



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

BEYOND ISOLATED INCIDENTS: TECHNOLOGY, FACILITATED COERCIVE CONTROL AND THE FRAGMENTATION OF LEGAL RESPONSE IN INDIA, THE UNITED KINGDOM, AND INTERNATIONAL LAW

~ *Sharanya Das*

ABSTRACT

Domestic violence law has historically been organised around the discrete incident. Evan Stark's theory of coercive control and Liz Kelly's continuum of sexual violence together displaced this model, showing that the harm of intimate, partner abuse lies less in any single act than in a cumulative pattern of domination, isolation, surveillance, and restriction of autonomy. Digital technology has since become a principal instrument through which that pattern is sustained, allowing partners and Ex, partners to monitor location, finances, and communication long after physical proximity and even physical separation would once have ended the abuse. This paper argues that legal systems continue to conceptualise technologically facilitated abuse through the vocabulary of isolated offences – a captured image, a threatening message, an act of impersonation – even where the technology sustains a continuing relationship of control. Examining India's constitutional, criminal, cyber, and domestic violence statutes alongside the United Kingdom's offence of controlling or coercive behaviour and the international standards set by CEDAW, UN Women, and the Council of Europe's 2026 Recommendation on technology, facilitated violence, the paper contends that the deeper legal problem is not the absence of law but its fragmentation: one continuing experience of digital coercive control is split across criminal law, cyber law, and family law, forcing survivors to translate a single relationship of domination into several unconnected legal claims.

I. Introduction

In February 2018, an Orissa court held a man criminally liable for creating a fake social media profile in the name of a woman he had once proposed to marry, populating it with

morphed nude photographs and obscene messages sent to her family over an extended period.¹ A year earlier, a West Bengal court convicted a man of uploading intimate images of his former partner to a pornography website after she refused to continue seeing him – images he had covertly copied from her phone during the relationship and later used to blackmail her.² Both cases were charged and reported as cybercrime – stalking, obscenity, privacy violation. Neither was framed, in law, as what the underlying relationship actually was: a sustained pattern of surveillance and control exercised by an intimate partner through the ordinary instruments of modern life a phone, a social media account, a shared password.

This paper builds on a body of feminist criminological theory, developed before the smartphone existed, that identified precisely this gap between incident and pattern. Evan Stark's theory of coercive control reframed domestic abuse as a liberty crime rather than a crime of assault, arguing that a singular focus on injury obscures the more devastating reality of a relationship organised around domination.³ Liz Kelly's earlier concept of a continuum of sexual violence made a structurally similar point: harm cannot be sorted into discrete categories of “offence” and “non,offence”, because typical and aberrant behaviour shade into one another along a single continuum.⁴ Both theories share one diagnostic insight this paper treats as its foundation: acts that look insignificant in isolation acquire severity only when read cumulatively, as a pattern restricting another person's autonomy.

Digital technology does not create a new category of harm so much as it supplies coercive control with a formidable new set of instruments – GPS data, spyware, financial applications, smart,home devices, near,permanent social connectivity – while erasing the one limitation that has always contained coercive control within a shared home: physical proximity. UN Women now treats technology,facilitated violence against women and girls (TF VAWG) as inseparable from this continuum, defining it as any act committed, assisted, aggravated, or amplified through digital tools that results in, or is likely to result in, physical, sexual, psychological, social, political, or economic harm.⁵ The question this paper investigates is whether domestic

¹Kalandi Charan Lenka v State of Odisha, BLAPL No 7596 of 2016, Orissa High Court, judgment dated 16 January 2017 (Choudhury J).

²State of West Bengal v Animesh Boxi, GR No 1587/17, Judgment of the Judicial Magistrate, 1st Class, 3rd Court, Tamluk, Purba Medinipur, dated 7 March 2018.

³Evan Stark, *Coercive Control: The Entrapment of Women in Personal Life* (Oxford University Press 2007).

⁴Liz Kelly, *Surviving Sexual Violence* (Polity Press 1988); Liz Kelly, 'Standing the Test of Time? Reflections on the Concept of the Continuum of Sexual Violence' in Jennifer M Brown and Sandra L Walklate (eds), *Handbook on Sexual Violence* (Routledge 2012).

⁵UN Women, *UN Women Strategy on Preventing and Eliminating Technology,Facilitated Violence against Women and Girls* (2025).

legal systems have caught up with that framing, or remain organised, as Stark warned in 2007, around the injury model his theory was written to displace.

The paper proceeds in four movements. Part II develops the theoretical scaffolding – coercive control, the continuum of violence, and the analytical chain by which a technological act (GPS tracking) converts into behavioural control (restriction of movement, and eventually entrapment). Part III examines India's constitutional, criminal, cyber, and domestic violence framework, asking of each provision whether it recognises an isolated act or a continuing pattern. Part IV turns to the United Kingdom, whose offence of controlling or coercive behaviour offers the clearest comparative model for a pattern-based, method-neutral response, and whose post-separation abuse literature offers the strongest evidence for why incident-based law is inadequate. Part V places both jurisdictions against the international standards articulated by CEDAW, UN Women, and the Council of Europe's 2026 Recommendation on accountability for technology-facilitated violence – the first international instrument devoted specifically to this subject.⁶ Part VI synthesises the comparison into a single argument: the deeper legal problem is not the absence of law, but the persistence of an offence-based vocabulary that fragments one continuing relationship of control across unconnected areas of law.

