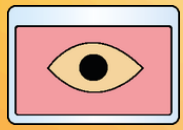
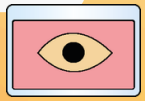
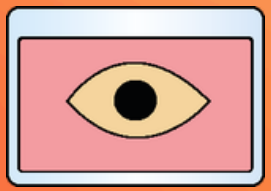


Violência Digital contra Mulheres

A violência que atravessa corpos, telas e algoritmos





Secretaria de Comunicação da Presidência da República | Ministério das Mulheres

LUIZ INÁCIO LULA DA SILVA
Presidente da República

GERALDO ALCKMIN
Vice-Presidente da República

MINISTÉRIO DAS MULHERES

MÁRCIA HELENA CARVALHO LOPES
Ministra de Estado das Mulheres

EUTÁLIA BARBOSA RODRIGUES
Secretária-Executiva

ESTELA BEZERRA DE SOUZA
Secretária Nacional de Enfrentamento à Violência contra Mulheres

CAROLINA MACHADO ROCHA BUSCH PEREIRA
Chefe de Gabinete

JANARA KALLINE LEAL LOPES DE SOUSA
Chefe da Assessoria Especial de Comunicação Social

SECRETARIA DE COMUNICAÇÃO DA PRESIDÊNCIA DA REPÚBLICA

SIDÔNIO CARDOSO PALMEIRA
Ministro de Estado

TIAGO CESAR DOS SANTOS
Secretário-Executivo

JOÃO BRANT
Secretário de Políticas Digitais

NINA SANTOS
Secretária Adjunta de Políticas Digitais

DAVID ALMANSA BERNARDO
Diretor do Departamento de Direitos na Rede e Educação Midiática

DÊNIS RODRIGUES DA SILVA
Coordenador-Geral de Proteção de Direitos na Rede

DANDARA MARIA BARBOSA SILVA
Coordenadora de Proteção de Direitos na Rede

FICHA TÉCNICA

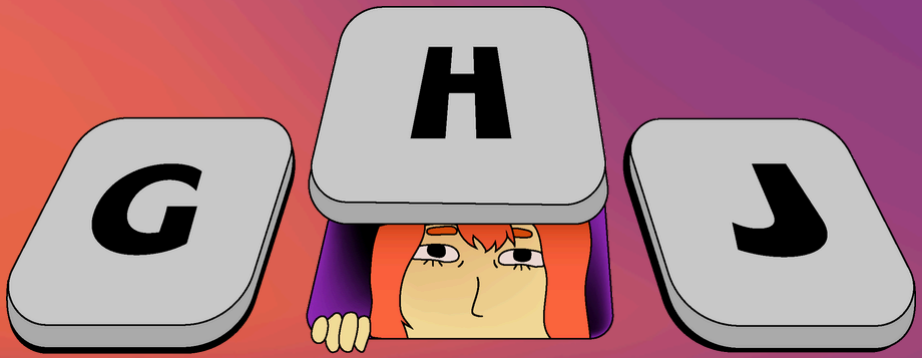
Texto
Almerinda Lopes Pinto Vasconcelos
Janara Kalline Leal Lopes de Sousa
Nina Santos

Revisão
Dandara Maria Barbosa Silva
David Almansa Bernardo
Dênis Rodrigues da Silva

Projeto Gráfico e diagramação
Giulia Blainner Souza Silva

10 de junho de 2026

SUMÁRIO



APRESENTAÇÃO

A cartilha **"Violência Digital contra Mulheres: a violência que atravessa corpos, telas e algoritmos"** foi elaborada como um instrumento de apoio pedagógico para profissionais, equipes e instituições que atuam na prevenção, na atenção e no acolhimento de mulheres vítimas de violência digital. Seu objetivo é oferecer uma linguagem clara, acessível e tecnicamente orientada para ajudar a reconhecer, nomear, registrar e encaminhar situações de violência que acontecem no ambiente online, mas produzem efeitos concretos na vida, na segurança, na saúde emocional, na reputação e na autonomia das mulheres.

A violência digital contra mulheres não é um fenômeno isolado, nem uma violência menor. Ela expressa, nas plataformas, aplicativos e redes sociais, desigualdades de gênero que já atravessam a vida social. No ambiente digital, essas violências ganham velocidade, escala e permanência, podendo envolver intimidação, exposição indevida, humilhação, controle, ameaça, perseguição, manipulação de imagens, divulgação de conteúdo íntimo, invasão de dispositivos, crimes contra a honra, doxxing, deepfakes e outras formas de agressão mediadas por tecnologia.

Ao longo do material, a cartilha apresenta conceitos, exemplos práticos e enquadramentos jurídicos que podem auxiliar o atendimento e fortalecer a atuação da rede. A proposta é contribuir para que cada caso seja escutado com atenção, registrado com precisão e compreendido em sua complexidade, considerando que uma mesma situação pode envolver diferentes formas de violência e mais de um crime. Também são abordadas orientações sobre provas digitais, preservação de registros, responsabilidade das plataformas e caminhos para a proteção das vítimas.

Nomear corretamente a violência digital é parte fundamental do enfrentamento à impunidade e da garantia de direitos. Por isso, esta cartilha se coloca como uma ferramenta de formação, apoio e fortalecimento da rede de atenção e acolhimento, reafirmando que proteger mulheres no ambiente digital exige informação qualificada, escuta sensível, atuação articulada e compromisso permanente com uma internet mais segura para todas.

O que é Violência Digital contra Mulheres?

> Violência digital é toda forma de intimidação, exposição indevida, agressão, ameaça ou humilhação feita em ambiente digital. É uma extensão do machismo cotidiano, com maior alcance e rapidez.

ESTRUTURAL

Não é um evento isolado, mas uma matriz histórica orientada por pressupostos patriarcais, operando como um instrumento de dominação e controle direcionado à mulher.

PLURAL

Abrange violências sexuais, psicológicas, patrimoniais e morais. O mesmo ato pode configurar múltiplos crimes simultaneamente.

SEM FRONTEIRAS

A tecnologia elimina as barreiras de espaço e tempo, permitindo que a violência invada a vida da vítima a qualquer tempo e lugar. A rápida propagação em larga escala e a dificuldade de apagar conteúdo prolongam a exposição da mulher.

Classificação essencial para entender os crimes digitais

CRIME DIGITAL PRÓPRIO

O meio digital é ELEMENTO DO TIPO — sem internet, o crime não existe.

- Invasão de dispositivo informático (art. 154-A CP).
- Divulgação não consensual de conteúdo íntimo (art. 218-C CP).
- Fraude eletrônica (art. 171, §2º-A CP).
- Cyberbullying (art. 146-A, par. único CP).
- Induzimento ao suicídio digital (art. 122, §4º CP).

CRIME DIGITAL IMPRÓPRIO

O crime existe fora do digital, mas é POTENCIALIZADO pela tecnologia.

