



Protecting Victims of Online Gender-Based Violence in Indonesia and South Africa

*Rani Santika¹

Institut Islam Kuningan,
Indonesia

Rafi Farizki²

Politeknik Siber Cerdika Internasional,
Indonesia

Jaco Barkhuizen³

Rabdan Academy,
United Arab Emirates

Ade Fitri Fatimah⁴

Universitas Gadjah Mada,
Indonesia

***Corresponding author:**

Rani Santika, Institut Islam Kuningan.
rsantika851@gmail.com

Article Info:

Article history:

Received: July 30, 2026

Revised: September 11, 2026

Accepted: September 14, 2026

Available Online: September 23,
2026

Keywords:

Online Gender-Based Violence;
Image-Based Sexual Abuse; Victim
Protection; Comparative Law;
Indonesia; South Africa



This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

Copyright © 2026 by Author. Published by
Politeknik Siber Cerdika Internasional

Abstract

Background: Online gender-based violence has risen sharply in Indonesia and South Africa. Yet the two countries have responded through markedly different legislative routes. This article compares the legal frameworks governing such violence in the two jurisdictions.

Objective: The study compares these frameworks and draws reciprocal lessons for a victim-centered model of regulation suited to Global South jurisdictions.

Methods: The study employs a doctrinal comparative method. It evaluates both legal regimes through a victimological lens attentive to secondary victimization. For Indonesia, it examines the *Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual* (Law No. 12 of 2022 on Sexual Violence Crimes), the amended Electronic Information and Transactions Law, and the Personal Data Protection Law. For South Africa, it examines the Cybercrimes Act 19 of 2020 and its companion legislation on films and publications, data protection, and domestic violence.

Results: Three findings emerge. First, South African law defines the paradigmatic offense of the non-consensual disclosure of intimate images with a degree of precision that Indonesian law has yet to achieve. It also expressly extends protection to simulated imagery. Second, Indonesian law provides a more comprehensive framework of victim rights, restitution, and recovery. Third, both systems continue to exhibit enforcement weaknesses that expose victims to secondary victimization.

Conclusion: The article draws reciprocal lessons from the two jurisdictions and outlines a victim-centered model of regulation for Global South jurisdictions.

To cite this article: Santika, R., Farizki, R., Barkhuizen, J., & Fatimah, A. F. (2026). Protecting Victims of Online Gender-Based Violence in Indonesia and South Africa. *Journal of Law & Social Politics*, 4 (4), 739-751. <https://doi.org/10.59261/jlsp.v4i4.253>

INTRODUCTION

The digitization of everyday life has changed how gender-based violence is perpetrated (Barter & Koulu, 2021; Dunn, 2020). Harassment that once required physical proximity can now be inflicted remotely, anonymously, at scale, and with a permanence that physical acts rarely possess. International human rights bodies have acknowledged this shift. General Recommendation No. 35 of the CEDAW Committee extends the understanding of gender-based violence against women to conduct occurring through technology-mediated environments and confirms that such violence engages the due diligence obligations of states (CEDAW Committee, 739 | Journal of Law & Social Politics

2017). A substantial body of scholarship now documents the phenomenon under labels such as technology-facilitated sexual violence and online gender-based violence, an umbrella term encompassing online sexual harassment, image-based sexual abuse, sextortion, doxxing, cyberstalking, and, increasingly, abuse generated or amplified by artificial intelligence (Henry & Powell, 2018).

Indonesia and South Africa form an instructive comparative pairing. Both are populous Global South democracies with high internet penetration, both record severe levels of gender-based violence, and both enacted landmark digital-era legislation within the relatively short period between 2019 and 2022. In Indonesia, the National Commission on Violence Against Women (Komnas Perempuan) has recorded a steep and sustained rise in reported cases of online gender-based violence, from 16 reported cases in 2017 to well above 1,700 annually by 2021, while civil society monitors such as SAFEnet document a parallel escalation of digital attacks that disproportionately affect women (Komnas Perempuan, 2025; SAFEnet, 2025). Figure 1 charts this trajectory.

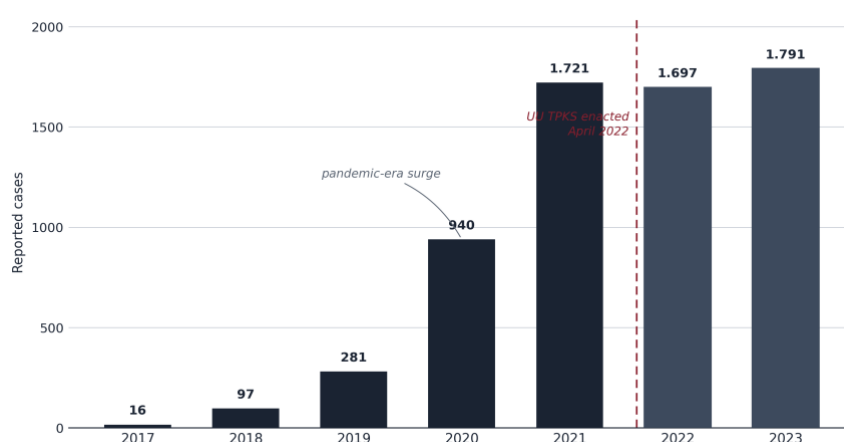


Figure 1. Reported cases of online gender-based violence against women in Indonesia, 2017 to 2023. The dashed line marks the enactment of UU TPKS in April 2022. Source: compiled by the authors from successive editions of Komnas Perempuan, *Catatan Tahunan* (CATAHU). The figures reflect reported cases only and understate actual prevalence.