II. Theoretical Foundations: From Incidents to Patterns

A. Coercive Control and the Sociology of Entrapment

Before Stark, the dominant “injury model” of domestic violence law measured abuse by the severity of a discrete physical act – a punch, a broken bone, a hospital record. Stark's central contribution was to show that this model captures only a fraction, and frequently the less consequential fraction, of what victims experience.⁷ Coercive control, in his account, is a course of conduct built around intersecting tactics of intimidation, isolation, surveillance, and the regulation of everyday life: dictating whom a partner may see, what she may wear, how she spends money, when she may leave the house.⁸ Stark describes coercion (force or threats compelling a response) combined with control (structural deprivation compelling indirect

⁶Council of Europe, Recommendation CM/Rec(2026)2 of the Committee of Ministers to Member States on Accountability for Technology-Facilitated Violence against Women and Girls (adopted 2026).

⁷Stark (n 2) chs 3–4.

⁸Stark (n 2) ch 7 ('The Theory of Coercive Control').

obedience) as producing a “condition of unfreedom” experienced as entrapment – a state closer to hostage-taking than to an assault charge.⁹

The significance for this paper is structural. If abuse is a pattern of domination, a legal system that recognises only discrete, injurious acts will under-protect its victims, because most tactics sustaining the pattern – a demand for a password, a check on a location history – are lawful, or unremarkable, in isolation. Only their repetition and cumulative function convert them into abuse. Stark's own closing chapter, “The Technology of Coercive Control”, anticipated in 2007 that the instruments of domination would keep expanding; his account is now cited as one basis for pattern-based offences such as the United Kingdom's controlling, or, coercive, behaviour provision, discussed in Part IV.¹⁰

B. The Continuum of Violence

Liz Kelly's continuum framework, developed a generation before Stark, made a related argument: legal definitions of sexual violence, built around discrete prosecutable offences, fail to capture harm that runs from pressure, to harassment, to assault, without a clean break between what the law criminalises and what it ignores.¹¹ The concept now describes violence against women generally: a spectrum from everyday controlling behaviour, through psychological and economic abuse, to physical and sexual violence, in which forms of harm are interconnected rather than categorically separate.¹² UN Women has adopted this framing for its own work, situating TF VAWG within the wider “EVAW continuum” and treating digital violence as closely connected to offline violence rather than a separate online phenomenon.¹³

The originality this paper claims lies in joining Kelly's continuum to a second continuum running from offline to online. The everyday controlling behaviour Kelly located on a spectrum toward physical violence also runs along a second axis, from a request to share a location “just in case”, through covert tracking, to the digital surveillance that in aggregate constitutes coercive control. A single instance of checking a partner's phone and a sustained campaign of

⁹Stark (n 2) 205, 228–229; Lauren Bennett Cattaneo, 'Rethinking Coercive Control' (2009) 15 Violence Against Women.

¹⁰Stark (n 2) ch 8; Cattaneo (n 6), noting Stark's book as foundational to the UK offence.

¹¹Kelly, *Surviving Sexual Violence* (n 3) 74–137.

¹²Kelly (n 3), as applied in Women's Aid Scotland, *The Concept of a Continuum of Violence against Women* (2022).

¹³UN Women, *UN Women Strategy* (n 4).

spyware surveillance cannot be neatly separated on this axis: both are points on the same line of escalating control.

C. Technology as an Instrument of Coercive Control: The Analytical Chain

The claim that technology “facilitates” coercive control requires an account of the mechanism converting a technological act into a psychological constraint. This paper adopts a simple chain: a technological capability (GPS tracking) enables surveillance; surveillance restricts the victim's actual or perceived freedom of movement; that restriction produces fear; and fear produces behavioural modification the victim acts as though watched, whether or not she is, at that moment, being watched. The chain's end, state is coercive control in Stark's sense: a condition of unfreedom sustained without any single injurious act.

Empirical research documents each stage across a consistent set of tactics: spyware and concealed trackers for location surveillance; unauthorised access to email, banking, and social accounts through previously shared passwords or unrevoked family, sharing settings; smart, home devices repurposed for covert monitoring; fake accounts and impersonation; and non, consensual capture or distribution of intimate images, used both as a surveillance tool during the relationship and a coercive threat after it ends.¹⁴ None of these tactics need be independently unlawful to perform a controlling function: a request to share location is not, without more, an offence anywhere discussed in this paper. Offence, based frameworks are consequently weakest exactly where coercive control is strongest – in the accumulation of lawful or borderline acts into a pattern of domination.