- Ameaça praticada por WhatsApp (art. 147 CP).
- Registro não autorizado de intimidade (art. 216-B CP).
- Perseguição / Stalking digital (art. 147-A CP).
- Crimes contra a honra em redes sociais (arts. 138-140 CP).
- Violência psicológica digital (art. 147-B CP).

A distinção importa para o registro no relato: crimes impróprios exigem que a atendente capture o MODO digital de execução para viabilizar o enquadramento correto.

Blocos Temáticos e Tipos Criminais:

BLOCO I - CRIMES SEXUAIS E CONTRA A INTIMIDADE NO AMBIENTE DIGITAL

- Registro Não Autorizado de Intimidade Sexual;
- Disseminação não Consentida de Imagens Íntimas;
- Sextorsão;
- Estupro Virtual;
- Importunação Sexual.

BLOCO II - CONTROLE COERCITIVO, PERSEGUIÇÃO E VIGILÂNCIA DIGITAL

- Ameaça;
- Invasão de Dispositivo Informático;
- Perseguição Digital e Software de Vigilância Abusiva;
- Violência Psicológica: Deepfake e IA.

BLOCO III - CYBERBULLYING E ASSÉDIO EM AMBIENTES DIGITAIS

- Intimidação Sistemática Virtual (Cyberbullying);
- Assédio em Jogos / Streaming.

BLOCO IV - CRIMES CONTRA A HONRA

- Calúnia;
- Difamação;
- Injúria.

BLOCO V - CRIMES CONTRA A PRIVACIDADE, DADOS E IDENTIDADE

- Perfil falso (falsa identidade digital);
- Doxxing (exposição de dados pessoais.

BLOCO VI - VIOLÊNCIA POLÍTICA NO AMBIENTE DIGITAL

- Violência Política.

BLOCO VII - CRIMES PATRIMONIAIS

- Extorsão Digital;
- Estelionato Digital.

BLOCO VIII - INDUZIMENTO AO SUICÍDIO

- Induzimento / instigação / auxílio ao suicídio ou automutilação.

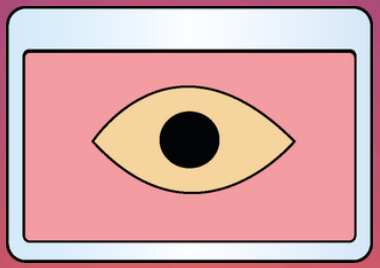
BLOCO IX - OUTRO TIPO PENAL RELEVANTE

- Descumprimento de medida protetiva por meios digitais.

BLOCO X - PROVAS DIGITAIS E CAMINHOS DE PROTEÇÃO

- Provas Digitais;
- Decreto nº 12.976/2026 — Proteção de Mulheres na Internet;
- Medidas Protetivas de Urgência.

BLOCO I



CRIMES SEXUAIS E CONTRA A INTIMIDADE NO AMBIENTE DIGITAL

Registro Não Autorizado de Intimidade Sexual

Art. 216-B Código Penal (CP) · Lei nº 13.772/2018 · Pena: 6 meses a 1 ano + multa

O QUE É?

Produzir, fotografar, filmar ou registrar conteúdo íntimo (nudez/ato de natureza sexual) sem autorização.
Par. único: montagem/deepfake também configura o crime.

NO COTIDIANO DIGITAL

· Câmera oculta em banheiro ou hotel
· Gravação de relação íntima sem consentimento
· Upskirting (câmera por baixo da roupa)
· Montagem com IA/deepfake.

PONTO-CHAVE

Não exige divulgação. O registro em si já é crime. A ausência de consentimento é o elemento central do tipo.

Disseminação não Consentida de Imagens Íntimas

Art. 218-C CP · Lei nº 13.718/2018 · Pena: 4 a 10 anos + multa

O QUE É?

Oferecer, trocar, disponibilizar, transmitir, vender, publicar ou divulgar cena de sexo, nudez ou pornografia sem consentimento.
Abrange também cenas de estupro.

CAUSA DE AUMENTO DE PENA

Pena aumentada de 1/3 a 2/3 quando há relação íntima de afeto com a vítima ou a divulgação tem finalidade de vingança ou humilhação.

Sextorsão — Extorsão Sexual Digital

Art. 158 CP (Extorsão) · Pena: 4 a 10 anos + multa

Não existe tipo penal autônomo de 'sextorsão' no Brasil. Nesses casos, a conduta costuma ser enquadrada, principalmente, no crime de extorsão (art. 158 do Código Penal) e, conforme o caso, a outros tipos.

NÚCLEO DA CONDUTA

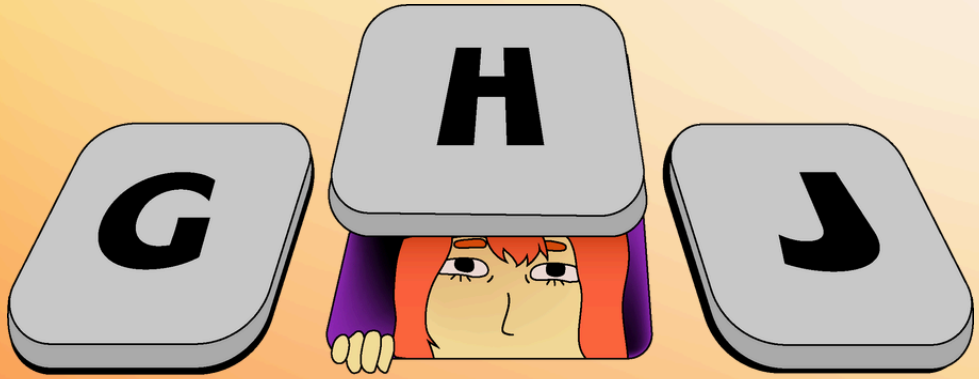
Constranger a vítima mediante grave ameaça — especificamente a ameaça de divulgação de conteúdo íntimo — com o fim de obter vantagem indevida.

COMO ACONTECE

· Ameaça via WhatsApp exigindo PIX
· Chantagem por perfil falso
· Deepfake criado para forçar envio de novos conteúdos
· Vazamento progressivo para coagir.

IMPORTANTE!

Consuma-se com o CONSTRANGIMENTO, independentemente de o agente obter a vantagem exigida (Súmula 96/STJ). Não precisa pagar para ser vítima.



QUANDO A VIOLÊNCIA ENVOLVE MAIS DE UM CRIME

Invasão ou espionagem digital

Invadir celular ou computador, ou usar câmera/aplicativo espião para captar dados, mensagens ou imagens.

Conteúdo íntimo sem autorização

Registrar, montar ou guardar imagem, vídeo ou áudio íntimo da vítima sem consentimento.

Ameaça, chantagem ou extorsão

Usar imagens, mensagens ou dados da vítima para ameaçar, constranger ou exigir vantagem.

Estupro Virtual

Art. 213 CP · Pena: 6 a 10 anos

O contato físico NÃO é requisito. O crime configura-se quando há CONSTRANGIMENTO mediante grave ameaça à prática de ato sexual, mesmo que tudo ocorra por tela.