South Africa presents an equally pressing picture. Gender-based violence and femicide have been declared a national crisis, a recognition embodied in the National Strategic Plan on Gender-Based Violence and Femicide 2020 to 2030, and the scale of gender-based violence has now been measured nationally: the first South African national prevalence study, conducted by the Human Sciences Research Council, found that more than seven million women aged 18 and older had experienced physical violence in their lifetime (Zungu, 2024). The migration of this violence into digital spaces has been documented among South African women generally and among structurally vulnerable groups in particular (Ned et al., 2026).

What has not yet been done, so far as we are aware, is to place the two responses side by side. Indonesian scholarship on the subject has looked inward, assessing the adequacy of the Electronic Information and Transactions Law, the Pornography Law, and, since 2022, the Sexual Violence Crimes Law (Faizah & Hariri, 2022; ICJ, 2023; Stella Hita Arawinda, 2022). South African scholarship has concentrated on the domestic operation of the Cybercrimes Act and its companion instruments. Comparative work on image-based sexual abuse, meanwhile, has concentrated on European and Anglophone jurisdictions (Caletti, 2024; Mania, 2024; Yar & Drew, 2019). The Global South comparative space remains largely unoccupied, which is regrettable because it is precisely in jurisdictions with newer institutions and thinner enforcement capacity that the design choices of a statute matter most.

Three questions guide the analysis. First, how do the Indonesian and South African frameworks define and criminalize online gender-based violence? Second, what protection,

support, and recovery does each framework offer a victim? Third, what can each jurisdiction learn from the other?

The article contributes a first doctrinal comparison of the two post-2019 regimes; it brings a victimological perspective, attentive to secondary victimization and reporting barriers, into an analysis that would otherwise risk becoming an exercise in parallel statutory description; and it distills from the comparison a set of transferable elements for victim-centered regulation in comparable jurisdictions. Section 2 sets out the working concepts. Section 3 describes the method. Section 4 maps the two frameworks. Section 5 compares them and develops the victimological assessment. Section 6 concludes.

We use the term online gender-based violence for gendered harms perpetrated or facilitated through information and communication technologies. Public discourse long treated the paradigmatic harm under the label of revenge pornography. That label has been persuasively criticized for foregrounding the perpetrator's supposed motive and trivializing the injury, and scholarly usage has settled on image-based sexual abuse to describe the nonconsensual taking, creation, or distribution of intimate images, including threats to distribute such images (McGlynn, 2017). Within the wider field, the typology developed by Powell and Henry distinguishes digital sexual harassment, image-based sexual abuse, technology-facilitated sexual aggression or coercion, and gender- or sexuality-based harassment (Henry et al., 2019; Henry & Powell, 2018). To these must be added adjacent forms that recur in both jurisdictions studied here: doxxing, sextortion, cyberstalking, and synthetic sexual imagery of the kind now commonly referred to as deepfake content.

The framing of these harms as gender-based violence, rather than as generic cybercrime, carries legal weight. Under the CEDAW framework, violence directed at a woman because she is a woman, or violence that affects women disproportionately, constitutes discrimination that states must prevent, investigate, punish, and redress (CEDAW Committee, 2017). In both Indonesia and South Africa, the overwhelming majority of reported victims are women and girls, which brings the harms examined here squarely within that obligation.

Doctrinal comparison can establish what two legal systems say. It cannot, by itself, establish what those systems do to and for victims. The analysis therefore proceeds through two victimological ideas. The first is secondary victimization, the further harm inflicted on a victim not by the original offense but by the response to it: disbelief, blame, invasive questioning, and procedural indifference. The phenomenon is documented so consistently in sexual violence cases that it must be treated as a predictable feature of the victim's trajectory rather than an aberration (Pemberton & Mulder, 2025; Wieberneit et al., 2024). Online abuse sharpens each of these mechanisms. The content is permanent and replicable; the evidence is technical, and the burden of preserving it falls on the victim; and the harm is readily dismissed as merely virtual, which invites exactly the minimizing first response that the literature identifies as most damaging.

The second idea is a simple evaluative sequence. Any regulatory regime for online gender-based violence can be assessed at four points: whether it names and proscribes the harm with precision; whether it offers the victim rapid and practical protection, including restriction or removal of the offending content; whether it secures recovery in the form of restitution, rehabilitation, and psychosocial support as a matter of right; and whether it prevents future harm through deterrence, education, and institutional capacity. The attention to shame and to the victim's sense of control draws on victimological research on sexual victimization in Asian settings, including the doctoral work of the third author on sexual molestation in public transportation and the Indonesian pilot of the Asian Passengers' Safety Study, which documented how shame and perceptions of control shape victims' disclosure decisions (Barkhuizen, 2007).

METHOD

The study is doctrinal legal research combining statutory, conceptual, and comparative approaches. The comparison was functional rather than textual. What was compared was not statutory language in isolation but each system's response to a common social problem, namely, the protection of victims of online gender-based violence. This approach is consistent with recent comparative scholarship on image-based sexual abuse (Caletti, 2024; Mania, 2024).

The primary materials for Indonesia were Law No. 12 of 2022 on Sexual Violence Crimes,

Law No. 11 of 2008 on Electronic Information and Transactions, as most recently amended by Law No. 1 of 2024, Law No. 27 of 2022 on Personal Data Protection, Law No. 44 of 2008 on Pornography, and Supreme Court Regulation No. 3 of 2017. For South Africa, the primary materials were the Cybercrimes Act 19 of 2020, the Films and Publications Amendment Act 11 of 2019, the Protection of Personal Information Act 4 of 2013, the Domestic Violence Act 116 of 1998, as amended in 2021, and the National Strategic Plan on Gender-Based Violence and Femicide. Secondary materials comprised peer-reviewed scholarship and institutional reports, including those of Komnas Perempuan and SAFEnet for Indonesia and equivalent South African sources.

