ARTIFICIAL INTELLIGENCE AS AN ENABLER OF CRIMES AGAINST WOMEN: AN EXPLORATION OF LEGAL AND ETHICAL CHALLENGES

Ananya Mishra, Amity Law School, Noida

Amity University, Uttar Pradesh

1. Introduction

The rapid advancement of artificial intelligence technologies has fundamentally disrupted traditional legal paradigms, creating unprecedented challenges for protecting women from technologically mediated violence and discrimination. As AI systems become increasingly sophisticated and ubiquitous, they have enabled new forms of gender-based harm that existing legal frameworks— developed primarily in pre-digital eras—are ill-equipped to address. This chapter provides a comprehensive examination of how contemporary legal systems across major jurisdictions are grappling with the complex intersection of artificial intelligence and crimes against women.

1.1 The Challenge of Legal Evolution in the Digital Age

The emergence of AI-enabled crimes against women presents legal systems with a fundamental dilemma: how to apply centuries-old legal principles to rapidly evolving technological realities. Traditional criminal and civil law frameworks were conceptualized in contexts where harm was primarily physical, perpetrators were identifiable individuals, and the mechanisms of abuse were tangible and comprehensible to courts and lawmakers. AI technologies have disrupted each of these assumptions, creating forms of harm that can be:

- **Algorithmically mediated**: Where discriminatory outcomes emerge from complex computational processes rather than direct human decisions
- **Synthetically generated**: Where realistic but fabricated content can cause profound reputational and psychological harm
- **Automatically scaled**: Where individual acts of abuse can be amplified and

systematized through technological processes

- **Cross-jurisdictionally distributed**: Where perpetrators, victims, platforms, and technical infrastructure span multiple legal systems

These characteristics of AI-enabled crimes create novel challenges for legal frameworks designed around different assumptions about the nature of harmful conduct.

1.2 Scope and Structure of Analysis

This chapter examines how legal systems in three major jurisdictions—the United States, United Kingdom, and European Union—are attempting to address AI-enabled crimes against women. These jurisdictions represent distinct regulatory philosophies and approaches to technology governance, providing important comparative insights into different strategies for addressing algorithmic harm.

The analysis proceeds through several interconnected sections:

- **International Legal Framework (Section 3.1)** examines the limitations of existing international instruments, including CEDAW, the Budapest Convention on Cybercrime, and the Istanbul Convention, in addressing AI-specific forms of gender-based violence. This section explores how pre-digital international frameworks struggle to encompass algorithmic discrimination, synthetic media abuse, and automated harassment systems.

- **United States Legal Landscape (Section 3.2)** analyses the fragmented American approach, examining how federal statutes like Section 230 of the Communications Decency Act, the Violence Against Women Act, and emerging state legislation create a complex patchwork of protections with significant gaps. The section explores how the American preference for platform immunity and state-level experimentation affects victims of AIenabled crimes.

- **United Kingdom Regulatory Approach (Section 3.3)** examines the UK's more centralized response, particularly through the Online Safety Act (2023), and how existing criminal legislation addresses technologyfacilitated abuse. This section explores the UK's attempt to balance platform accountability with free expression concerns in the context of AI-enabled harms.

- **European Union Digital Governance Framework (Section 3.4)** provides detailed analysis of the EU's comprehensive regulatory approach, including the General Data Protection Regulation (GDPR), the proposed Artificial Intelligence Act, and the Digital Services Act. This section examines how the EU's multi-layered regulatory strategy addresses different dimensions of AI-enabled crimes against women.

- **Cross-Jurisdictional Analysis (Section 3.5)** synthesizes findings across jurisdictions, identifying common limitations and protection gaps that persist despite different regulatory approaches. This comparative analysis reveals structural challenges that transcend specific national frameworks.

1.3 Key Themes and Arguments

Throughout this examination, several critical themes emerge that illuminate the broader challenges facing legal systems attempting to address AI-enabled crimes against women:

- **Technological Determinism vs. Legal Adaptability**: The analysis reveals persistent tensions between rapidly evolving technological capabilities and the necessarily deliberative processes of legal development. Legal systems consistently lag behind technological developments, creating periods of regulatory uncertainty that can be exploited by those seeking to harm women through AI technologies.

- **Platform Immunity vs. Accountability**: Across jurisdictions, debates over digital platform responsibility represent crucial battlegrounds for determining how AI-enabled crimes will be addressed. The balance struck between protecting platforms from liability and ensuring they take adequate steps to prevent harm has profound implications for victims' ability to seek redress.