CENÁRIO TÍPICO

Agente ameaça divulgar imagens íntimas se a vítima não se masturbar em videochamada, enviar novas fotos ou realizar atos libidinosos online.

ELEMENTO-CHAVE

Grave ameaça — a coação deve ser capaz de suprimir a autodeterminação sexual da vítima. Pode ser psicológica, moral ou dirigida a terceiros.

NÃO CONFUNDA

Mero reenvio de imagem ou vídeo íntimo já existente não é estupro. Para haver estupro virtual, a vítima deve ser obrigada, por grave ameaça, a praticar novo ato sexual ou libidinoso online.

QUANDO A VANTAGEM EXIGIDA MUDA O ENQUADRAMENTO:

Vantagem exigida for DINHEIRO / PIX

→ Ameaçar divulgar imagens ou dados da vítima para conseguir dinheiro pode configurar **extorsão**.

Vantagem exigida for ATO SEXUAL (fotos, vídeos)

→ Obrigar a vítima, por ameaça ou chantagem, a se expor, enviar conteúdo íntimo ou praticar ato sexual pode configurar **estupro**.

Importunação Sexual no Ambiente Digital

Art. 215-A CP · Lei nº 13.718/2018 · Pena: 1 a 5 anos
Crime subsidiário (quando a conduta não constituir crime mais grave)

O QUE É?

Praticar ato libidinoso contra alguém, sem anuência, com objetivo de satisfazer o próprio desejo sexual ou de outra pessoa. No ambiente digital, isso pode acontecer por mensagem, foto, vídeo ou chamada. O digital é apenas o meio usado para praticar a conduta.

EXEMPLOS DIGITAIS

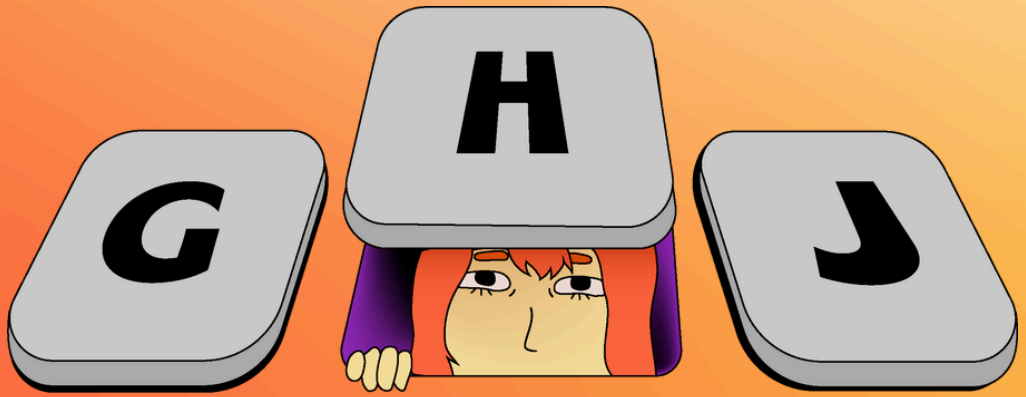
· Envio não solicitado de fotos ou vídeos de genitália
· Envio insistente e reiterado de conteúdo pornográfico ou sexual
· Videochamada com masturbação sem consentimento da vítima
· Inserção da vítima em live sexual de contéudo sexual.

ATENÇÃO!

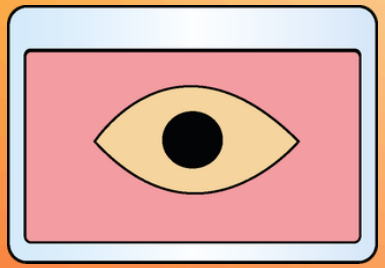
Ocorre sem violência ou grave ameaça. O ponto central é a falta de consentimento da vítima. Ter conversado antes, ter relação anterior ou já ter recebido outro conteúdo não autoriza novas abordagens sexuais.

COMO DISTINGUIR DOS CRIMES RELACIONADOS:

Importunação Sexual (215-A)	→	Não há ameaça/violência. Ato libidinoso não consentido.
Estupro (213 CP)	→	Há violência ou grave ameaça que suprime a vontade da vítima.
Divulgação (218-C CP)	→	Exposição de material preexistente, não ato libidinoso direto.



BLOCO II



CONTROLE COERCITIVO, PERSEGUIÇÃO E VIGILÂNCIA DIGITAL

Ameaça — Modalidade Digital

Art. 147 CP · Lei nº 14.994/2024 (pena em dobro contra mulher por razões de gênero)

O QUE É?

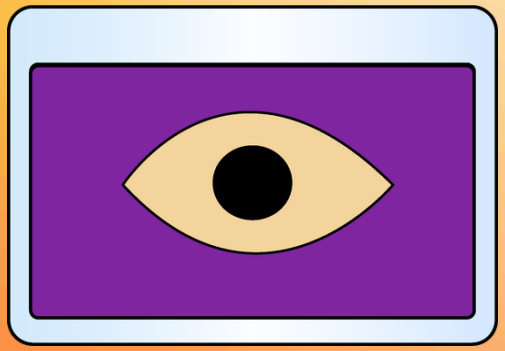
Ameaçar alguém de causar mal injusto e grave. Pode ocorrer por WhatsApp, e-mail, mensagens privadas (Direct Message), redes sociais, áudios, vídeos ou qualquer outro meio digital.

MUDANÇA IMPORTANTE

Lei nº 14.994/2024: quando praticado contra mulher por razões da condição do sexo feminino, a pena é aplicada em DOBRO e a ação penal passa a ser PÚBLICA INCONDICIONADA.

ATENÇÃO AO RELATO

No registro da ocorrência, é importante informar se a ameaça ocorreu em contexto de violência doméstica, familiar, íntima ou por desprezo/discriminação à condição de mulher.



DISTINÇÃO CRÍTICA PARA O ATENDIMENTO:

Ameaça genérica (sem recorte de gênero)
Ação penal CONDICIONADA à representação

→ Prazo para representação: 6 meses a partir do conhecimento da autoria.

Ameaça contra mulher por razões da condição do sexo feminino
Ação penal PÚBLICA INCONDICIONADA

→ Não depende de representação da vítima; o Ministério Público pode atuar independentemente da vontade da vítima.

Invasão de Dispositivo Informático

Art. 154-A CP · Lei nº 12.737/2012 (Lei Carolina Dieckmann), aprimorada pela Lei nº 14.155/2021 · Pena: Reclusão de 1 a 4 anos e multa.

O QUE É?

Invadir dispositivo informático alheio (celular, e-mail, redes sociais), conectado ou não à rede de computadores, com fim de obter, adulterar ou destruir dados, sem a autorização da usuária.

SITUAÇÃO MAIS GRAVE

Reclusão de 2 (dois) a 5 (cinco) anos, e multa, quando resultar obtenção de comunicações privadas, segredos ou controle remoto não autorizado.

