusão.

COMO OCORRE NA PRÁTICA

Grupos de ataque, exposição vexatória e "tribunais virtuais" Escolas têm dever de prevenção e comunicação

TIPIFICAÇÃO

**Art. 146-A do Código Penal
(Lei
14.811/2024)**

PENA

Cyberbullying: reclusão de 2 a 4 anos e multa. Bullying presencial: multa

CRIMES EM ESPÉCIE

Violência psicológica contra a mulher e IA

O art. 147-B do CP pune quem causa dano emocional à mulher mediante ameaça, constrangimento, humilhação, vigilância constante ou qualquer meio que prejudique sua saúde psicológica e autodeterminação. A Lei 15.123/2025 agravou a pena quando o crime é cometido com uso de inteligência artificial ou outro recurso tecnológico que altere imagem ou som da vítima – resposta direta aos deepfakes.

COMO OCORRE NA PRÁTICA

Montagens e nudes falsos gerados por IA
Vigilância digital pelo parceiro ou ex-parceiro

TIPIFICAÇÃO

Art. 147-B do Código Penal
(Leis 14.188/2021 e 15.123/2025)

PENA

Reclusão de 6 meses a 2 anos, aumentada de metade se houver uso de IA ou tecnologia similar

CRIMES EM ESPÉCIE

Divulgação de cena íntima sem consentimento

A chamada "pornografia de vingança" (Revenge Porn) foi tipificada pela Lei 13.718/2018: divulgar, por qualquer meio, fotografia ou vídeo de cena de nudez, sexo ou pornografia sem o consentimento da vítima. A pena é aumentada quando o agente mantém ou manteve relação íntima com a vítima, ou age com fim de vingança ou humilhação. O Marco Civil garante a remoção do conteúdo mediante simples notificação à plataforma (art. 21).

COMO OCORRE NA PRÁTICA

Registro não autorizado da intimidade: art. 216-B do CP
Indenização por danos morais é cumulável

TIPIFICAÇÃO

Art. 218-C do Código

Penal

PENA

Reclusão de 1 a 5 anos, com aumento de 1/3 a 2/3 nas hipóteses qualificadas

Deepfakes e fraudes com inteligência artificial

Vídeos, áudios e imagens sintéticas hiper-realistas já são usados para clonar vozes de familiares em golpes, criar falsos endossos de celebridades em anúncios e produzir conteúdo íntimo falso. Além do agravamento do art. 147-B (Lei 15.123/2025), a manipulação de mídia, conforme o caso, configura estelionato, falsidade, crimes contra a honra ou crimes eleitorais – a Justiça Eleitoral já regulamentou o uso de IA em campanhas.

COMO OCORRE NA PRÁTICA

Golpe da "voz clonada" de parente pedindo dinheiro
Desconfie de urgência e confirme por outro canal

TIPIFICAÇÃO

Enquadramento múltiplo: arts. 147-B, 171, § 2º-A, 218-C do CP e legislação eleitoral

PENA

Varia conforme o tipo penal;
a
tendência legislativa é de agravamento específico

Crimes do ECA no ambiente digital

O Estatuto da Criança e do Adolescente contém um dos núcleos mais severos do direito penal informático brasileiro, voltado ao combate à exploração sexual infantil na rede:

1

Art. 241-A

Oferecer, divulgar ou transmitir registro ilícito envolvendo criança ou adolescente – reclusão de 3 a 6 anos e multa.

2

Art. 241-B

Adquirir, possuir ou armazenar esse material – reclusão de 1 a 4 anos e multa.

3

Art. 241-D

Aliciar ou assediar criança pela internet com fim libidinoso (grooming) – reclusão de 1 a 3 anos e multa.

Denúncias podem ser feitas anonimamente pelo Disque 100 e pela SaferNet.

ECA Digital - Lei 15.211/2025 ("Lei Felca")

Aprovada após ampla mobilização contra a "adultização" de crianças na internet, a lei impõe às plataformas digitais deveres de proteção: verificação de idade, vinculação de contas de menores aos pais, prevenção a conteúdos nocivos e remoção célere de material de exploração. Estabelece sanções administrativas severas às empresas descumpridoras e reforça a responsabilização pela exposição comercial indevida de crianças e adolescentes.

COMO OCORRE NA PRÁTICA

Plataformas devem adotar mecanismos eficazes de verificação etária. Multas podem alcançar percentual do faturamento no Brasil.

TIPIFICAÇÃO

Lei 15.211/2025, em diálogo

com o ECA e a LGPD

PENA

Sanções administrativas às plataformas; condutas individuais seguem os tipos do ECA e do CP

Marco Civil da Internet (Lei 12.965/2014)

IP

Registros de conexão

Provedores de conexão devem guardar logs por 1 ano (art. 13), permitindo identificar o IP utilizado.

LOG

Registros de aplicação

Plataformas devem guardar registros de acesso por 6 meses (art. 15), fornecidos mediante ordem judicial.

X

Remoção de conteúdo

Após o Tema 987/STF (2025), plataformas respondem por conteúdos ilícitos graves mesmo sem ordem judicial prévia em hipóteses definidas.