III. India: Fragmented Recognition of a Unified Pattern

India's legal response to technology, facilitated coercive control is distributed across four bodies of law that were drafted for different purposes at different times: the Constitution's fundamental rights jurisprudence, the general criminal law now consolidated in the Bharatiya Nyaya Sanhita, 2023 (BNS), the cyber, specific provisions of the Information Technology Act, 2000 (IT Act) and its 2021 intermediary rules, and the civil, remedial architecture of the Protection of Women from Domestic Violence Act, 2005 (PWDVA). Examined individually, each body of law contains provisions capable of reaching particular tactics of digital coercive control. Examined together, they reveal a structural pattern: Indian law is competent to punish or

¹⁴The Cyber Helpline, 'What is Tech Facilitated Abuse? A Guide to Online Gender, Based Violence' (2025); Lisa Sugiura and others, 'The Technification of Domestic Abuse: Methods, Tools and Criminal Justice Responses' (2026) *Criminology & Criminal Justice*.

restrain the instrument – the image, the message, the act of monitoring but has no single provision, outside the general and still under-tested language of the PWDVA, designed to recognise the underlying relationship of control.

A. The Constitutional Framework: Privacy, Dignity, and Autonomy

The Supreme Court's nine-judge decision in Justice K.S. Puttaswamy (Retd) v Union of India supplies the constitutional vocabulary within which any Indian argument about digital coercive control must be built. The Court unanimously held that privacy is a fundamental right located principally within Article 21 but reinforced by Articles 14 and 19, protecting not mere secrecy but “the ability to make decisions on matters fundamental to personal life” bodily integrity, informational self-determination, and decisional autonomy.¹⁵ The Court held that any invasion of privacy must satisfy tests of legality, necessity, and proportionality a standard built for state surveillance, but whose underlying values map directly onto intimate, partner digital surveillance, even where the perpetrator is a private individual.

Articles 21, 19, and 14 together supply a normative case that coercive digital surveillance is a constitutional harm independent of physical injury. The difficulty is that this vocabulary has not yet become a freestanding cause of action treating sustained digital surveillance as an autonomous wrong; Puttaswamy's language of dignity and autonomy currently informs reasoning about individual offences, as in the revenge, pornography case discussed below, rather than supplying an independent remedy for coercive control as such.

B. Criminal Law: The Bharatiya Nyaya Sanhita, 2023

Section 78 of the BNS, replacing section 354D of the Penal Code, criminalises stalking in two forms: physically following and repeatedly contacting a woman despite clear disinterest, and monitoring her use of the internet, email, or electronic communication.¹⁶ Courts applying the equivalent IPC provision had already held that physical proximity is not essential to stalking, and that cyberstalking is simply stalking by digital means a welcome recognition of the online–offline continuum described in Part II.¹⁷ Voyeurism (section 77) and criminal intimidation by an anonymous or concealed identity (section 351(4)) supply further discrete offences reaching individual tactics of technology-facilitated abuse.¹⁸

¹⁵Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (nine-judge bench).

¹⁶Bharatiya Nyaya Sanhita 2023, s 78(1)–(2).

¹⁷Discussed in 'Section 78 BNS: Cyberstalking, Gender and Digital Evidence in Contemporary India' (2026) International Journal of Law, Law and Legal Studies.

¹⁸Bharatiya Nyaya Sanhita 2023, ss 77, 351(4).

The limitation common to these provisions is that each is built around a discrete act, or repetition of the same act following, monitoring, capturing an image, uttering a threat – rather than the relationship of domination those acts may sustain. Section 78 comes closest to a pattern-based offence, but remains defined by the character of the acts rather than their cumulative effect on autonomy, and does not extend, as the UK's coercive behaviour offence does, to tactics that are not acts of contact or monitoring at all controlling a partner's digital finances, for instance, or misusing smart home devices.

C. The Information Technology Act, 2000 and the Intermediary Guidelines Rules, 2021

The IT Act targets the digital instrumentality of abuse directly. Section 66E penalises intentional capture, publication, or transmission of images of a person's private area without consent – inserted in 2008 for digital voyeurism, and read by courts as reinforced by Article 21 following *Puttaswamy*.¹⁹ Sections 67 and 67A criminalise obscene and sexually explicit electronic material; sections 66C and 66D criminalise identity theft and impersonation – directly relevant to the fake profiles and morphed images recurring in the case law below.²⁰

The 2021 Intermediary Guidelines Rules add a platform-facing layer: intermediaries must acknowledge complaints within twenty-four hours, resolve them within fifteen days, take down content within thirty-six hours of a valid order, and “significant social media intermediaries” must appoint a resident grievance officer.²¹ As with the BNS, the limitation is one of unit of analysis: sections 66E, 66C, 66D, 67, and 67A, and the Rules' grievance mechanism, are content, and transaction-specific each targets a particular image or account, not a course of conduct. None of this machinery asks whether a given image or message was one instalment in an ongoing campaign of control.