PODE GERAR OUTROS CRIMES

Frequentemente é o ponto de entrada para outros crimes: divulgação de conteúdo íntimo, sextorsão, doxxing, perseguição. Os crimes concorrem materialmente. Procede-se mediante de representação.

COMO ESSE CRIME APARECE NAS LIGAÇÕES:

- Parceiro que acessou o WhatsApp da vítima sem permissão para ler mensagens
- Ex-companheiro faz clonagem de conta para monitorar conversas
- Instalação de aplicativo espião (stalkerware) no celular da vítima
- Acesso a e-mail ou rede social mediante descoberta/roubo de senha

Perseguição Digital + Software de Vigilância Abusiva

Art. 147-A CP (Perseguição) · Art. 154-A CP (Stalkerware) · Dois crimes que frequentemente coexistem

CYBERSTALKING — ART. 147-A

- Requer insistência ou repetição: mensagens, ligações, monitoramento constante da vítima em redes sociais, criação de perfis falsos, rastreamento de localização ou tentativas constantes de contato.
- É importante registrar se a conduta aconteceu mais de uma vez.
- Pena: reclusão de 6 meses a 2 anos, e multa (aumentada de metade se vítima for mulher).

SOFTWARE ESPIÃO / STALKERWARE — ART. 154-A

- Invadir celular, conta, e-mail ou computador da vítima.
- Instalar aplicativo espião ou acessar dados sem autorização.
- Pode permitir acesso indevido a mensagens, localização, fotos, senhas, câmera, microfone e controle remoto do aparelho.
- Pena: reclusão de 1 a 4 anos e multa.

Violência Psicológica — Deepfake e IA

Art. 147-B do Código Penal · Lei nº 14.188/2021 · Pena: 6 meses a 2 anos e multa.

QUANDO AUMENTA A PENA?

A pena aumenta de metade quando a violência psicológica contra a mulher é praticada com uso de inteligência artificial, deepfake ou outro recurso tecnológico que altere imagem ou som da vítima.

O QUE INCLUI?

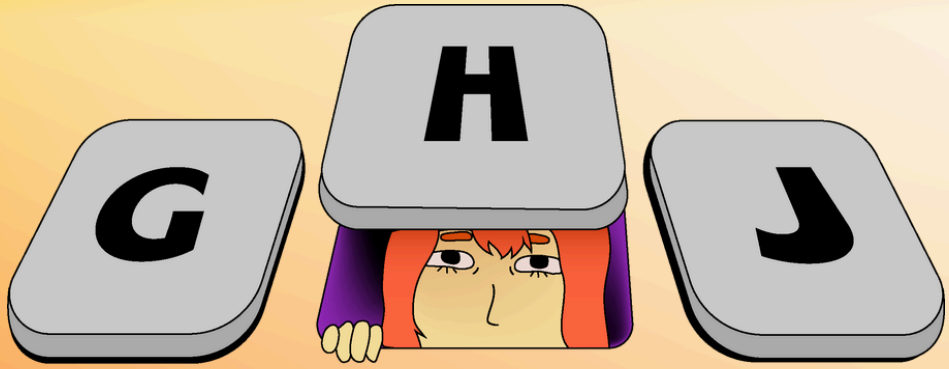
· Deepfakes;
· Clonagem de voz ;
· Manipulação de fotos, vídeos ou áudios;
· Perfis sintéticos com imagem gerada por IA;
· Qualquer tecnologia que altere imagem ou som.

O QUE NÃO INCLUI?

Texto ofensivo gerado por IA, sem alteração de imagem ou som da vítima. A conduta pode configurar outro crime, mas não essa causa de aumento específica.

EFEITO PRÁTICO

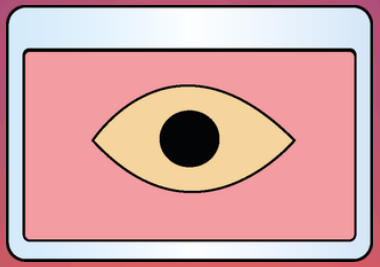
A pena de 6 meses a 2 anos tem a pena aumentada da metade quando há uso de IA/deepfake, passando para até 3 anos.



EXEMPLOS DE MODALIDADES EXECUTIVAS DIGITAIS (NÚCLEO: CAUSAR DANO EMOCIONAL À MULHER):

Deepfake pornográfico	Imagem da vítima em vídeo sexual falso gerado por IA. Envio a colegas de trabalho. Abalo psicológico + afastamento.
Montagem degradante	Ex-companheiro insere foto da vítima em montagem humilhante e publica no grupo de WhatsApp da família ou do trabalho dela.
Clonagem de voz	App de clonagem de voz para criar áudio no qual a vítima aparentemente confessa conduta desonrosa e envia a familiares.

BLOCO III



CYBERBULLYING E ASSÉDIO EM AMBIENTES DIGITAIS

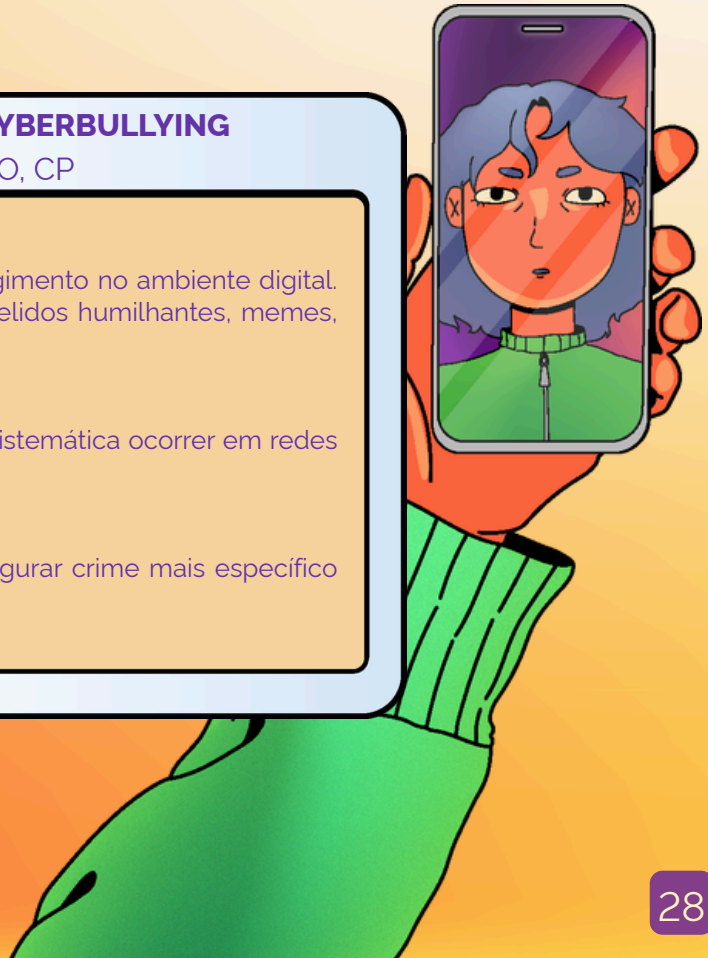
INTIMIDAÇÃO SISTEMÁTICA VIRTUAL · CYBERBULLYING

ART. 146-A, PARÁGRAFO ÚNICO, CP

O QUE É?
Conduta reiterada de humilhação, exposição ou constrangimento no ambiente digital. Campanha de ataques, reenvio de conteúdo ofensivo, apelidos humilhantes, memes, montagens ou perseguição online.