- **Individual Rights vs. Systemic Approaches**: Legal frameworks struggle to balance individual-focused remedies (such as criminal prosecution or civil suits) with systemic approaches that address the structural dimensions of AI-enabled discrimination and abuse. Many harmful AI applications operate at scales that make individual-focused remedies inadequate.

- **Gender-Neutral Approaches vs. Gender-Responsive Regulation**: The analysis reveals how ostensibly neutral technology regulation often fails to address the disproportionate and qualitatively different impacts of AI systems on women and other marginalized groups. This highlights the need for explicitly gender-responsive approaches to AI governance.

• Implications for Legal Reform

The comprehensive analysis presented in this chapter has significant implications for legal reform efforts. By examining both the strengths and limitations of existing frameworks across multiple jurisdictions, this chapter provides a foundation for understanding what elements of current approaches show promise and where fundamental reconceptualization may be necessary.

The findings suggest that addressing AI-enabled crimes against women requires more than merely extending existing legal categories to cover new technologies. Instead, it demands fundamental reconsideration of legal frameworks to address the unique characteristics of algorithmic harm: its potential for scale, its distributed nature, its technical complexity, and its intersection with existing patterns of gender-based discrimination and violence.

This analysis thus serves not only as a descriptive account of current legal approaches but as a critical foundation for the normative arguments about legal reform that follow in subsequent chapters. Understanding the limitations and gaps in existing frameworks is essential for developing more effective approaches to protecting women from AI-enabled harm while preserving the benefits that AI technologies can provide for gender equality and women's empowerment.

The examination reveals that while no jurisdiction has yet developed a fully adequate response to AI-enabled crimes against women, different approaches offer valuable insights into potential paths forward. The challenge for policymakers, advocates, and legal scholars is to synthesize these insights into more comprehensive and effective frameworks that can provide meaningful protection for women in an increasingly AI-mediated world.

2. Existing Legal Frameworks & Their Limitations

2.1 International Legal Framework

The international legal landscape governing AI-enabled crimes against women comprises a patchwork of instruments developed primarily before the emergence of sophisticated artificial intelligence technologies. While these frameworks provide important general principles regarding gender-based violence and discrimination, they have significant limitations in addressing the specific challenges posed by algorithmically mediated harms.[1]

The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), adopted in 1979, represents the most comprehensive international instrument addressing gender discrimination. Article 2 obligates state parties to "pursue by all appropriate means and without delay a policy of eliminating discrimination against women," while subsequent provisions address specific domains such as political participation, education, employment, and healthcare[2]. The CEDAW Committee has interpreted these obligations as encompassing technology-facilitated gender-based violence through General Recommendation No. 35, which recognizes that "gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private, including in the contexts of...technology mediated environments."

However, CEDAW's application to AI-enabled crimes faces significant limitations. The convention predates the development of modern AI systems by decades, creating conceptual gaps regarding algorithmic discrimination, synthetic media abuse, and automated harassment. Implementation and enforcement

mechanisms remain weak, relying primarily on periodic reporting and non-binding recommendations. The United States' failure to ratify CEDAW further limits its effectiveness in one of the world's primary AI development centres. The Budapest Convention on Cybercrime (2001) provides more specific coverage of technology facilitated offenses, requiring signatories to criminalize computer-related forgery, fraud, child pornography, and copyright infringement. A 2003 additional protocol addresses racist and xenophobic acts committed through computer systems[3]. However, the Convention contains no specific provisions addressing gender-based cybercrime or AI-enabled offenses. Its conceptual

[1] Aldoseri, Abdulaziz, Khalifa N. Al-Khalifa, and Abdel Magid Hamouda. "Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges." *Applied Sciences* 13.12 2023.

[2] Krook, Joshua, et al. "A systematic literature review of artificial intelligence (AI) transparency laws in the European Union (EU) and United Kingdom (UK): a socio-legal approach to AI transparency governance." *AI and Ethics* (2025).

[3] Al-Maamari, Amir. "Between Innovation and Oversight: A Cross-Regional Study of AI Risk Management Frameworks in the EU, US, UK, and China." *arXiv preprint arXiv:2503.05773* (2025).

framework focuses primarily on unauthorized access and system interference rather than algorithmic exploitation or synthetic media abuse, creating significant coverage gaps for AIenabled crimes against women.