D. The Protection of Women from Domestic Violence Act, 2005

The PWDVA is, on its text, the one Indian statute already built around a continuing relationship. Section 3 defines domestic violence as any act, omission, or conduct that harms or endangers the aggrieved person's well-being, expressly including physical, sexual, verbal and emotional, and economic abuse covering insult and humiliation, economic

¹⁹Information Technology Act 2000, s 66E; Rahul Kailas Bharati, 'Violation of Privacy in Cyberspace (Section 66E of the IT Act, 2000)' (2025).

²⁰Information Technology Act 2000, ss 66C, 66D, 67, 67A.

²¹Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rr 3, 4.

abuse covering deprivation of financial resources.²² A magistrate may grant protection, residence, monetary relief, and compensation orders, ideally within sixty days.²³

Because emotional and economic abuse are not confined to any method, they are wide enough, as a matter of statutory language, to reach spyware, enabled tracking, digital financial control, or covert monitoring, provided these endanger well, being within the meaning of section 3. What is presently missing the clearest doctrinal gap this paper identifies is a reported decision squarely applying these categories to a pattern of digital surveillance. The statutory raw material already exists; what has not occurred is the judicial or legislative act of naming it.

E. Judicial Recognition: Isolated Offence or Continuing Pattern?

The two most significant reported decisions illustrate both the competence and the limitation of the existing framework. In Kalandi Charan Lenka, the accused subjected the victim to a sustained campaign anonymous obscene messages, defamatory pamphlets at her college and hostel, and a fake Facebook profile bearing morphed nude photographs. The Orissa High Court, denying bail, found him prima facie guilty of an offence combining stalking, forgery, criminal intimidation, and insult to modesty under the Penal Code together with identity theft, impersonation, and obscenity under the IT Act.²⁴ In Animesh Boxi, India's first reported “revenge pornography” conviction, the accused obtained intimate images during a three-year relationship, blackmailed the victim, and uploaded the images with identifying information when she refused him. The trial court imposed five years' imprisonment, expanded “injury” to include reputational and psychological harm, directed compensation comparable to that of a sexual assault survivor, and drawing on Puttaswamy recognised a nascent “right to be forgotten”.²⁵

Both decisions show Indian courts capable of recognising the severity and continuity of technology-facilitated abuse, and willing to draw on constitutional privacy doctrine. But in both, that recognition proceeds through the accumulation of separately named offences charged and analysed one by one, rather than through a single category naming the underlying pattern as the offence. The “pattern” is reconstructed retrospectively from a charge-sheet; it is not, as in the UK model discussed in Part IV, the unit of the offence itself.

²²Protection of Women from Domestic Violence Act 2005, s 3 and Explanation I.

²³Protection of Women from Domestic Violence Act 2005, ss 2(f), 12, 17–22.

²⁴Kalandi Charan Lenka (n 5).

²⁵Animesh Boxi (n 5); Puttaswamy (n 12); 'Justice in the Digital Age: Addressing Non-Consensual Dissemination of Intimate Images in India's Penal Code' (2025).

F. Procedural and Remedial Fragmentation

The practical consequence is that a woman experiencing technology-facilitated coercive control in India must translate one continuing experience into several distinct legal claims addressed to several distinct authorities: a cybercrime complaint, a platform grievance under the 2021 Rules bounded by a fifteen-day timeline, and, if she seeks protection within the relationship itself, a separate civil application under the PWDVA. Electronic evidence must satisfy the Bharatiya Sakshya Adhiniyam, 2023's admissibility requirements, and cross-platform conduct, anonymous accounts, and cross-border data storage compound each difficulty. The claim this paper advances is therefore not that Indian law lacks remedies – section 78 of the BNS, sections 66C to 67A of the IT Act, the 2021 Rules, and section 3 of the PWDVA between them cover most of the tactics catalogued in Part II.C but that these remedies are fragmented across criminal, cyber, regulatory, and family law in a way that requires the survivor to re-characterise a single continuing relationship of control as several unconnected legal events, none of which is designed to ask directly: has this woman been placed, over time, in a condition of unfreedom by another's sustained use of technology against her?

IV. The United Kingdom: A Conceptual Model for Recognising Patterns

A. From Incident to Pattern: The Statutory Definition of Domestic Abuse

The Domestic Abuse Act 2021 (DAA 2021) supplied England and Wales with their first statutory definition of domestic abuse. Behaviour between two people aged sixteen or over who are “personally connected” expanded to include those who are or have been married, engaged, civil partners, or in an intimate personal relationship – is abusive if it consists of physical or sexual abuse, violent or threatening behaviour, controlling or coercive behaviour, economic abuse, or psychological, emotional, or other abuse such as stalking; the statute specifies this behaviour “can be a single incident or a course of conduct”.²⁶ By placing controlling or coercive behaviour on the same footing as physical abuse, and contemplating a course of conduct rather than a single act, the DAA 2021 gives Stark's theory direct legislative form.

B. The Controlling or Coercive Behaviour Offence

²⁶Domestic Abuse Act 2021, s 1; s 68, amending the definition of 'personally connected' in the Serious Crime Act 2015, s 76(6).