Two limitations deserved mention. Both statutory regimes were relatively young, and reported case law under their most relevant provisions remained limited, so conclusions about enforcement rested partly on monitoring data and institutional reports rather than settled jurisprudence. Moreover, because the study was doctrinal, it did not itself generate victimization data. A cross-national empirical study was proposed in the conclusion as the natural sequel.

RESULTS AND DISCUSSION

Results

Indonesia

The Sexual Violence Crimes Law

Law No. 12 of 2022, commonly cited as UU TPKS, is the centerpiece of the Indonesian response, and its significance runs in two directions. Substantively, it is the first Indonesian statute to expressly recognize electronic-based sexual violence, *kekerasan seksual berbasis elektronik*, as a distinct offense. Article 14(1) reaches three forms of conduct: recording or capturing images or screenshots containing sexual content without the consent of the person depicted; transmitting electronic information or documents containing sexual content against the will of the recipient; and stalking or tracking a person through an electronic system for sexual purposes. The basic offense carries imprisonment of up to four years and/or a fine of up to Rp200 million, aggravated under Article 14(2) to six years and/or Rp300 million where the conduct is committed for purposes of extortion, threat, coercion, or deception. The offense is prosecutable upon complaint, except where the victim is a child or a person with a disability, and the statute exempts recording or transmission undertaken in the public interest or in self-defense. The structure captures much of what the international literature classifies as image-based sexual abuse and digital sexual harassment (Faizah & Hariri, 2022).

The procedural and institutional side of the statute is, if anything, more distinctive. UU TPKS codifies victims' rights to handling, protection, and recovery as enforceable entitlements that attach from the reporting of the offense and continue through post-judgment rehabilitation. Under Article 16(1), for any sexual violence offense carrying a penalty of four years or more, the judge must determine the amount of restitution in addition to the principal penalty. Article 35 further provides for a state compensation mechanism, paid through the *Dana Bantuan Korban* (Victim Assistance Fund), where the seized assets of the convicted offender are insufficient to satisfy the restitution award. This mechanism has subsequently been supplemented by Government Regulation No. 29 of 2025 concerning the Victim Assistance Fund. It prohibits the settlement of sexual violence cases outside court, subject to a narrow exception concerning child offenders, and thereby forecloses informal peaceful resolutions that have historically extinguished victims' claims under family and community pressure. It also requires investigators, prosecutors, and judges handling sexual violence cases to meet specified competency and training requirements, provides for victim companions, and restricts retraumatizing lines of questioning.

The Electronic Information and Transactions Law

Before 2022, online gender-based violence was prosecuted, where it was prosecuted at all, under Article 27(1) of the Electronic Information and Transactions Law (UU ITE), which criminalized the distribution, transmission, or making accessible of electronic information or documents containing content that violated decency. The provision has a well-documented pathology. Because it criminalized the dissemination of prohibited content without adequately distinguishing the perpetrator from the person depicted, victims of non-consensual distribution themselves came under investigation and, in some instances, were convicted under it (Safela et

al., 2024; Stella Hita Arawinda, 2022). The 2024 amendment revised the decency provisions, while UU TPKS, as the *lex specialis* governing sexual violence, should in principle channel prosecutions involving sexual violence toward its more specific provisions. Whether charging practice follows that principle is an open question of enforcement rather than doctrine.

Supporting Instruments

Three further instruments complete the picture. The Pornography Law of 2008 has functioned as a second double-edged sword: enacted to suppress pornographic content, it has at times been invoked against the very persons depicted in intimate material, including victims of non-consensual distribution (Adkiras, 2021). The Personal Data Protection Law of 2022 supplies Indonesia's first general data protection regime and is a natural instrument against doxxing and related abuses involving victims' personal data, although its institutional enforcement architecture remains comparatively new. Supreme Court Regulation No. 3 of 2017 directs judges, in adjudicating cases involving women in conflict with the law, to avoid gender stereotyping and victim-blaming reasoning, making it a judicial-culture instrument of particular value in trials where attacks on the victim's credibility are routine.

Institutions

Implementation runs through the Witness and Victim Protection Agency (LPSK), regional technical units for the protection of women and children (UPTD PPA), the SAPA 129 national complaint service, and Komnas Perempuan as the national monitoring body. The principal weakness documented since 2022 has been the staggered development and implementation of the regulatory framework. Although important implementing instruments have now been issued—including Government Regulation No. 27 of 2024 on coordination and monitoring and Government Regulation No. 29 of 2025 on the Victim Assistance Fund—monitoring continues to identify gaps between the statutory framework and implementation at the frontline level (ICJ, 2023; Komnas Perempuan, 2025).

South Africa

The Cybercrimes Act 19 of 2020

The Cybercrimes Act was assented to on 26 May 2021, and its malicious communications provisions have been in operation since 1 December 2021. Part II of Chapter 2 creates three offenses of immediate relevance: data messages that incite damage to property or violence (section 14); data messages that threaten persons with damage to property or violence (section 15); and the disclosure of a data message of an intimate image (section 16). Conviction attracts a fine or imprisonment for up to three years, or both (section 19), and section 17 extends liability to those who attempt, conspire, aid, abet, induce, incite, instigate, instruct, command, or procure the commission of the offense.