More recent international initiatives have begun addressing digital gender-based violence more explicitly. The Council of Europe's Istanbul Convention (2011) recognizes technologyfacilitated abuse in Article 40 on sexual harassment, interpreted by the Expert Group as encompassing online stalking and harassment. United Nations Human Rights Council Resolution 38/5 (2018) specifically acknowledges "emerging forms of online violence against women and girls" and calls on states to address them through appropriate legal measures. The UN General Assembly's 2018 resolution on "intensification of efforts to prevent and eliminate all forms of violence against women and girls: sexual harassment" similarly recognizes technology as a potential facilitator of gender-based violence requiring specific policy attention.

Despite these developments, the international framework remains fundamentally reactive and fragmented, with significant gaps regarding AI-specific offenses. No binding international instrument directly addresses deepfakes, algorithmic discrimination, or AI-facilitated exploitation. Existing instruments operate primarily through state implementation, creating inconsistent protection levels across jurisdictions[4]. Enforcement mechanisms remain weak, with limited accountability for noncompliance with international standards.

The United Nations' recent work on AI governance, including the Secretary-General's Roadmap for Digital Cooperation and the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021), has begun incorporating gender dimensions but lacks binding force or specific provisions addressing AI-enabled crimes. The 2023 UN General Assembly Resolution on "guiding principles for safe, secure and trustworthy artificial intelligence systems" acknowledges potential harmful impacts but provides only general guidance rather than concrete legal obligations regarding gender-specific harms.

Several structural factors limit the effectiveness of international frameworks in addressing AIenabled crimes against women. Technological development consistently outpaces international consensus building processes, creating persistent regulatory lag. Geopolitical

[4] Wong, Anthony. "The laws and regulation of AI and autonomous systems." *Unimagined futures–ICT opportunities and challenges* (2020).

tensions regarding digital governance models impede development of binding international standards. The distributed nature of AI development and deployment creates jurisdictional complexities that traditional international law mechanisms struggle to address[5].

As a result, protection against AI-enabled crimes against women varies dramatically across jurisdictions, with victims frequently falling through gaps in an inconsistent international framework. While international instruments provide important normative foundations and general principles, they currently offer limited practical protection against rapidly evolving forms of algorithmic harm.

2.2 United States Legal Landscape

The United States lacks comprehensive federal legislation specifically addressing AI-enabled crimes against women. Instead, victims must navigate a complex patchwork of federal and state laws developed primarily for other purposes and only partially adapted to technological contexts. This fragmented approach creates significant protection gaps while imposing substantial burdens on victims seeking legal redress.

Federal Legislative Framework

Section 230 of the Communications Decency Act (1996) represents perhaps the most significant federal provision affecting victims of AI-enabled abuse. This legislation immunizes internet platforms from liability for user-generated content, providing that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Courts have interpreted this immunity broadly, shielding platforms from liability even when they have been notified about harmful content and failed to remove it.[6]

For victims of AI-enabled crimes, Section 230 creates substantial barriers to holding platforms accountable for hosting deepfakes, automated harassment, or AI-generated defamatory content. In Herrick v. Grindr (2019), for example, the Second Circuit held that Section 230 barred claims against a platform even when it allegedly failed to address algorithmically facilitated

[5] Arora, Saransh, and Sunil Raj Thota. "Ethical considerations and privacy in AI-driven big data analytics." *no. May* (2024).

[6] Castets-Renard, Céline. "AI and the Law in the EU and the US." *Artificial Intelligence and the Law in Canada* 2020.

impersonation and harassment. While Section 230 contains exceptions for federal criminal law, intellectual property claims, and certain sex trafficking provisions, these carve-outs provide limited protection against most forms of AI-enabled gender-based violence.

The Violence Against Women Act (VAWA), first enacted in 1994 and most recently reauthorized in 2022, represents another relevant federal framework. The 2022 reauthorization includes provisions addressing "cybercrimes against individuals," including cyberstalking, video streaming of intimate partner violence, and non-consensual pornography. However, VAWA contains no specific provisions addressing AI generated content, deepfakes, or algorithmic targeting, creating uncertainty about its applicability to novel technological threats[7].

Federal computer crime legislation, particularly the Computer Fraud and Abuse Act (CFAA), criminalizes unauthorized access to protected computers and related offenses. However, the CFAA's focus on hacking and unauthorized access makes it poorly suited to addressing AIenabled crimes that may occur without traditional system breaches. The narrow interpretation of the CFAA in Van Buren v. United States (2021) further limited its applicability to many forms of algorithmic abuse. Federal anti-discrimination laws, including Title VII of the Civil Rights Act, the Equal Credit Opportunity Act, and the Fair Housing Act, provide potential avenues for challenging algorithmic discrimination. However, these frameworks typically require demonstrating either discriminatory intent or disparate impact, both challenging to establish in the context of opaque AI systems. Enforcement typically relies on individual complaints rather than proactive oversight, creating significant barriers for victims who may never know they have been subjected to algorithmic discrimination.