The substantive offence predates the 2021 Act. Section 76 of the Serious Crime Act 2015, in force since December 2015, criminalises controlling or coercive behaviour in an intimate or family relationship: a person (A) commits the offence where A repeatedly or continuously engages in controlling or coercive behaviour towards a personally connected person (B), the behaviour has a serious effect on B causing fear of violence on at least two occasions, or serious alarm or distress substantially affecting B's day-to-day activities and a reasonable person would consider it likely to have that effect. The maximum sentence is five years.²⁷

Crown Prosecution Service guidance stresses the precise analytical point developed in Part II: a pattern can be “well established before a single incident is reported”, individual instances “might seem innocent especially if considered in isolation”, and prosecutors must weigh the cumulative impact rather than assessing each incident independently.²⁸ The offence is regularly described in the secondary literature as a direct legislative response to Stark's own scholarship.²⁹ Its comparative significance is structural: unlike section 78 of the BNS, it is defined by the pattern and its effect on the victim fear, or serious alarm substantially affecting daily life – rather than by any enumerated method of contact or monitoring. It does not matter whether control was exercised by following, by withholding money, or by tracking a phone; what matters is the repeated character of the behaviour and its cumulative effect. This is the method-neutral, pattern-based model India's stalking-centred approach lacks.

C. Technology Within the Coercive Control Framework

The DAA 2021 does not itself mention technology, notwithstanding the Government's claim that the legislation was “future-proof”.³⁰ Recent research on the “technification” of domestic abuse confirms this silence has not stopped technology-facilitated conduct from being captured by the existing offence: a Women's Aid survey found close to a third of survivors reported spyware or GPS locators used against them, and the first UK conviction for stalking via a smart-home device came in 2018, after a perpetrator was found to have listened to his ex-partner's conversations through an iPad mounted on her kitchen wall.³¹

²⁷Serious Crime Act 2015, s 76; Crown Prosecution Service, 'Controlling or Coercive Behaviour in an Intimate or Family Relationship' (legal guidance).

²⁸Crown Prosecution Service (n 25).

²⁹Cattaneo (n 6), noting Stark's 2007 book as a basis for the UK offence.

³⁰Lisa Sugiura and others, 'The Technification of Domestic Abuse: Methods, Tools and Criminal Justice Responses' (2026) *Criminology & Criminal Justice*, citing UK Parliament Post, 2020.

³¹Sugiura and others (n 26); Delanie Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' (2017) 23 *Violence Against Women* 584; Weightmans, 'Technology-Facilitated Abuse: An Emerging Frontier of Coercive Control' (2025).

This is the structural lesson for India: because section 76 is defined by the pattern and its effect rather than the instrumentality used, digital tactics required no bespoke offence to be absorbed – they simply became new evidence for an offence already broad enough to receive them. India's stalking provision, drafted around specific acts of following, contacting, and monitoring, must instead be judicially stretched to cover tactics, such as controlling digital finances, that are not, in ordinary language, acts of “following” at all.

D. Post, Separation Digital Abuse

The clearest empirical demonstration of why incident-based law is inadequate comes from research on abuse continuing after physical separation. Technology lets an abusive partner sustain control long after a relationship ends: through unrevoked shared passwords, family sharing settings, cloud synchronisation of location data, concealed trackers in a vehicle or child's belongings, and co-parenting applications whose record-keeping and real-time location functions – designed to reduce conflict – are instead repurposed for ongoing monitoring.³²

A study of separated mothers' use of court-recommended co-parenting applications found that the very record-keeping functions meant to protect both parties could be manipulated by an abusive former partner to continue surveillance established during the relationship, while mothers simultaneously used those functions to resist and document the abuse; a separate Home Office-funded study found children's own devices increasingly exploited in shared-parenting arrangements to monitor the other parent.³³ This evidence is the strongest factual vindication of Part II's theoretical claim: technology does not merely add a venue for pre-existing abuse; it removes the one boundary – physical separation – on which incident-based law has always implicitly relied.

E. Other Relevant United Kingdom Law

The Protection from Harassment Act 1997 supplies general stalking and harassment offences extending to cyberstalking, but courts had found it poorly suited to controlling behaviour within an ongoing, outwardly affectionate relationship – the specific gap section 76 was designed to close.³⁴ The Online Safety Act 2023 (OSA 2023) supplies the platform-regulation layer,

³²Michelle Irving and Hayley Boxall, 'Post, Separation Parenting Apps as Tools for Control and Resistance' (2026); University of Kent and University of Portsmouth, 'Increasing Use of Technology Driving New Forms of Domestic Abuse' (Home Office Domestic Abuse Perpetrators Research Fund report, January 2022).

³³Irving and Boxall (n 28); University of Kent and University of Portsmouth (n 28).

