1º Eixo: Enquadramento Jurídico

1. Lei Maria da Penha (Lei 11.340/2006)

Objetivo: Criar mecanismos para prevenir e coibir a violência doméstica e familiar contra a mulher.

Relevância para a violência digital:

- Embora tenha foco no espaço doméstico/familiar, a Lei Maria da Penha pode ser aplicada em casos de **violência psicológica, moral ou sexual, cometida por parceiros ou ex-parceiros no ambiente digital**, como perseguições, ameaças ou exposição de intimidade online.

2. Marco Civil da Internet (Lei 12.965/2014)

Objetivo: Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

Relevância para a violência digital:

- Garante a **liberdade de expressão**, mas também protege **direitos de privacidade** e **remoção de conteúdo** quando há violação de direitos.
- Prevê que o provedor de aplicações (como redes sociais) deve remover conteúdos mediante ordem judicial — o que é importante em casos de exposição íntima não consentida, por exemplo.

3. Lei Carolina Dieckmann (Lei 12.737/2012)

Objetivo: Tipifica crimes informáticos, como invasão de dispositivos eletrônicos.

Origem do nome: Criada após o vazamento de fotos íntimas da atriz Carolina Dieckmann, sem seu consentimento.

Relevância para a violência digital:

- Penaliza a **invasão de dispositivos eletrônicos**, como celulares e computadores, para obtenção de informações privadas.
- É usada em casos de **acesso não autorizado a dados, imagens ou arquivos com a intenção de humilhar, ameaçar ou coagir mulheres**.

4. Lei do Stalking (Lei 14.132/2021)

Objetivo: Cria o crime de perseguição, também conhecido como “stalking”.

Relevância para a violência digital:

- Abrange **perseguição online**, como o envio excessivo de mensagens, monitoramento constante, ameaças repetidas, etc.

- É especialmente relevante para mulheres que são vítimas de ex-parceiros abusivos ou desconhecidos em redes sociais.

5. LGPD - Lei Geral de Proteção de Dados (Lei 13.709/2018)

Objetivo: Regulamentar o tratamento de dados pessoais, garantindo privacidade e controle aos titulares.

Relevância para a violência digital:

- Protege contra o uso indevido de dados pessoais, como nome, CPF, telefone, imagens e localização.
- Ajuda a combater práticas como **doxxing** (exposição de dados pessoais com o intuito de prejudicar), muito comum em ataques online a mulheres.

<u>2º Eixo: Monitoramento e Produção de Dados</u>

1. Coleta sistemática de dados

A lei pode estabelecer que **órgãos públicos (como delegacias, Ministério Público, defensorias, etc.)** e plataformas digitais:

- **Registrem e classifiquem** os casos de violência digital com **recorte de gênero**
- Informem **meios utilizados** (redes sociais, e-mail, apps de mensagem, etc.)
- Indiquem **perfil da vítima e do agressor**, **frequência** e **motivações**

Isso ajuda a entender padrões, prevenir reincidências e orientar campanhas educativas.

2. Desagregação de dados

A coleta de dados deve considerar recortes como:

- **Gênero**
- **Raça/etnia**
- **Idade**
- **Orientação sexual e identidade de gênero**
- **Localização geográfica**
- **Situação socioeconômica**

Ex: mulheres negras e LGBTQIAPN+ são desproporcionalmente afetadas por ataques digitais.

3. Criação de banco de dados nacional

Proposta de criação (ou obrigatoriedade de integração) de um **banco de dados público e atualizado** com:

- Indicadores de violência digital por região;
- Taxas de denúncia, inquérito, processo e condenação;
- Tempo de resposta das autoridades;
- Nível de cooperação das plataformas digitais.

Pode ser gerenciado por um órgão como o Ministério da Justiça ou um Observatório de Direitos Digitais.

- Banco de dados comparativo de todos os países envolvidos nesta lei;
- Monitoramento de conteúdos que são direcionados para adolescentes e crianças através das redes sociais - criando um banco de dados de perfis e responsáveis que sejam banidos.

4. Avaliação e revisão da política

O projeto de lei pode prever:

- **Relatórios anuais** de resultados e impactos;
- **Avaliação independente** por universidades ou entidades da sociedade civil;
- Propostas de **aperfeiçoamento da legislação** com base nesses dados.

5. Parcerias estratégicas

Estimular acordos com:

- **Universidades e centros de pesquisa;**
- **Organizações da sociedade civil** (Ex: SaferNet, InternetLab);
- **Plataformas digitais** (Ex: Meta, Google, TikTok) para compartilhamento de dados agregados e anônimos sobre denúncias e remoções;
- Exigir que as plataforma digitais mantenham suas Políticas de Segurança para que se evite os crimes, assim como tenha uma consequência mais severa para quem cometê-los;
- Aplicativos de paquera, para que se exija a comprovação de identidade dos usuários a fim de evitar golpes de perfis falsos.

Exemplo de dispositivo legal:

“Os órgãos responsáveis pela segurança pública deverão coletar e divulgar, de forma transparente e acessível, dados desagregados sobre violência digital com base em gênero, raça, idade e orientação sexual, a fim de subsidiar políticas públicas eficazes.”