A identificação do autor parte da quebra de sigilo dos registros – por isso, preservar provas e URLs é essencial.

INSTRUMENTOS DE PROTEÇÃO

LGPD e o vazamento de dados pessoais

A Lei Geral de Proteção de Dados (Lei 13.709/2018) disciplina o tratamento de dados pessoais e impõe às empresas deveres de segurança. Vazamentos alimentam diretamente os golpes: com nome, CPF e telefone, o criminoso personaliza a abordagem e ganha credibilidade. A ANPD pode aplicar multas de até 2% do faturamento, limitadas a R\$ 50 milhões por infração, sem prejuízo da indenização às vítimas.

COMO OCORRE NA PRÁTICA

Vazamentos não geram crime autônomo na LGPD, mas viabilizam fraudes

Titular pode exigir informações e eliminação de dados

TIPIFICAÇÃO

Lei 13.709/2018; sanções administrativas pela ANPD e responsabilidade civil

PENA

Multas de até R\$ 50 milhões por infração, além de danos morais e materiais às vítimas

Outras condutas criminosas no meio digital

147

Ameaça

Por mensagem, e-mail ou rede social; pena de detenção de 1 a 6 meses ou multa.

307

Falsa identidade

Perfis falsos para obter vantagem ou causar dano a terceiros.

R

Racismo

Discriminação em redes sociais; crime inafiançável e imprescritível.

286

Incitação ao crime

Inclui o incentivo à automutilação e ao suicídio em comunidades virtuais.

\$

Lavagem de dinheiro

Uso de criptoativos e contas-laranja para ocultar produto dos golpes.

288

Associação criminosa

Quadrilhas estruturadas de fraude digital, com divisão de tarefas.

Quem investiga e quem julga?

i

Regra geral

Em regra, a competência é da Justiça Estadual e a investigação cabe às Polícias Civis, muitas delas com delegacias especializadas em crimes cibernéticos. A Justiça Federal atua quando há transnacionalidade prevista em tratado, lesão a bens e serviços da União ou crimes contra o sistema financeiro.

!

Jurisprudência em destaque

STJ: competência do local onde a vítima mantém a conta (furto eletrônico). Súmula 528/STJ e precedentes definem foros específicos. O Brasil aderiu à Convenção de Budapeste sobre o Crime Cibernético (Decreto 11.491/2023), facilitando a cooperação internacional.

Fui vítima: como denunciar?

- 1 Preserve as provas** Capture telas com data e URL, guarde conversas, e-mails, comprovantes e extratos. Considere ata notarial para conteúdo relevante.
- 2 Comunique o banco** Em fraudes financeiras, acione imediatamente a instituição e peça o bloqueio via MED (Pix) e a contestação das operações.
- 3 Registre a ocorrência** Boletim na delegacia especializada ou pela delegacia eletrônica do seu estado. Em crimes contra crianças, use o Disque 100 e a SaferNet.
- 4 Procure um advogado** Para remoção de conteúdo, indenização, medidas protetivas e acompanhamento da persecução penal.

ORIENTAÇÃO PRÁTICA

Dez medidas de proteção digital

01

Ative a verificação em duas etapas em todas as contas

02

Desconfie de urgência: golpista sempre tem pressa

03

Confirme pedidos de dinheiro por ligação ou pessoalmente

04

Evite redes Wi-Fi públicas para operações bancárias

05

Verifique URLs antes de clicar – atenção a domínios falsos

06

Use senhas longas, únicas e um gerenciador de senhas

07

Nunca informe senhas ou códigos recebidos por SMS

08

Mantenha sistema e antivírus sempre atualizados

09

Cadastre limites reduzidos para o Pix noturno

10

Faça backups periódicos de dados importantes

DIREITOS DA VÍTIMA

Responsabilidade civil de bancos e plataformas

A Súmula 479 do STJ afirma que as instituições financeiras respondem objetivamente pelos danos causados por fraudes e delitos praticados por terceiros em operações bancárias – o chamado fortuito interno. A jurisprudência, porém, afasta a responsabilidade quando a vítima entrega voluntariamente senhas e códigos por culpa exclusiva. Cada caso exige análise da falha de segurança: transações atípicas, em horários e valores destoantes do perfil do cliente, indicam dever de bloqueio.

COMO OCORRE NA PRÁTICA

Plataformas: dever de remoção e responsabilização conforme o Tema 987/STF

Vítima pode cumular restituição e danos morais

TIPIFICAÇÃO

Súmula 479/STJ; CDC; Marco

Civil da Internet

PENA

Restituição dos valores e indenização, conforme a falha do serviço

Informação é a primeira linha de defesa

O direito penal brasileiro evoluiu rapidamente para alcançar a criminalidade digital – da Lei Carolina Dieckmann ao ECA Digital. Mas nenhuma lei substitui a vigilância do usuário: desconfiar, verificar e denunciar continuam sendo as condutas mais eficazes.

Compartilhe esta cartilha e ajude a proteger quem você conhece.



juristas:  INSTITUTO
JURISTAS

MUITO OBRIGADO!

Wilson Roberto

 [@awfroberto](https://www.instagram.com/awfroberto)

www.juristas.com.br