Section 16 is the dedicated offense for the non-consensual disclosure of intimate images, and its drafting repays close reading. The offense is committed by a person who unlawfully and intentionally discloses, by means of an electronic communications service, a data message of an intimate image of another person without that person's consent. Three definitional choices give the provision unusual reach. The definition of an intimate image extends to depictions that are real or simulated and made by any means, language broad enough to reach manipulated, drawn, and synthetically generated imagery, a point of considerable comparative significance to which Section 5.1 returns. The protected person includes not only someone identifiable from the image itself but also a person described as being displayed or identifiable from other information, which closes the loophole exploited by perpetrators who circulate content with the victim named in accompanying text. The definition is also conditioned on a reasonable expectation of privacy at the time the data message was made, together with a violation or offense against the person's sexual integrity or dignity, or sexual exploitation, thereby anchoring the offense in privacy, dignity, and sexual integrity rather than in public morality. The provision expressly encompasses female, transgender, and intersex persons in its description of the intimate body.

The Act also confronts two structural problems endemic to online abuse. It extends the jurisdiction of South African courts over offenses with cross-border elements (section 24), which

matters where perpetrators, victims, or relevant conduct are situated abroad. However, an important qualification is necessary concerning section 20. Section 20 provides for a complainant to seek an ex parte protection order pending finalization of criminal proceedings, including an order directing an electronic communications service provider to remove or disable access to the relevant data message. Part VI of Chapter 2, which contains sections 20–23, however, has not yet commenced. Accordingly, the protection-order mechanism is a statutory remedy on the books rather than an operative remedy presently available under the Cybercrimes Act. This distinction is critical to any assessment of the Act's practical protection architecture.

The Films and Publications Amendment Act 11 of 2019

The Cybercrimes Act did not write on a blank slate. The Films and Publications Amendment Act 11 of 2019 created, with effect from 1 March 2022, section 24E of the Films and Publications Act 65 of 1996, which criminalizes the knowing distribution of private sexual photographs and films without the prior consent of the person depicted. Section 24E(1) requires an intention to cause harm and carries a maximum penalty of R150,000 or two years' imprisonment, or both. Section 24E(2), by contrast, applies where the person depicted is identified or identifiable and carries a maximum penalty of R300,000 or four years' imprisonment, or both, without requiring proof of an intention to cause harm. South Africa thus operates a partially overlapping statutory regime for non-consensual intimate images, with the older Films and Publications Act provision differing in important respects from section 16 of the Cybercrimes Act, alongside the complaints and takedown machinery of the Film and Publication Board. How prosecutors choose between the overlapping offenses remains unsettled.

POPIA

The Protection of Personal Information Act 4 of 2013 (POPIA), whose principal enforcement provisions have been fully operative since 1 July 2021, gives legislative effect to the constitutional right to privacy in section 14 of the Constitution. Its relevance to victims is twofold. Doxxing and other malicious processing of a victim's personal information may fall within its regulatory scope, and the Information Regulator provides a complaint avenue outside the criminal process. Scholarship has begun to map the convergence between POPIA and the Cybercrimes Act, observing that the non-consensual processing of intimate data may engage both statutes at once. In practice, however, POPIA remains more of a complementary regulatory instrument than a route victims routinely pursue.

The Domestic Violence Amendment Act 14 of 2021

The Domestic Violence Amendment Act 14 of 2021 expanded the statutory conception of domestic violence to encompass technology-facilitated conduct, including forms of harassment, disclosure of private or sexually harmful electronic communications, unauthorized access, and the monitoring or tracking of a complainant through technology. The relevant provisions commenced on 14 April 2023. Victims of intimate-partner abuse conducted online may therefore obtain domestic violence protection orders where the statutory requirements are met. The resulting framework creates a procedural fork between a domestic violence protection order, the protection-order mechanism contemplated by section 20 of the Cybercrimes Act, and a criminal complaint. The difficulty is that the section 20 mechanism under the Cybercrimes Act has not yet commenced, whereas the domestic violence protection-order framework is operative.

Institutions

Enforcement runs through the South African Police Service and the National Prosecuting Authority, supported by the Thuthuzela Care Centres, the one-stop interdisciplinary facilities for sexual-offense victims designed to reduce secondary victimization; the network of sexual-offenses courts; the Film and Publication Board; and the Information Regulator, all framed by the National Strategic Plan. The weakness that monitoring consistently records is not architectural but operational: enforcement of gender-based violence legislation lags well behind its ambition, and digital-forensic capacity in policing remains limited.

Recent South African victimization research illustrates the breadth of the phenomenon

these institutions must govern. Figure 2 presents the prevalence of forms of technology-facilitated gender-based violence reported in a recent baseline study of South African women with disabilities, a structurally vulnerable group, in which cyberbullying, hate speech, and hacking emerged as the most common experiences (Ned et al., 2026).