³⁴See the Home Office circular summarised in '25 Bedford Row, Section 76 of the Serious Crime Act 2015' (analysis of Home Office guidance).

inserting cyberflashing and four non,consensual intimate,image offences into the Sexual Offences Act 2003 that, unlike their 2015 predecessor, do not require proof of intent to cause distress, and imposing duties on platforms enforced by Ofcom with penalties up to £18 million or ten per cent of global turnover; Ofcom itself lists “online domestic abuse – using tech to control or coerce” among its four principal areas of concern for women and girls online.³⁵ The OSA 2023 addresses the instrumentality of abuse – the image, the message – rather than the relationship of domination in which it is deployed; it is the DAA 2021 and section 76 that reach the relationship itself. Together the two regimes divide regulatory labour – platform accountability for content, pattern,based criminal law for the relationship – in a way neither India's IT Act framework nor its BNS stalking provision presently replicates.

V. International Law: The Emerging Normative Standard

A. CEDAW: Due Diligence and State Responsibility

The Committee on the Elimination of Discrimination against Women's General Recommendation No 19 of 1992 brought violence against women within the scope of the Convention, characterising it as a form of discrimination and holding that states could be responsible for private acts of gender,based violence where they failed to act with due diligence to prevent, investigate, punish, and compensate.³⁶ General Recommendation No 35, adopted in 2017, elaborated this standard: states must adopt laws, institutions, and functioning systems to prevent, investigate, prosecute, punish, and remedy gender,based violence by non,state actors, obligations General Recommendation No 35 treats as extending even to extraterritorial corporate conduct, within a broader recognition of the prohibition on gender,based violence as customary international law.³⁷

The due,diligence standard supplies the doctrinal bridge to technology,facilitated violence: if the obligation to prevent, investigate, prosecute, and remedy gender,based violence by private actors is general rather than confined to any method, and coercive control increasingly operates digitally, the obligation extends to regulating the platforms and devices that enable it – precisely the direction UN Women's and the Council of Europe's instruments have since taken.

³⁵Online Safety Act 2023, ss 187–188, inserting Sexual Offences Act 2003, ss 66A–66D; Rebecca Young, 'Your Digital Footprint and the Online Safety Act 2023' (Insider Media, 2025).

³⁶CEDAW Committee, General Recommendation No 19 (1992), as summarised in OHCHR, 'Launch of CEDAW General Recommendation No 35' (2017).

³⁷CEDAW Committee, General Recommendation No 35 on Gender,Based Violence against Women, Updating General Recommendation No 19, UN Doc CEDAW/C/GC/35 (2017) paras 21–24, 38.

B. UN Women: Technology, Facilitated Violence as Continuum

UN Women's 2025 Strategy on Preventing and Eliminating Technology-Facilitated Violence Against Women and Girls positions TF VAWG explicitly within the continuum of violence against women, describing digital and offline violence as connected manifestations of gendered power imbalance rather than separate phenomena.³⁸

Its November 2025 brief on a Model Framework for Legislation on TF VAWG is the most directly relevant international document: it finds that more than half the world's women lack adequate legal protection, that existing legislation “does not usually include the full spectrum” of TF VAWG, and that laws “have failed to keep pace with rapid technological change” – precisely the fragmentation diagnosis this paper applies to India.³⁹ The brief points to Brazil's “duty of care” standard under Article 19 of the Marco Civil da Internet and the United States' Take It Down Act as comparative models of platform-facing obligations going beyond conventional criminal law.⁴⁰

C. The Council of Europe: Accountability Beyond Criminal Law

The most significant recent development is the Council of Europe's Recommendation CM/Rec(2026)2 on accountability for technology-facilitated violence, adopted by the Committee of Ministers in early 2026 and launched in Strasbourg on 10 June 2026 – described by the Council of Europe as the first international legal standard focused specifically on this subject.⁴¹ It explicitly situates TF VAWG within the continuum of violence and – echoing the post-separation abuse evidence in Part IV.D – recognises that such violence “often accompanies” domestic violence, allowing perpetrators to “extend surveillance, coercion and control through digital tools” even after separation.⁴²

Rather than fitting TF VAWG into existing criminal categories, the Recommendation builds accountability extending into civil and administrative fields: a victim-centred, trauma-informed approach; multi-stakeholder engagement with civil society and technology companies; accessible justice preventing secondary victimisation; and a “safety-by-design” obligation

³⁸UN Women, UN Women Strategy (n 4).

³⁹UN Women, Model Framework for Legislation on Technology-Facilitated Violence against Women and Girls (Brief, November 2025).

⁴⁰UN Women, Model Framework (n 33).

⁴¹Council of Europe (n 8); Council of Europe, 'Accountability for Technology-facilitated Violence against Women and Girls: New Council of Europe Recommendation' (Committee on Crime Problems, 2026).

⁴²Council of Europe, 'Council of Europe Unveils Roadmap to Tackle Online Violence against Women and Girls' (Portal, 2026).

requiring that products not facilitate violence in the first place.⁴³ It is the first instrument examined here that does not organise its response around discrete offences at all: where India's BNS and IT Act, and even the UK's section 76, remain fundamentally criminal, law instruments, the Recommendation builds accountability directly around the continuum concept – prevention, safety, by, design, and civil and administrative liability operating alongside the criminal law. It is the most advanced articulation yet of Part II's theoretical claim: that coercive control, once mediated by technology, cannot be fully addressed by any offence, based model.