State-Level Developments

In the absence of comprehensive federal legislation, states have begun developing more targeted approaches to AI-enabled harms. California's AB 602 (2019) created a private right of action against anyone who "creates and intentionally discloses sexually explicit material" if the person depicted did not consent to its creation or disclosure. Virginia, Texas, and New York have enacted similar legislation specifically addressing deepfake pornography, though with

[7] Ponkin, Igor V., and Alena I. Redkina. "Artificial intelligence from the point of view of law." *RUDN Journal of Law* 22.1 (2018).

varying definitions, exceptions, and remedies.[8]

Some states have also begun addressing AI-enabled discrimination more comprehensively. California's Automated Decision Systems Accountability Act requires businesses using automated decision systems that impact consumers to implement risk management processes and conduct impact assessments. Illinois' Artificial Intelligence Video Interview Act requires notice, consent, and limited data sharing when employers use AI to analyze video interviews. However, these emerging frameworks remain inconsistent across states, creating a complex regulatory patchwork with significant protection gaps.

Judicial Approaches

U.S. courts have struggled to apply existing legal frameworks to AI-enabled harms against women. In the deepfake context, courts have reached inconsistent conclusions about whether synthetic media constitutes defamation, given its technically fictional nature, and whether privacy torts adequately capture the harm of having one's likeness synthetically manipulated. Tort doctrines like intentional infliction of emotional distress provide potential remedies but typically require demonstrating "extreme and outrageous conduct" and severe emotional distress, high thresholds that courts have inconsistently applied to digital harms.

The Supreme Court's decision in Mahanoy Area School District v. B.L. (2021), while focused on student speech rights, included dicta recognizing that "the school's regulatory interests remain significant in some off-campus circumstances," including "severe bullying or harassment targeting particular individuals." This recognition of digital harassment as legally cognizable harm may influence future jurisprudence regarding AI-enabled abuse, though its implications remain undeveloped.

In algorithmic discrimination cases, courts have reached inconsistent conclusions about whether statistical evidence of disparate outcomes satisfies legal standards for discrimination. The Southern District of New York held in Sandvig v. Barr (2020) that testing algorithms for discriminatory outcomes was protected activity, potentially facilitating future algorithmic discrimination litigation. However, the procedural and evidentiary barriers to successful

[8] Evgenievich, Kolenteev Konstantin, and Korolev Artem Sergeevich. "LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE ON THE EXAMPLE OF THE JAPAN, SINGAPORE, USA." *B 93* (2022).

discrimination claims remain substantial, particularly given limited discovery access to proprietary algorithms.[9]

Enforcement Challenges

Even where applicable legal provisions exist, enforcement faces significant practical challenges. Federal agencies including the Federal Trade Commission, Equal Employment Opportunity Commission, and Department of Justice have limited resources and technical expertise for addressing AI-enabled crimes. Cross-jurisdictional issues frequently arise when perpetrators, platforms, and victims are in different states or countries. Victims often lack resources for protracted civil litigation, while public prosecutors may deprioritize technology facilitated crimes perceived as less severe than physical violence. The U.S. legal landscape thus presents a fragmented and inconsistent approach to AI-enabled crimes against women. While emerging state legislation shows promising developments, the fundamental lack of comprehensive federal frameworks creates significant protection gaps and places substantial burdens on victims navigating a complex legal terrain.

2.3 United Kingdom Regulatory Approach

The United Kingdom has adopted a more centralized approach to regulating digital harms than the United States, with several recent legislative initiatives explicitly addressing online abuse. This regulatory framework provides important protections against some forms of AI-enabled crimes against women, though significant gaps remain, particularly regarding algorithmic discrimination and synthetic media manipulation.