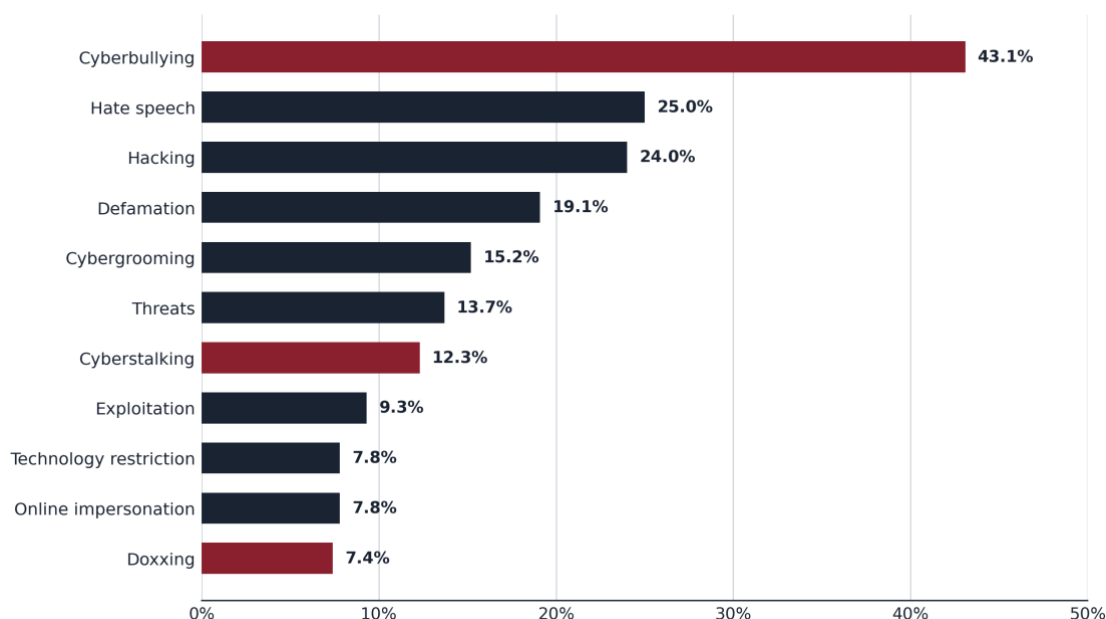


Figure 2. Prevalence of forms of technology-facilitated gender-based violence among South African women with disabilities (n = 204). Source: adapted by the authors from Ned, Tyabashe-Phume, Tunggal, and Soldatić (2026). Highlighted bars indicate the forms most directly governed by the provisions discussed in this article.

Table 1

Principal legal instruments governing online gender-based violence in Indonesia and South Africa

Dimension	Indonesia	South Africa
Core offence	Electronic-based sexual violence, Art. 14 UU TPKS: non-consensual recording, non-consensual transmission, electronic stalking	Disclosure of an intimate image, s 16 Cybercrimes Act; distribution of private sexual images with intent to harm, s 24E FPAA
Synthetic imagery	No express coverage; interpretive extension only	Express: an intimate image includes real or simulated depictions made by any means
Penalty	Up to 4 years and/or Rp200 million (Art. 14(1)); up to 6 years and/or Rp300 million if aggravated (Art. 14(2))	Fine and/or up to 3 years (s 19 CCA); R150,000/2 years, doubled where the victim is identifiable (s 24E FPAA)
Pre-conviction protection	Victim rights attach from complaint, but no dedicated content-restriction order	s 20 protection order on prima facie evidence, including orders restricting further availability; DV Act orders for intimate-partner abuse
Recovery	Mandatory restitution on conviction; state backstop contemplated; rehabilitation rights	No integrated statutory recovery charter; support through the TCC service model and general policy
Informal settlement	Prohibited by statute	Not addressed by statute
Data protection	UU PDP (Law No. 27 of 2022)	POPIA (Act 4 of 2013)

Dimension	Indonesia	South Africa
Risk of use against victims	Art. 27(1) UU ITE and the Pornography Law have been applied to persons depicted	Breadth of the malicious communications offences; unsettled CCA/FPAA overlap
Institutions	LPSK, UPTD PPA, SAPA 129, Komnas Perempuan	SAPS, NPA, Thuthuzela Care Centres, sexual offences courts, FPB, Information Regulator

Source: compiled by the authors from the instruments cited in Section 4.

Comparative Analysis

The Scope of Criminalization

The clearest contrast between the two systems lies in how each names the harm. Section 16 of the Cybercrimes Act is a purpose-built offense whose elements—unlawful and intentional disclosure, a data message, an intimate image, and absence of consent—map directly onto the wrong as victims experience it, and whose placement among malicious communications avoids the moralizing register of decency and pornography offenses. Article 14 of UU TPKE is broader. It reaches non-consensual recording and electronic stalking as well as transmission, and it sits within a statute whose entire architecture is protective of victims. Breadth, however, is bought at the price of granularity. The compressed drafting of Article 14 leaves some questions concerning the outer boundary of electronic-based sexual violence, and its relation to surviving offenses under older statutes, to prosecutorial discretion and eventual jurisprudence, which in Indonesian practice has contributed to inconsistent charging.

On synthetic sexual imagery, the comparison is asymmetric, and the advantage lies with South Africa. Section 16 extends in terms to depictions that are real or simulated and made by any means, giving prosecutors a statutory foothold against deepfake content, although the offense reaches disclosure rather than creation or possession, and the provision's application to synthetic imagery remains judicially untested. Indonesian law contains no comparable express language. Deepfake abuse must therefore be addressed, if at all, through the interpretation of Article 14, other provisions of UU TPKE, or related statutes, and Indonesian scholarship has begun to identify abuse mediated by artificial intelligence as a regulatory blind spot. Neither framework cleanly addresses all forms of cyberflashing or gendered hate speech that fall short of a threat.

One further point belongs under criminalization because it is a design question rather than an enforcement one. Both jurisdictions carry a documented risk of criminal provisions being turned against the people they should protect. In Indonesia, the risk has materialized through decency and pornography offenses. In South Africa, it lies in the potential breadth of the malicious communications provisions. A victim-centered assessment must treat this inversion risk as a first-order flaw of drafting, not merely as an accident of implementation (McGlynn, 2017).