D. State Responsibility: Prevent, Protect, Investigate, Prosecute, Remedy

Read together, CEDAW's due, diligence doctrine, UN Women's continuum framing, and the Council of Europe's 2026 Recommendation answer, affirmatively, the questions this paper's research plan set out to investigate. Criminalisation alone is not sufficient – anonymous perpetrators and cross, border platforms routinely defeat purely criminal enforcement, and UN Women's Model Framework identifies this as the central reason existing laws fail to cover the “full spectrum” of TF VAWG.⁴⁴ States must regulate platforms directly, as the OSA 2023's illegal, content duties and the Council of Europe's safety, by, design obligation now require. Victims must have accessible remedies, as General Recommendation No 35's reparations obligation requires. And anonymity and cross, border enforcement remain, on the evidence of both jurisdictions examined here, the most persistent obstacles to effective response – obstacles only coordinated platform accountability, rather than domestic criminal law alone, appears capable of addressing.

VI. Synthesis: From Isolated Offences to a Continuum, Based Legal Response

The argument of this paper can now be stated as a single chain connecting theory, comparative doctrine, and international standard, setting. Coercive control theory establishes that the harm of intimate, partner abuse lies in a cumulative pattern of domination rather than any single injurious act. The continuum of violence establishes that this pattern cannot be cleanly divided into discrete legal categories, and that the same continuum runs, with equal force, between offline and online conduct. Technology does not introduce a new category of harm; it expands, and in the case of post, separation abuse effectively removes, the physical and temporal limits within which coercive control has historically operated.

⁴³Council of Europe, Technology Facilitated Violence against Women and Girls (Committee on Crime Problems, 2026).

⁴⁴UN Women, Model Framework (n 33).

Set against that baseline, India's framework tends to address stalking, intimidation, privacy violation, non-consensual intimate imagery, and domestic violence as separate legal problems, each with its own statute, procedure, and forum – even though the same facts frequently implicate several categories at once, as Part III.E showed. The United Kingdom's controlling, or, coercive, behaviour offence demonstrates, by contrast, that a single pattern, based, method, neutral offence – built around the cumulative effect of behaviour on a victim's freedom rather than any enumerated method – can absorb new technological tactics without bespoke new offences. It offers a stronger conceptual framework for recognising coercive control as a pattern, though even the UK statute achieves this only because its definition happens to be broad enough to receive digital tactics its drafters did not explicitly contemplate.

International standards, developing independently, converge on the same insight from the opposite direction. CEDAW's due diligence doctrine establishes that state responsibility for gender-based violence by private actors is continuing, not confined to discrete episodes. UN Women's continuum framing and 2025 Model Framework make explicit what India's, and to a lesser extent the UK's, domestic frameworks illustrate implicitly: legislation enumerating specific technological acts, rather than the continuing relationship those acts sustain, will always lag behind technological change and leave gaps for anonymous or cross-border perpetrators. The Council of Europe's 2026 Recommendation is the clearest evidence yet that the most advanced normative thinking has moved past the criminal, offence model altogether, toward accountability built around prevention, safety, by, design, and civil and administrative liability across the online–offline continuum.

The unifying claim is not that technology has created an entirely new species of violence unknown to existing law. It is that legal systems – India's most visibly, the United Kingdom's only partially less so – continue to conceptualise technologically facilitated abuse through the vocabulary of isolated offences even where the technology sustains an underlying, continuing pattern of coercive control. The deeper reform this comparison points toward is not merely new cyber-specific offences, but a shift in the unit of legal analysis itself: from the discrete act, however serious, to the continuing relationship of domination the act may serve.

VII. Conclusion

This paper has argued that technology-facilitated coercive control exposes a structural weakness common to incident-based legal systems: their inability to treat a continuing pattern of domination, sustained through individually lawful or borderline digital acts, as a single legal

wrong. India's constitutional privacy jurisprudence, its stalking, privacy, and obscenity offences, its intermediary grievance architecture, and its domestic violence statute each competently address particular tactics; none, on the present state of the case law, is designed or has yet been judicially extended to recognise the underlying relationship those tactics sustain. The United Kingdom's controlling,or,coercive,behaviour offence, built around the pattern and its effect rather than any enumerated method, offers a workable comparative model – one that required no purpose,built “digital abuse” offence to absorb spyware, GPS tracking, and social,media surveillance into its existing definition. International standard,setting, culminating in the Council of Europe's 2026 Recommendation, points further still, toward accountability operating through prevention and platform design rather than the criminal law alone.