Online Safety Act

The Online Safety Act (2023) represents the UK's most significant recent legislation addressing digital harms. The Act imposes a statutory "duty of care" on user-to-user services and search engines to protect users from illegal and harmful content. Services must conduct risk assessments, implement proportionate systems and processes to mitigate identified risks, and provide transparent reporting on their safety measures. The Act establishes Ofcom as the

[9] Cortez, Elif Kiesow, and Nestor Maslej. "Adjudication of artificial intelligence and automated decision-making cases in Europe and the USA." *European Journal of Risk Regulation* 14.3 (2023).

regulator with powers to issue codes of practice, investigate compliance, and impose substantial fines for violations.[10]

For victims of AI-enabled crimes, the Act provides several important protections. It specifically addresses "priority content that is harmful to adults," including content promoting violence against women and girls, which encompasses certain forms of AI-generated harassment. The Act creates expedited content removal procedures for illegal content and establishes user advocacy mechanisms. Notably, the Act's focus on platform responsibility partially circumvents the attribution challenges inherent in identifying individual perpetrators of AI-enabled abuse.

However, the Online Safety Act has significant limitations regarding AI-specific harms. It primarily addresses content moderation rather than algorithmic system design, potentially leaving gaps regarding automated discrimination and algorithmic amplification of harmful content. The Act's implementation remains ongoing, with important details still to be determined through regulatory codes of practice. Critics have raised concerns about potential chilling effects on legitimate expression, which could affect discussion of gender-based violence and discrimination.

Existing Criminal Legislation

Beyond the Online Safety Act, several existing UK statutes address aspects of technology-facilitated abuse, though with varying applicability to AI-enabled crimes. The Protection from Harassment Act (1997) criminalizes "a course of conduct" that the defendant "knows or ought to know amounts to harassment," potentially encompassing AI-facilitated stalking and targeted harassment. Courts have interpreted "course of conduct" broadly to include technological mechanisms, though questions remain about whether deploying automated systems constitutes the required course of conduct.

The Malicious Communications Act (1988) prohibits sending communications with intent to cause distress or anxiety, while the Communications Act (2003) criminalizes sending "grossly offensive" or menacing messages through public electronic communications networks. These

[10] Krook, Joshua, et al. "A systematic literature review of artificial intelligence (AI) transparency laws in the European Union (EU) and United Kingdom (UK): a socio-legal approach to AI transparency governance." *AI and Ethics* (2025).

provisions potentially address some forms of AI-generated harassing content, though they typically require demonstrating specific intent, creating challenges when harmful content results from algorithmic processes without direct human direction.[11]

The Criminal Justice and Courts Act (2015) specifically criminalizes "revenge pornography"—disclosing private sexual images with intent to cause distress. Courts have inconsistently applied this legislation to manipulated or synthetic images, creating uncertainty about its applicability to deepfakes and other AI-generated content. The Domestic Abuse Act (2021) expanded protections against technology facilitated domestic abuse but contains no specific provisions addressing AI-enabled methods.

Data Protection and Equality Frameworks

The UK's implementation of GDPR through the Data Protection Act (2018) provides additional protections relevant to AI-enabled harms. Article 22 of GDPR establishes rights regarding automated decision making, including the right not to be subject to purely automated decisions with significant effects.[12] The Information Commissioner's Office has issued guidance indicating that synthetic media creation may require data protection impact assessments and potentially explicit consent. However, exemptions for personal use and legitimate interests create potential gaps in protection.

The Equality Act (2010) prohibits discrimination based on protected characteristics including sex, potentially addressing algorithmic discrimination against women.[^44] However, enforcement typically requires demonstrating either direct discrimination (treating someone less favorably because of a protected characteristic) or indirect discrimination (applying a provision that disadvantages people with a protected characteristic), both challenging to establish in the context of opaque algorithmic systems.

Enforcement and Implementation

While the UK's legislative framework provides more comprehensive coverage than the US approach, significant enforcement challenges persist. The Online Safety Act's implementation remains ongoing, with important aspects of the regulatory regime still under development. Law

[11] Roberts, Huw, et al. "Artificial intelligence regulation in the United Kingdom: a path to good governance and global leadership?" *Internet Policy Review* 12.2 (2023): 1-31.

[12] Kemp, Richard. "Legal Aspects of Artificial Intelligence (v. 2.0)." *Kemp IT Law.2016.*

enforcement agencies often lack specialized expertise in digital investigations, particularly regarding advanced AI technologies. Cross border enforcement remains challenging, with many perpetrators and platforms operating outside UK jurisdiction.[13]

The UK's approach thus represents a more centralized and comprehensive framework than the US model, with recent legislation explicitly addressing online safety. However, significant gaps remain regarding AI specific harms, particularly algorithmic discrimination, synthetic media manipulation, and automated harassment systems. The effectiveness of the emerging regulatory regime will depend substantially on implementation details still under development and enforcement resources yet to be allocated.