Protection and Recovery

If South Africa prevails on offense specificity, Indonesia has the more developed victim architecture. UU TPKE constructs a comparatively integrated pathway. Rights to handling, protection, and recovery attach from the reporting of the offense; restitution is mandatory on conviction for offenses carrying a sentence of four years or more; the state provides compensation through the Victim Assistance Fund where the offender's seized assets are insufficient; informal settlement is barred except where the offender is a child; and the procedural rules restrict retraumatizing treatment. Indonesia also expressly recognizes a victim's right to the removal of sexually charged content in cases of sexual violence involving electronic media, while Article 46 authorizes the central government to remove or block access to electronic information or documents containing sexual violence offenses. South African legislation contains no equivalent integrated statutory charter. Victim support is distributed across the Domestic Violence Act, the Cybercrimes Act's uncommenced protection-order provisions, the service model of the Thuthuzela Care Centres, and general victim policy.

The South African model nonetheless contains a potentially important front-end innovation in section 20 of the Cybercrimes Act. A victim of intimate-image disclosure can, under the statutory design, seek an ex parte order without awaiting a criminal conviction, including an

order directed at a service provider to remove or disable access to the relevant message. The critical qualification, however, is that Part VI of Chapter 2, including section 20, has not yet commenced. The remedy therefore represents an important legislative design feature rather than an operative remedy. By contrast, the Indonesian framework expressly recognizes content removal as a victim right and gives the government statutory authority to remove or block access, although the effectiveness and speed of that mechanism remain questions of implementation.

The data protection statutes mirror one another in function. UU PDP and POPIA each supply regimes relevant to doxxing and each provide institutional mechanisms for data-protection complaints. Each remains, however, a complementary instrument rather than a substitute for a specialized framework governing gender-based violence.

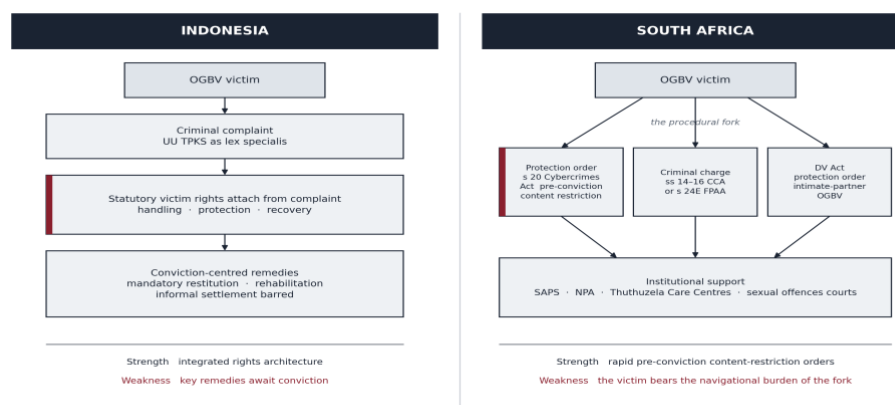


Figure 3. Victim remedial pathways under the two frameworks. Indonesia offers a single integrated but conviction-centred pathway; South Africa offers rapid pre-conviction remedies at the cost of a procedural fork that the victim must navigate. Source: compiled by the authors from the instruments cited in Section 4.

Enforcement

The two systems converge most strongly in their weaknesses. In Indonesia, the staggered development of implementing regulations and continuing institutional-capacity problems have meant that a victim-centered statute is administered by institutions still adapting to the new framework. Monitoring bodies continue to record complaints redirected into mediation, declined for insufficient evidence, or charged under provisions that UU TPKS was intended to displace (ICJ, 2023; Komnas Perempuan, 2025). At the same time, the regulatory framework has materially developed since 2024, and the existence of implementing regulations should be distinguished from the continuing problem of uneven implementation. In South Africa, sophisticated statutory provisions confront chronic constraints in digital-forensic policing and prosecutorial capacity, while the Cybercrimes Act's section 20 protection-order mechanism remains uncommenced.

Three shared structural problems stand out. The evidentiary burden falls heavily on victims, since the practical work of preserving screenshots, metadata, account information, and other digital traces is often left to the person least equipped and most distressed. Remedies also depend substantially on platforms and intermediaries because removal of content, the relief victims most urgently need, requires cooperation from entities operating outside or across national jurisdictions. Finally, statutory victim-centeredness collides, in both countries, with institutional cultures in which online abuse may be treated as trivial, private, or self-inflicted.

Secondary Victimization

Assessed against the framework of Section 2.2, both systems reproduce conditions conducive to secondary victimization, although in different registers. In Indonesia, the phenomenon has taken its starkest legal form. The documented pattern of victims being investigated, and occasionally charged, under Article 27(1) and the Pornography Law for content distributed without their consent means that the protective apparatus itself has operated as an instrument of harm, which the victimological literature would describe as a severe form of

institutional betrayal. Beneath the legal layer lie the cultural strata familiar from Indonesian victimization research: shame, family honor, and victim-blaming norms that suppress disclosure, compounded in the online setting by the knowledge that reporting cannot necessarily undo distribution and may widen the audience. UU TPKS answers this diagnosis directly. Its bar on informal settlement, its trained-investigator requirements, its victim-assistance provisions, and its restrictions on retraumatizing questioning are, in design terms, devices against secondary victimization. The continuing gap between statutory guarantees and frontline implementation means that these safeguards are not yet applied uniformly across institutions (ICJ, 2023; Komnas Perempuan, 2025).