PENA
Pena de RECLUSÃO de 2 a 4 anos quando a intimidação sistemática ocorrer em redes sociais, aplicativos, jogos online ou transmissões ao vivo.

ATENÇÃO
O cyberbullying só se aplica quando a conduta não configurar crime mais específico ou mais grave, como injúria racial.



Assédio em Plataformas Digitais + Intimidação Sistemática Virtual

Art. 146-A, par. único CP (cyberbullying) · Crimes contra a honra como enquadramento subsidiário em jogos/streaming

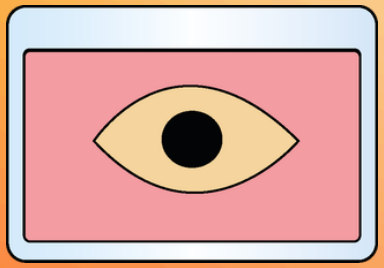
ASSÉDIO EM JOGOS / STREAMING

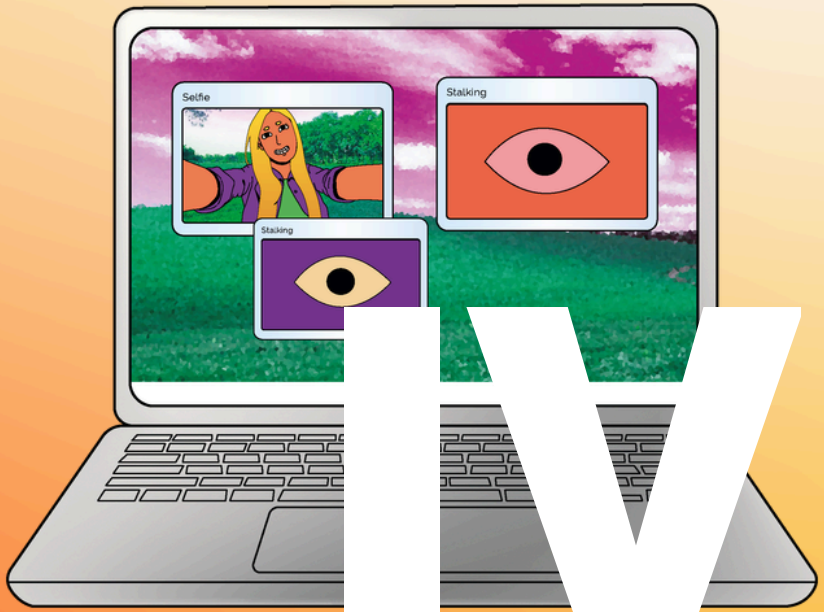
TIPO PENAL
O enquadramento depende do conteúdo (honra, ameaça, cyberbullying). Exige vítima determinada ou determinável.

EXEMPLOS CONCRETOS
Insultos reiterados contra jogadora em partidas online · Flood de mensagens no chat · Exclusão sistemática de grupo · Ataques em lives (Twitch, YouTube)

QUANDO VIRA CRIME?
Quando há vítima identificável e direcionamento da conduta.

BLOCO IV





IV

CRIMES CONTRA A HONRA

Crimes Contra a Honra no Ambiente Digital

DIFAMAÇÃO
Art. 139 CP

Pena base: 3 meses a 1 ano + multa

Atribuir à vítima fato ofensivo à sua reputação, ainda que esse fato não seja crime.

Ex: "Ela foi promovida porque se relacionou com o chefe."

CALÚNIA
Art. 138 CP

Pena base: 6 meses a 2 anos + multa

Imputar FALSAMENTE fato definido como CRIME. A imputação falsa é elemento essencial.

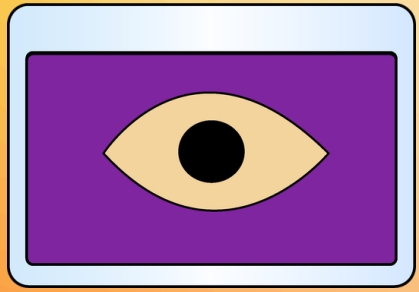
Ex: 'Ela praticou tráfico de drogas' (falso).

INJÚRIA
Art. 140 CP

Pena base: 1 a 6 meses ou multa

Ofender a dignidade ou decoro da vítima. Não imputa fato — é xingamento, humilhação direta.

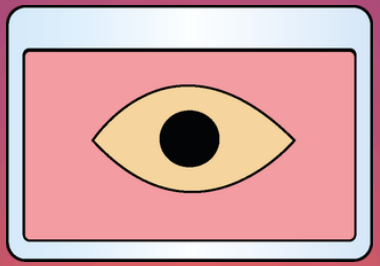
Ex: 'Sua vadia, sua burra' — mensagem direta.

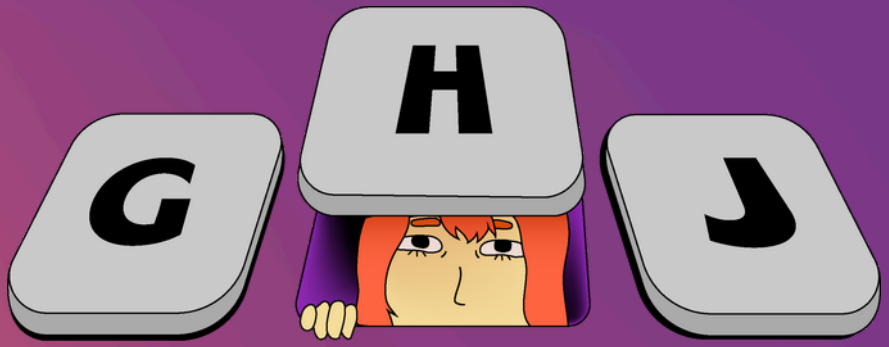


POR QUE O RELATO DIGITAL IMPORTA? — ART. 141 CP: CAUSAS DE AUMENTO DE PENA

SITUAÇÃO	AUMENTO
Qualquer meio que facilite a divulgação (ex: e-mail, app)	+ 1/3
Praticado em REDES SOCIAIS (qualquer modalidade)	x 3 (triplo)
Contra a mulher por razões da condição do sexo feminino	x 2 (dobro)
INJÚRIA RACIAL (raça, cor, etnia, origem — art. 2º-A, Lei 7.716)	2 a 5 anos reclusão

BLOCO V





V

CRIMES CONTRA A PRIVACIDADE, DADOS E IDENTIDADE

PERFIL FALSO

Art. 307 CP · Pena: 3 meses a 1 anos, ou multa, se o fato não constitui elemento de crime mais grave.