2.4 European Union Digital Governance Framework

The European Union has developed the world's most comprehensive regulatory framework addressing digital technologies, with several initiatives specifically relevant to AI-enabled crimes against women. This approach includes both binding legislation and soft law instruments, creating a multifaceted governance structure with significant implications for addressing algorithmic harm.

General Data Protection Regulation

The General Data Protection Regulation (GDPR), implemented in 2018, establishes foundational principles that address several dimensions of AI-enabled crimes against women. Article 5 requires that personal data processing be lawful, fair, transparent, purpose-limited, and secure – principles that potentially constrain abusive AI applications. Article 22 establishes specific rights "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her," creating potential protections against harmful algorithmic decision-making[14].

For victims of deepfakes and other synthetic media abuse, GDPR offers several relevant protections. Article 7 establishes strict standards for consent, requiring that it be "freely given, specific, informed and unambiguous," standards rarely met in non-consensual AI content

[13] Cath, Corinne, et al. "Artificial intelligence and the 'good society': the US, EU, and UK approach." *Science and engineering ethics* 24 (2018).

[14] Hildebrandt, Mireille. "The Artificial Intelligence of European Union Law." *German Law Journal* 21.1 (2020): 74-79.

generation. The "right to erasure" under Article 17 potentially enables victims to demand removal of intimate images used to generate deepfakes, though its effectiveness depends on identifying where training data is stored.

However, GDPR has significant limitations regarding AI-enabled crimes. Exemptions for personal use create potential gaps regarding individually created deepfakes or harassment tools. Enforcement varies significantly across national Data Protection Authorities, creating inconsistent protection levels.[15] The regulation's focus on data processing rather than content means it addresses some aspects of AI-enabled crimes while leaving others unregulated.

Artificial Intelligence Act

The proposed Artificial Intelligence Act represents the EU's most ambitious attempt to specifically regulate AI systems. The regulation establishes a risk-based approach, categorizing AI applications based on their potential harm and imposing graduated obligations accordingly. "Unacceptable risk" applications are prohibited entirely, "high-risk" applications face substantial regulatory requirements, "limited risk" applications must meet transparency obligations, and "minimal risk" applications face few restrictions.

For addressing AI-enabled crimes against women, several provisions have relevance. The regulation prohibits AI systems that "exploit vulnerabilities of specific vulnerable groups" or use "subliminal techniques beyond a person's consciousness" to materially distort behavior in harmful ways, potentially addressing certain forms of algorithmic exploitation. High-risk classification for employment, education, and law enforcement AI systems triggers requirements for risk assessment, human oversight, and accuracy that could mitigate algorithmic discrimination.

However, the AI Act's effectiveness in addressing gender-based harms faces important limitations. The regulation primarily focuses on system developers and deployers rather than establishing individual rights for those harmed by AI systems[16]. Enforcement relies substantially on conformity assessments and technical standards rather than victim-cantered

[15] Pagallo, Ugo, Jacopo Ciani Sciolla, and Massimo Durante. "The environmental challenges of AI in EU law: lessons learned from the Artificial Intelligence Act (AIA) with its drawbacks." *Transforming Government: People, Process and Policy* 16.3 (2022).

[16] Smuha, Nathalie A., et al. "How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act." (2021).

remedies. Critics have argued that the regulation's risk classifications inadequately incorporate gender-specific concerns, with insufficient attention to how seemingly low-risk applications can create disproportionate harms for women.

Digital Services Act

The Digital Services Act (DSA), which entered into force in 2022, establishes new obligations for digital platforms regarding content moderation, transparency, and user protection. For victims of AI-enabled crimes, several provisions offer important protections: "Very Large Online Platforms" must assess and mitigate systemic risks, including those related to gender-based violence; notice-and-action mechanisms must enable efficient reporting of illegal content; and transparency reporting must include information about content moderation actions.

The DSA's focus on platform responsibility partially addresses attribution challenges inherent in identifying individual perpetrators of AI-enabled crimes. By establishing platform obligations regarding risk assessment and mitigation, the regulation creates accountability mechanisms that operate regardless of whether individual perpetrators can be identified.[17] The regulation's graduated obligations based on platform size recognize the amplified harm potential of larger services. However, the DSA's effectiveness in addressing AI-enabled crimes against women depends substantially on implementation details still under development. The regulation's primary focus on illegal content may create gaps regarding harmful but not clearly illegal AI applications. Cross-border enforcement remains challenging despite the regulation's harmonized approach.