In South Africa, secondary victimization is documented at the police-station threshold and within court processes, notwithstanding an institutional model—the Thuthuzela Care Centres and the sexual-offences courts—built expressly to counter it. For online abuse specifically, victims may encounter officials who are insufficiently trained in digital evidence, and a dismissive first response to an intimate-image complaint functions, in victimological terms, no differently from disbelief of a rape complaint. The procedural complexity of the South African framework adds a distinct burden: although section 20 of the Cybercrimes Act would provide a dedicated route for protection orders if brought into operation, victims must currently navigate the operative domestic-violence framework and other available remedies. Victimological research on sexual victimization in transit and public settings has long shown that shame and the victim's perceived control over the situation govern disclosure decisions Barkhuizen (2007) and Henry et al. (2019), and both mechanisms operate with particular force where the abusive material itself persists online.

The comparative observation that emerges is that statutory design can either mitigate or manufacture secondary victimization. Indonesia has embedded more of the mitigating devices directly in the statute, including content-removal rights and an integrated victim-rights framework, but still faces institutional and implementation gaps. South Africa possesses specialized institutional mechanisms and a carefully drafted intimate-image offense, but distributes protection across several instruments, while a significant Cybercrimes Act remedy remains uncommenced. Each system holds, in developed form, an element the other lacks.

Reciprocal Lessons

The comparison yields lessons in both directions rather than a ranking. Table 2 consolidates the assessment.

Table 2

Assessment of the two frameworks against the four-stage victim-centred sequence

Stage	Indonesia	South Africa	Stronger regime
Criminalisation	Broad but compressed; no express deepfake coverage; older victim-hostile provisions survive	Precise offence for intimate images, extending to simulated content; unsettled two-statute overlap	South Africa
Protection	Rights attach from complaint, but no dedicated content-restriction order	Pre-conviction protection orders, including against service providers	South Africa
Recovery	Integrated statutory charter: restitution, rehabilitation, state backstop; informal settlement barred	Distributed across the service model and policy; no statutory charter	Indonesia
Prevention and capacity	Implementing-regulation lag; institutions in transition	Strong service model; chronic enforcement and forensic deficits	Neither

Source: the authors' analysis, Sections 4 and 5.

From South Africa, Indonesia can take three elements: a dedicated and precisely drafted offense for non-consensual intimate images that expressly encompasses synthetic imagery, whether by amendment or interpretive clarification, so that definitional ambiguity is reduced and charging under victim-hostile provisions is further foreclosed; a fully operational interim protection mechanism for online harms, including orders directed at service providers; and express jurisdictional rules for offenses with cross-border elements.

From Indonesia, South Africa can take three others: a more integrated statutory charter of victim rights that attaches from the reporting of the offense rather than being distributed across instruments and policy; a restitution and state-compensation architecture with a clear backstop; and a statutory restriction on the informal settlement of sexual violence cases.

Taken together, these elements describe a victim-centered model of regulation for jurisdictions in a comparable position: name the harms precisely, in provisions that cannot be inverted against victims; protect before conviction, including through rapid content-restriction mechanisms binding on intermediaries; guarantee recovery as of right, with the state as backstop; prevent informal disposal of sexual violence cases; and invest in institutional capacity and culture, without which the first four elements remain guarantees on paper.

CONCLUSION

This article asked how Indonesia and South Africa define, criminalize, and remedy online gender-based violence, and what each can learn from the other. The answers may be stated briefly. On definition, South African law names the paradigmatic harm with a precision Indonesian law has not yet achieved, and its express extension to simulated imagery anticipates a threat that Indonesian law does not expressly address, while Indonesian law casts the wider substantive net but leaves some boundaries unsettled. On protection and recovery, Indonesia has built the more complete architecture on paper, with enforceable victim rights, mandatory restitution, content-removal mechanisms, and a bar on informal settlement, while South Africa has designed a specialized pre-conviction protection-order mechanism whose potential practical value is considerable but whose relevant Cybercrimes Act provisions have not yet commenced. On enforcement, the systems converge in weakness: regulatory and implementation gaps, capacity deficits, evidentiary burdens borne by victims, dependence on platforms and intermediaries, and institutional cultures that can reproduce secondary victimization.

Neither regime suffices alone. The strongest available model combines South African precision in criminalization with the Indonesian architecture of victim protection and recovery, delivered through institutions trained and resourced to apply both. For the two legislatures, the immediate agenda includes express provision for synthetic imagery and doxxing, stronger statutory duties of platform accountability, continued consolidation of implementing mechanisms in Indonesia, operationalization of South Africa's section 20 protection-order framework, and sustained investment in specialized enforcement capacity in both countries.

The natural sequel to this doctrinal study is empirical: a cross-national victimization survey applying a common instrument in both countries to measure prevalence, reporting behavior, and victims' experiences of the frameworks compared here. The present authors intend this article as the first part of that agenda.

ACKNOWLEDGEMENT

The authors would like to express sincere gratitude to Institut Islam Kuningan for the institutional support provided during the preparation of this research. The author also acknowledges the contribution of the legal and institutional sources consulted in developing the comparative analysis of online gender-based violence in Indonesia and South Africa.

AUTHOR CONTRIBUTION STATEMENT

Rani Santika: conceptualization, development of the research framework, methodology, comparative legal analysis, interpretation of findings, drafting and writing of the manuscript, revision, final approval of the submitted version, and correspondence with the journal.

Rafi Farizki: literature and legal document review, data curation of Indonesian statutes and policy materials, drafting of the sections on the Indonesian legal framework, and revision of

the manuscript.

Jaco Barkhuizen: supervision, validation of the victimological and criminological framework, critical review of the analysis of South African legislation, and substantive revision of the manuscript for important intellectual content.

Ade Fitri Fatimah: literature review, verification of references and legal sources, editing and formatting of the manuscript, and revision of the final version.