For India, three directions of reform follow. First, a method,neutral, effect,and,pattern,based offence – whether by amendment to section 78 of the BNS or as a standalone provision modelled on section 76 of the Serious Crime Act 2015 – would let criminal law recognise coercive control as a continuing relationship rather than discrete acts of following or monitoring. Second, explicit recognition, through guidance, judicial interpretation, or amendment, that section 3 of the PWDVA's emotional, and economic,abuse categories extend to digital surveillance and coercive financial monitoring would activate remedial machinery that, on its current text, already appears broad enough to reach these harms but has not yet been applied to them. Third, platform accountability duties, building on the 2021 Intermediary Guidelines Rules but strengthened along the safety,by,design and administrative,accountability lines the Council of Europe now sets out internationally, would extend India's regulatory reach beyond the take,down of individual content toward prevention of the underlying pattern.

The deeper point this paper has sought to establish is that the legal problem posed by technology,facilitated coercive control is not, at bottom, a problem of technology. It is the older problem Evan Stark identified in 2007, now sustained by newer instruments: a legal imagination still organised around the injury of a single incident, confronting a form of abuse whose entire logic – online exactly as much as offline – lies in what only becomes visible, and only becomes dangerous, when read as a pattern.

REFERENCES

Books and Journal Articles

- Cattaneo LB, 'Rethinking Coercive Control' (2009) 15 Violence Against Women.

- Kelly L, *Surviving Sexual Violence* (Polity Press 1988).
- Kelly L, 'Standing the Test of Time? Reflections on the Concept of the Continuum of Sexual Violence' in Jennifer M Brown and Sandra L Walklate (eds), *Handbook on Sexual Violence* (Routledge 2012).
- Stark E, *Coercive Control: The Entrapment of Women in Personal Life* (Oxford University Press 2007).
- Sugiura L and others, 'The Technification of Domestic Abuse: Methods, Tools and Criminal Justice Responses' (2026) *Criminology & Criminal Justice*.
- Irving M and Boxall H, 'Post,Separation Parenting Apps as Tools for Control and Resistance' (2026).
- Woodlock D, 'The Abuse of Technology in Domestic Violence and Stalking' (2017) 23 *Violence Against Women* 584.
- Bharati RK, 'Violation of Privacy in Cyberspace (Section 66E of the IT Act, 2000)' (2025).

India: Constitution, Statutes, and Rules

- The Constitution of India 1950, arts 14, 19, 21.
- Bharatiya Nyaya Sanhita 2023, ss 77, 78, 351.
- Information Technology Act 2000, ss 43, 66C, 66D, 66E, 67, 67A, 79.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.
- Protection of Women from Domestic Violence Act 2005, ss 2–22.
- Bharatiya Sakshya Adhiniyam 2023 (electronic evidence provisions).

India: Case Law

- Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
- Kalandi Charan Lenka v State of Odisha, BLAPL No 7596 of 2016, Orissa High Court, judgment dated 16 January 2017.
- State of West Bengal v Animesh Boxi, GR No 1587/17, Judicial Magistrate 1st Class, 3rd Court, Tamluk, Purba Medinipur, judgment dated 7 March 2018.

United Kingdom: Statutes and Guidance

- Serious Crime Act 2015, s 76.
- Domestic Abuse Act 2021, ss 1, 68.

- Protection from Harassment Act 1997.
- Online Safety Act 2023, ss 187–188 (inserting Sexual Offences Act 2003, ss 66A–66D).
- Crown Prosecution Service, 'Controlling or Coercive Behaviour in an Intimate or Family Relationship' (legal guidance).
- HM Government, Domestic Abuse Act 2021 Statutory Guidance (2022).

- ***International Instruments and Reports***

- CEDAW Committee, General Recommendation No 19 (1992).
- CEDAW Committee, General Recommendation No 35 on Gender-Based Violence against Women, Updating General Recommendation No 19, UN Doc CEDAW/C/GC/35 (2017).
- Council of Europe, Recommendation CM/Rec(2026)2 of the Committee of Ministers to Member States on Accountability for Technology-Facilitated Violence against Women and Girls (2026).
- UN Women, UN Women Strategy on Preventing and Eliminating Technology-Facilitated Violence against Women and Girls (2025).
- UN Women, Model Framework for Legislation on Technology-Facilitated Violence against Women and Girls (Brief, November 2025).
- UN Women, Repository of UN Women's Work on Technology-Facilitated Violence against Women and Girls (March 2025).
- OHCHR, 'Launch of CEDAW General Recommendation No 35 on Gender-Based Violence against Women, Updating General Recommendation No 19' (2017).

Secondary and News Sources

- The Cyber Helpline, 'What is Tech Facilitated Abuse? A Guide to Online Gender-Based Violence' (2025).
- Weightmans, 'Technology-Facilitated Abuse: An Emerging Frontier of Coercive Control' (2025).
- University of Kent and University of Portsmouth, 'Increasing Use of Technology Driving New Forms of Domestic Abuse' (Home Office Domestic Abuse Perpetrators Research Fund report, January 2022).
- Young R, 'Your Digital Footprint and the Online Safety Act 2023' (Insider Media, 2025).