Gender-Specific Instruments

Beyond these technology-focused regulations, the EU has developed several instruments specifically addressing gender-based violence that have relevance for AI-enabled crimes. The European Commission's Gender Equality Strategy 2020-2025 explicitly recognizes online violence against women as a priority area, committing to "facilitate the development of a new

[17] Krook, Joshua, et al. "A systematic literature review of artificial intelligence (AI) transparency laws in the European Union (EU) and United Kingdom (UK): a socio-legal approach to AI transparency governance." *AI and Ethics* (2025).

framework for cooperation of internet platforms" to address online violence against women.[18]

The proposed Directive on combating violence against women and domestic violence includes provisions specifically addressing cyber violence, defining it to include "non-consensual sharing of intimate or manipulated material" and "cyber stalking," categories that encompass certain AI-enabled crimes. If adopted, this directive would require member states to criminalize these behaviours and establish appropriate penalties, potentially closing some gaps in national legislation.

Implementation and Enforcement

The EU's comprehensive regulatory approach offers significant potential protections against AI-enabled crimes against women, but several implementation challenges affect its practical effectiveness. National transposition of EU directives creates some inconsistency across member states, though less than in the entirely decentralized US approach. Resource limitations affect enforcement capacity, particularly regarding technically complex AI systems.

Jurisdictional challenges persist when perpetrators operate from outside the EU.

The interaction between different regulatory instruments—GDPR, AI Act, DSA, and genderbased violence frameworks—creates both opportunities and complexities. In some cases, these instruments provide complementary protections addressing different aspects of AI-enabled crimes. In others, potential inconsistencies or gaps between regulatory regimes create uncertainty for both victims and regulated entities.

Despite these challenges, the EU's approach represents the most comprehensive regulatory framework addressing AI-enabled harms globally. Its multi-layered strategy combining data protection, AI-specific regulation, platform responsibility, and gender-based violence instruments provide a more coherent approach than the fragmentary frameworks in other jurisdictions.

[18] Jarota, Maciej. "Artificial intelligence in the work process. A reflection on the proposed European Union regulations on artificial intelligence from an occupational health and safety perspective." *Computer Law & Security Review* 49 (2023): 105825.

2.5 Cross-Jurisdictional Analysis and Common Limitations

Comparing regulatory approaches across the United States, United Kingdom, and European Union reveals important patterns in how legal systems are attempting to address AI-enabled crimes against women. Despite significant differences in regulatory philosophy and implementation, several common limitations persist across jurisdictions, creating consistent protection gaps for victims of algorithmically mediated harm.

Definitional Ambiguities

All examined jurisdictions struggle with definitional challenges regarding AI-enabled offenses. Traditional criminal statutes typically define prohibited conduct with reference to human actions and mental states, creating uncertainty about their applicability to algorithmic processes. Terms like "harassment," "stalking," and "non-consensual image sharing" were conceptualized before the emergence of AI technologies, leaving significant interpretive questions about their scope[19]. These definitional ambiguities create both substantive protection gaps and procedural barriers as victims and their representatives must navigate uncertain legal terrain.

Even jurisdictions that have enacted technology-specific legislation often employ definitions that quickly become outdated. California's deepfake legislation, for example, addresses "digitally produced or altered material" but may not clearly encompass future synthetic media technologies operating through fundamentally different technical mechanisms. The EU's proposed AI Act defines artificial intelligence broadly as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of humandefined objectives, generate outputs such as content, predictions,[20] recommendations, or decisions influencing the environments they interact with," but this definition will require continuous updating as new techniques emerge.

Fragmented Legal Frameworks

All examined jurisdictions address AI-enabled harms through multiple, often poorly

[19] Cath, Corinne, et al. "Artificial intelligence and the 'good society': the US, EU, and UK approach." *Science and engineering ethics* 24 2018.

[20] Akinola, Olanrewaju, Ogundipe Adebayo Tunbosun, and Bankole Oladapo. "Comparative Analysis Regulatory of AI and Algorithm in UK, EU and USA." *EU and USA* (2022).

coordinated legal frameworks. In the United States, victims must navigate federal criminal statutes, state-specific provisions, tort law, intellectual property protections, and platform immunity doctrines to address different aspects of AI-enabled crimes. The UK's approach spans the Online Safety Act, various criminal statutes, data protection law, and equality legislation. Even the EU's relatively comprehensive approach distributes relevant provisions across GDPR, the proposed AI Act, the Digital Services Act, and gender-based violence frameworks.