All authors have read and approved the final version of the manuscript.

REFERENCES

- Adkiras, F. (2021). Konstruksi Hukum Perlindungan Korban Kekerasan Berbasis Gender Online Menurut Hukum Hak Asasi Manusia. *Jurnal Lex Renaissance*, 6(2). <https://doi.org/10.20885/JLR.vol6.iss2.art12>
- Barkhuizen, J. (2007). *Sexual Molestation on Public Transportation: A Victimological Approach*. Unpublished Doctoral Dissertation, Mito: Tokiwa University.
- Barter, C., & Koulu, S. (2021). Digital technologies and gender-based violence – mechanisms for oppression, activism and recovery. In *Journal of Gender-Based Violence* (Vol. 5, Number 3). <https://doi.org/10.1332/239868021X16315286472556>
- Caletti, G. M. and K. S. (2024). *Criminalizing Intimate Image Abuse: A Comparative Perspective*. Oxford University Press.
- CEDAW Committee. (2017). General Recommendation No. 35 on gender-based violence against women, updating General Recommendation No. 19. UN Doc CEDAW/C/GC/35.
- Dunn, S. (2020). Technology-Facilitated Gender-Based Violence: An Overview. *Canadian Journal of Women and the Law*, 30(1).
- Faizah, A. F., & Hariri, M. R. (2022). Pelindungan hukum terhadap korban revenge porn sebagai bentuk kekerasan berbasis gender online ditinjau dari undang-undang nomor 12 tahun 2022 tentang tindak pidana kekerasan seksual. *Jurnal Hukum Lex Generalis*, 3(7), 520–541.
- Henry, N., Flynn, A., & Powell, A. (2019). Image-based sexual abuse: Victims and perpetrators. *Trends and Issues in Crime and Criminal Justice*, (572). <https://doi.org/10.52922/ti09975>
- Henry, N., & Powell, A. (2018). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence, and Abuse*, 19(2). <https://doi.org/10.1177/1524838016650189>
- International Commission of Jurists. (2023). Indonesia: Law No. 12 of 2022 on Sexual Violence Crimes and Online Gender-Based Violence. Briefing Paper. Geneva: ICJ.
- Komnas Perempuan. (2025). Catatan Tahunan Kekerasan terhadap Perempuan (CATAHU). Jakarta: Komnas Perempuan.
- Mahkamah Agung Republik Indonesia. Peraturan Mahkamah Agung Nomor 3 Tahun 2017 tentang Pedoman Mengadili Perkara Perempuan Berhadapan dengan Hukum.
- Mania, K. (2024). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study. In *Trauma, Violence, and Abuse* (Vol. 25, Number 1). <https://doi.org/10.1177/15248380221143772>
- McGlynn, C. E. R. and R. H. (2017). Beyond ‘revenge porn’: The continuum of image-based sexual abuse. *Feminist Legal Studies*, 25(1), 25–46.
- Ned, L., Tyabashe-Phume, B., Tungal, E., & Soldatić, K. (2026). A Baseline Quantitative Analysis of Technology-Facilitated Gender-Based Violence Against Women with Disabilities in South Africa. *Behavioral Sciences*, 16(5). <https://doi.org/10.3390/bs16050745>
- Pemberton, A., & Mulder, E. (2025). Bringing injustice back in: Secondary victimization as epistemic injustice. *Criminology and Criminal Justice*, 25(4). <https://doi.org/10.1177/17488958231181345>
- Republik Indonesia. Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual.
- Republik Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Republik Indonesia. Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi.
- Republic of South Africa. Cybercrimes Act 19 of 2020.

- Republic of South Africa. Films and Publications Amendment Act 11 of 2019.
- Republic of South Africa. Protection of Personal Information Act 4 of 2013.
- Republic of South Africa. Domestic Violence Act 116 of 1998.
- Republic of South Africa. Domestic Violence Amendment Act 14 of 2021.
- Republic of South Africa. National Strategic Plan on Gender-Based Violence and Femicide 2020 to 2030.
- Safela, A. W., Mahmud, H., & Dewi, N. (2024). PERLINDUNGAN HUKUM TERHADAP KORBAN KEKERASAN BERBASIS GENDER ONLINE (KBGO) DITINJAU DARI UU ITE. *JURNAL DIMENSI*, 13(1), 139–150. <https://doi.org/10.33373/dms.v13i1.6051>
- SAFEnet. (2025). Laporan Situasi Hak-Hak Digital Indonesia. Denpasar: SAFEnet.
- Stella Hita Arawinda. (2022). Perlindungan Hukum Terhadap Perempuan Korban Kekerasan Berbasis Gender Online di Indonesia. *JURNAL YUSTIKA: MEDIA HUKUM DAN KEADILAN*, 24(02). <https://doi.org/10.24123/yustika.v24i02.4599>
- Wieberneit, M., Thal, S., Clare, J., Notebaert, L., & Tubex, H. (2024). Silenced Survivors: A Systematic Review of the Barriers to Reporting, Investigating, Prosecuting, and Sentencing of Adult Female Rape and Sexual Assault. *Trauma, Violence, & Abuse*, 25(5), 3742–3757. <https://doi.org/10.1177/15248380241261404>
- Yar, M., & Drew, J. (2019). Image-based abuse, non-consensual pornography, revenge porn: A study of criminalization and crime prevention in Australia and England & Wales. *International Journal of Cyber Criminology*, 13(2). <https://doi.org/10.5281/zenodo.3709306>
- Zungu, N. P. (2024). *The first South African national gender-based violence study, 2022: a baseline survey on victimisation and perpetration*.