Criar ou usar identidade falsa no ambiente digital para obter vantagem ou causar dano à vítima.
Pode envolver ofensas, golpes, perseguição, exposição íntima, ameaça, difamação ou sextorsão.

**Imagem gerada por IA, meramente ilustrativa*

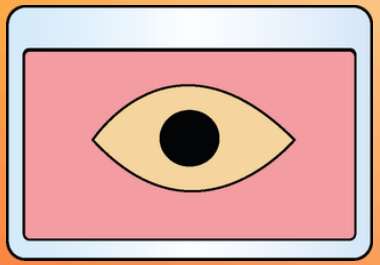
DOXXING

Exposição de dados pessoais da vítima, como endereço, telefone, CPF, local de trabalho ou rotina, para intimidar, constranger ou facilitar ataques.

Pode configurar: ameaça, perseguição, crimes contra a honra ou responsabilização civil pela LGPD.

**Imagem gerada por IA, meramente ilustrativa*

BLOCO VI



VIOLÊNCIA POLÍTICA NO AMBIENTE DIGITAL

Violência Política no Ambiente Digital

Art. 326-B do Código Eleitoral

Quem pode ser vítima?
Candidatas, detentoras de mandato eletivo ou mulheres que atuem na vida política.

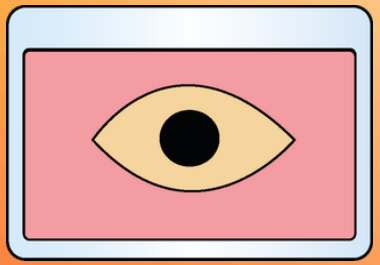
O que caracteriza?
Assediar, constranger, humilhar, perseguir ou ameaçar, por qualquer meio, com menosprezo ou discriminação à condição de mulher, cor, raça ou etnia.

Finalidade exigida
Impedir ou dificultar campanha eleitoral, mandato ou atuação política da mulher.

Exemplos digitais
Deepfake sexualizado para desacreditar candidata · Desinformação coordenada · Ameaças para forçar desistência de candidatura ou silenciar atuação política.

Pena: 1 a 4 anos + multa
A pena aumenta em 1/3 se o crime for cometido contra mulher gestante, maior de 60 anos ou com deficiência.

BLOCO VII



CRIMES PATRIMONIAIS

EXTORSÃO DIGITAL — Art. 158 CP

Sem elemento sexual
Na extorsão digital, a coação normalmente envolve ameaça relacionada a dinheiro, dados, reputação, segredos ou acesso indevido a contas.
Consuma-se com o constrangimento: a vítima não precisa realizar o pagamento.

Exemplos comuns
PIX sob ameaça de revelar segredo · Chantagem via e-mail ('hacker fake') · Extorsão em massa com ameaça padronizada.

Pena: 4 a 10 anos + multa
A pena aumenta de 1/3 até metade quando a extorsão é cometida por duas ou mais pessoas.

EXTORSÃO vs SEXTORSÃO:

Extorsão digital = ameaça envolvendo dinheiro, reputação, segredos, dados ou invasão de contas.

Sextorsão = ameaça de divulgação de conteúdo íntimo ou sexual.

Fraude Eletrônica — Estelionato praticado por meio digital

Art. 171, §2º-A CP · Pena: 4 a 8 anos + multa

O QUE CARACTERIZA?

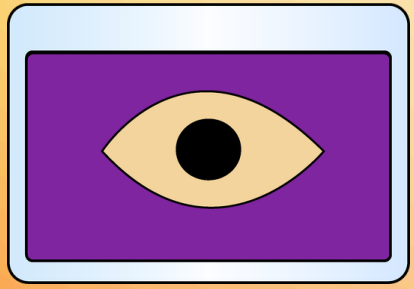
Fraude cometida com uso de informações fornecidas pela vítima ou por terceiro induzido a erro.
Abrange rmensagens falsas, ligações, perfis falsos, e-mails fraudulentos, aplicativos, sites clonados, contas invadidas ou dispositivos duplicados.

ROMANCE SCAM

Golpista cria identidade falsa e simula vínculo afetivo para obter vantagem econômica.
Pode envolver falsas promessas amorosas, pedidos urgentes de dinheiro, viagens, doenças ou supostas emergências.

EXIGE PREJUÍZO

A fraude eletrônica exige prejuízo patrimonial ou obtenção de vantagem econômica ilícita.
A tentativa ocorre quando a fraude é iniciada, mas não gera a transferência ou a obtenção da vantagem econômica.

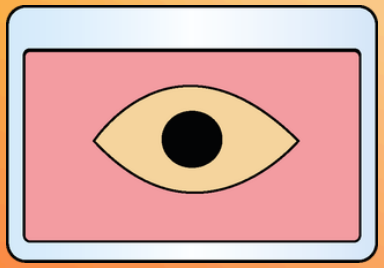


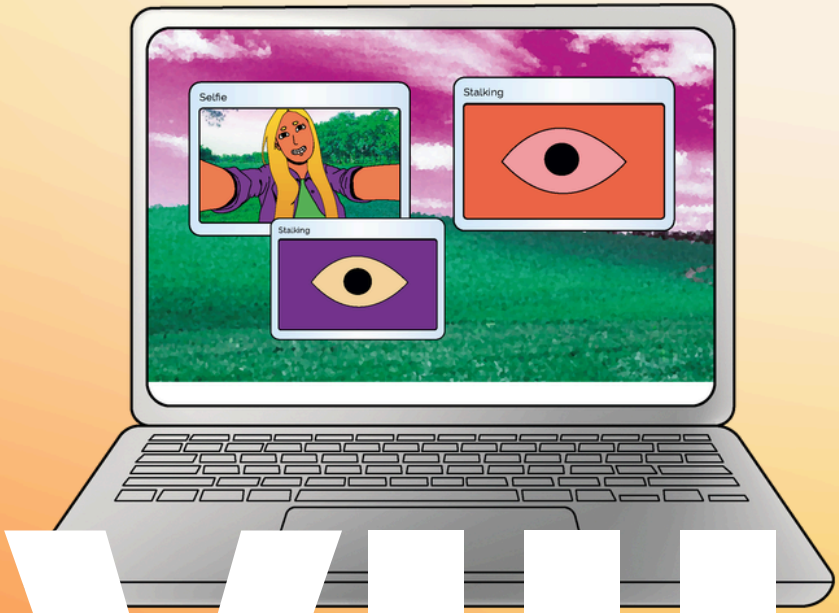
COMO DISTINGUIR FRAUDE DE EXTORSÃO:

	FRAUDE DIGITAL (171 CP)	EXTORSÃO DIGITAL (158 CP)
Mecanismo	Engano — a vítima age por erro	Coação — a vítima age por medo
Prejuízo	Necessário	Dispensável
Elemento central	Indução em erro	Grave ameaça

Atenção: se a vítima fez o PIX porque foi enganada, o caso pode ser fraude. Se fez porque foi ameaçada, pode ser extorsão. Mas, se o autor invadiu ou acessou a conta e retirou o valor sem que a vítima entregasse voluntariamente o dinheiro, o enquadramento pode ser furto mediante fraude ou furto eletrônico (art. 155, §4º-B, CP · pena: 4 a 8 anos e multa).