This fragmentation creates several practical challenges for victims. First, it imposes substantial information burdens, requiring victims to identify and understand multiple complex legal regimes to seek redress. Second, it creates potential gaps where harmful conduct falls between regulatory frameworks. Third, it complicates enforcement, often requiring coordination between multiple agencies with different mandates, priorities, and expertise levels.

Enforcement Challenges

Across all jurisdictions, significant enforcement challenges limit the practical effectiveness of legal protections. Law enforcement agencies often lack specialized expertise in investigating technologically sophisticated crimes, particularly those involving advanced AI applications.

Resource constraints affect both public prosecution and regulatory oversight, frequently resulting in DE prioritization of digital harms perceived as less severe than physical violence. Court systems similarly struggle with the technical complexity of many AI-enabled crimes, creating barriers to effective judicial resolution.

These enforcement challenges create substantial practical protection gaps even where applicable legal provisions exist in theory. Many victims report comprehensive failures in system response, with law enforcement declining to investigate, prosecutors unwilling to pursue charges, and courts struggling to apply existing legal frameworks to novel technological harms.

Limited Platform Accountability

Despite different approaches to intermediary liability, all examined jurisdictions struggle with establishing appropriate accountability mechanisms for digital platforms that host, amplify, or facilitate AI-enabled abuse. The United States' Section 230 immunity creates the widest protection for platforms, shielding them from liability for most user-generated content regardless of moderation practices. The UK's Online Safety Act establishes more robust platform obligations but remains under implementation with significant details still undetermined.

The EU's Digital Services Act creates graduated responsibilities for platforms but faces implementation and enforcement challenges.[21] This limited platform accountability creates significant obstacles for addressing AI-enabled crimes at scale. Individual perpetrators may be anonymous, judgment-proof, or located in jurisdictions with limited enforcement cooperation, making platform-level interventions essential for effective protection. However, current legal frameworks provide incomplete mechanisms for ensuring platforms implement adequate safeguards against AI-enabled exploitation of their services.

Cross-Border Enforcement Barrier

All examined jurisdictions face significant challenges in addressing the inherently transnational nature of many AI-enabled crimes. Perpetrators, victims, platforms, and technical infrastructure may be distributed across multiple national jurisdictions, creating complex questions about applicable law and enforcement authority. While the EU's harmonized approach reduces intra-

EU fragmentation, significant challenges remain regarding cooperation with non-EU jurisdictions.

Several structural factors exacerbate these cross-border challenges. Mutual legal assistance treaties typically involve lengthy processes poorly suited to rapidly evolving digital crimes. Jurisdictional claims based on server location create enforcement gaps when infrastructure is strategically located in countries with limited regulatory oversight. Extradition limitations and dual criminality requirements further complicate prosecution of cross-border offenses.

Gender-Blindness in Technology Regulation

A final common limitation across jurisdictions involves the frequent gender-blindness of

[21] Montasari, Reza. "National artificial intelligence strategies: a comparison of the UK, EU and US approaches with those adopted by state adversaries." *Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity*. Cham: Springer International Publishing, 2023.

technology regulation. Many AI governance frameworks adopt ostensibly neutral approaches that fail to address the disproportionate and qualitatively different impacts of technology on women and other marginalized groups. This neutrality frequently manifests in risk assessment frameworks that inadequately capture gender-specific harms, enforcement priorities that deprioritize digital violence against women, and regulatory impact assessments that overlook gendered dimensions of technological systems.[22]

Even when legal frameworks recognize gender-based violence in principle, they often fail to integrate this recognition into operational details. The EU's proposed AI Act, for example, acknowledges gender bias as a concern but provides limited specific mechanisms for addressing gendered impacts in its risk classification and assessment processes. The UK's Online Safety Act includes gender-based violence within its scope but offers few targeted provisions addressing the specific dynamics of AI-enabled gender-based crimes.

This gender-blindness creates protection gaps even in otherwise comprehensive regulatory frameworks. When laws and policies fail to explicitly address the gendered dimensions of technological harm, implementation and enforcement typically reproduce existing biases that deprioritize women's experiences. Gender-responsive approaches remain the exception rather than the norm across the examined jurisdictions, limiting the effectiveness of even well-designed regulatory interventions.

[22] Singay, Muhammad Ali. *AI Revolution on Trial: Protection of Women against Generative Artificial Intelligence in the USA and UK*. Diss. Central European University.