BLOCO VIII





VIII

INDUZIMENTO AO SUICÍDIO

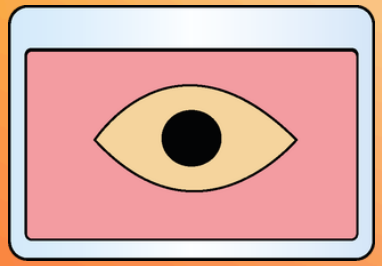
Induzimento ao Suicídio/Automutilação em Ambiente Digital

Art. 122 CP · Lei nº 13.968/2019

Estrutura escalonada de penas — o resultado e o contexto definem a gravidade:	
Incentivar, instigar ou ajudar suicídio ou automutilação	Reclusão 6 meses a 2 anos
Lesão grave ou gravíssima resultante	Reclusão 1 a 3 anos
Resultado morte	Reclusão 2 a 6 anos
Vítima vulnerável ou motivo cruel, banal ou injustificável	Pena em DOBRO
Se ocorrer por rede social, internet ou transmissão em tempo real	Aumento até o DOBRO
Se o autor for líder, coordenador ou administrador de grupo virtual	Pena em DOBRO

Em desafios online, grupos virtuais ou transmissões ao vivo, o meio digital pode ampliar o alcance da conduta, facilitar a instigação coletiva e agravar a responsabilização, especialmente quando houver líderes ou administradores envolvidos.

BLOCO IX



OUTRO TIPO PENAL RELEVANTE

IX

Descumprimento de Medida Protetiva no Ambiente Digital

Art. 24-A LMP · Art. 338-A CP (Lei nº 15.280/2025) · Reclusão 2 a 5 anos + multa

VALE TAMBÉM NO DIGITAL

Se a medida protetiva proíbe contato por qualquer meio, o agressor não pode procurar a vítima por mensagens, ligações, redes sociais, e-mail, perfis falsos ou por terceiros.

DESCUMPRIMENTO

WhatsApp de número diferente · Perfil falso para contato · Comentários em redes sociais da vítima · Monitoramento por apps · Contato via interposta pessoa.

PENA

Descumprir medida protetiva pode gerar reclusão de 2 a 5 anos e multa. A pena aumenta de 1/3 até metade se houver violação ou remoção de tornozeleira eletrônica.

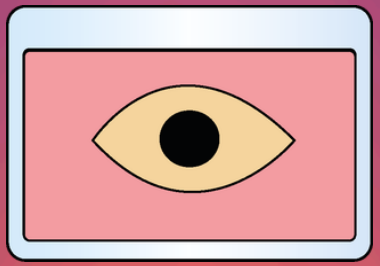
QUANDO O DESCUMPRIMENTO DA MEDIDA PROTETIVA ENVOLVE OUTROS CRIMES:

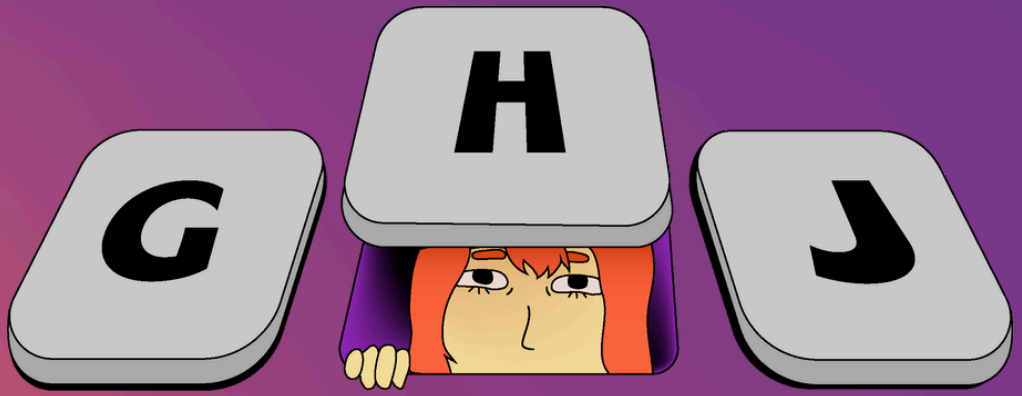
Descumprimento + Art. 147 CP (ameaça) — quando a pessoa proibida de se aproximar ou fazer contato descumpre a medida protetiva e ainda ameaça a vítima.

Descumprimento + Art. 147-A CP (perseguição) — quando a pessoa insiste em procurar, vigiar, mandar mensagens, ligar ou aparecer nos locais frequentados pela vítima.

Repetição do descumprimento — quando o descumprimento acontece mais de uma vez, isso deve ser registrado com clareza, pois pode reforçar a necessidade de prisão preventiva para proteger a vítima.

BLOCO X





X

PROVAS DIGITAIS E CAMINHOS DE PROTEÇÃO

O QUE É PROVA DIGITAL E COMO ELA DEVE SER COLETADA?

Prova digital: toda informação gerada, armazenada ou transmitida por meio eletrônico que possa demonstrar fato relevante ao processo penal.

Prints e capturas

URL, data e hora visíveis. Preserve antes de denunciar, porque a plataforma pode remover o conteúdo rapidamente.

Metadados

Informações do arquivo: data de criação, localização e origem do dispositivo.

Código hash SHA-256

Funciona como uma 'impressão digital' do arquivo e ajuda a demonstrar que ele não foi alterado.

Ata notarial

Art. 384 CPC: o cartório certifica o conteúdo digital (tela, URL, data e hora). Válido como prova documental em processo.

Dados em plataformas

IP, data de acesso, dados cadastrais e registros de uso podem ajudar a identificar o autor e devem ser preservados rapidamente.

Perícia técnica

Análise do dispositivo, validação de autenticidade, identificação de edições e recuperação de dados apagados.

A violência digital também gera deveres para as plataformas

Decreto nº 12.976/2026 — Proteção de Mulheres na Internet

O Decreto nº 12.976/2026 estabelece diretrizes para prevenção e enfrentamento da violência digital contra mulheres. ntre os deveres das plataformas digitais estão: canais acessíveis de denúncia, preservação de provas digitais, remoção rápida de conteúdos ilícitos e medidas contra ataques coordenados.

Objetivo:
Fortalecer a proteção de mulheres no ambiente digital e impedir o uso da tecnologia como instrumento de violência, intimidação ou perseguição.

OS 5 DEVERES DAS PLATAFORMAS DIGITAIS

Prevenção

Adotar medidas para impedir ou reduzir a circulação de conteúdos ilícitos.

Bloqueio de IA

Impedir a geração de conteúdo íntimo sintético de mulheres e meninas.

Canais de Denúncia

Disponibilizar canal gratuito, permanente e acessível para denúncias.

Redução de Alcance

Reduzir alcance, visibilidade e impulsionamento em ataques coordenados.

Apoio e Orientação

Divulgar o Ligue 180 como canal de apoio, acolhimento e denúncia.

A REGRA DE OURO: PRESERVAR A PROVA ANTES DA REMOÇÃO

Antes de remover conteúdo ilícito, a plataforma deve preservar os registros necessários para investigação e responsabilização do agressor.

1 - DENÚNCIA:

Denúncia realizada em canal oficial.

2 - PRESERVAÇÃO:

Preservação de links, perfis, horários, metadados e registros técnicos.

3 - ANÁLISE:

Análise conforme o prazo legal aplicável.

4 - REMOÇÃO:

Conteúdo removido e bloqueado para evitar recirculação.

A remoção sem preservação adequada pode **dificultar a investigação e a responsabilização do agressor.**

PRAZOS DE RESPOSTA DAS PLATAFORMAS DIGITAIS

Condutas relacionadas:
• divulgação não autorizada de conteúdo íntimo;
• registro íntimo sem consentimento;
• exposição sexual digital;
• deepfake íntimo;
• manipulação íntima por inteligência artificial;
• circulação de material sexualizante envolvendo mulheres e meninas.

2 HORAS
REMOÇÃO RÁPIDA DE EXPOSIÇÃO ÍNTIMA NÃO AUTORIZADA

OBRIGAÇÃO DA PLATAFORMA

Remover ou indisponibilizar o conteúdo em até **2 horas** após notificação.

ALÉM DA REMOÇÃO

- Preservar provas digitais
- Bloquear recirculação automática
- Permitir acompanhamento da denúncia.

PRAZOS DE RESPOSTA DAS PLATAFORMAS DIGITAIS

Crimes e violências relacionadas:

- Ameaças contra mulheres;
- Perseguição digital;
- Violência psicológica;
- Intimidação sistemática;
- Violência política contra a mulher;
- Conteúdos que propaguem ódio ou aversão às mulheres;
- Crimes contra a honra, como calúnia, difamação ou injúria, quando praticados contra a mulher em razão da condição do sexo feminino.

6 HORAS
ILEGALIDADE MANIFESTA

OBRIGAÇÃO DA PLATAFORMA

Remover ou indisponibilizar rapidamente conteúdos manifestamente ilícitos após denúncia.

ALÉM DA REMOÇÃO

- reduzir circulação do ataque;
- impedir amplificação coordenada;
- limitar alcance e impulsionamento.

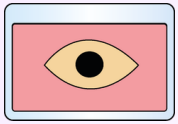
PRAZOS DE RESPOSTA DAS PLATAFORMAS DIGITAIS

24 HORAS — AVALIAÇÃO DE CONTEXTO

Conteúdo: casos que exigem avaliação mais cuidadosa, como imagens manipuladas, ameaças veladas, publicações ambíguas ou situações que dependem do contexto.

Obrigação da plataforma: analisar a denúncia e apresentar decisão fundamentada.

Se mantiver o conteúdo: deve explicar o motivo e permitir contestação.



Início: Denúnica de Ilegalidade Contextual enviada.

1ª Etapa (24h): Análise inicial da Plataforma.

Removido

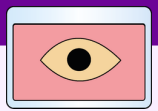
Obrigação: A plataforma deve emitir uma 'Decisão Motivada' explicando o motivo exato da recusa.

Direito de Contestação: A vítima aciona a revisão com base na recusa.

Reavaliação (+24h): Prazo final máximo. A plataforma reavalia o caso documentado e toma a decisão definitiva.

Mantido

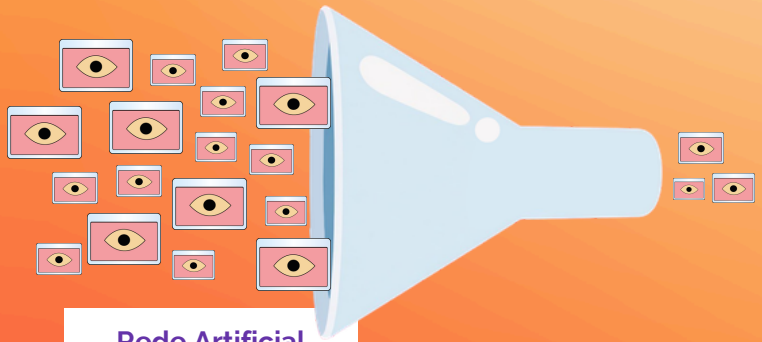
Nota: O tempo total do processo nunca é justificativa para a inação. A plataforma tem o dever legal de prover total transparência em cada etapa da decisão.



CONTENÇÃO DE ATAQUES COORDENADOS

Quando houver amplificação artificial ou coordenada de violência contra mulheres, a plataforma poderá adotar medidas mesmo sem denúncia prévia da vítima.

Isso inclui ataques massivos, redes artificiais, impulsionamento abusivo ou circulação automatizada de conteúdo violento.



Rede Artificial
Ataque Coordenado

Medidas possíveis:

- Redução de alcance;
- Diminuição de visibilidade;
- Limitação de recomendações;
- Contenção de impulsionamentos.

A TECNOLOGIA NÃO PODE SER O O MOTOR DA VIOLÊNCIA.

MEDIDAS PROTETIVAS DE URGÊNCIA NO AMBIENTE DIGITAL — O QUE A LEI GARANTE?

Proibição de contato digital

Inclui expressamente WhatsApp, e-mail, redes sociais, apps de mensagem e qualquer meio de comunicação digital.

Bloqueio judicial de perfis

Juiz pode comunicar diretamente à plataforma para bloquear ou suspender conta do agressor — sem necessidade de ação própria.

Remoção de conteúdo

Ordem judicial para remover imagens, vídeos e publicações — com prazo de cumprimento e multa diária (astreintes) pelo descumprimento.

Monitoramento eletrônico

Tornozeleira eletrônica quando há risco à integridade física. Violação da monitoração agrava a pena pelo §4º do art. 24-A LMP.

Afastamento digital forçado

O agressor pode ser impedido de acessar plataformas específicas como condição de soltura ou medida cautelar.

Multa por descumprimento

O juiz pode fixar multa diária quando a ordem judicial não for cumprida, especialmente em casos de remoção de conteúdo ou proibição de contato.

CADA RELATO PRECISO SALVA UMA VIDA

Nomear corretamente a violência é o primeiro passo para romper o ciclo da impunidade e proteger a vida das mulheres.

O Digital é nosso lugar.
Nossa conexão é livre.
A violência digital é crime.