PUNGGAWA LAW REVIEW
Punggawa Law Review
Volume 1, Number 2, 2026
E-ISSN: 3125-0580
Open Access: punggawajournal.com/plr

Technology-Facilitated Domestic Violence and Coercive Control: A Normative Legal Study on Victim Protection in Digital Intimate Relations

Sutiawati [1]
[1] Fakultas Hukum, Universitas Muslim Indonesia, Indonesia
Correspondence: sutiawati@umi.ac.id

Article Info
Article history:
Received May 15, 2026
Revised May 20, 2026
Accepted May 26, 2026

Keyword:
Domestic violence; Coercive control; Technology-facilitated abuse.

ABSTRACT
Technology-facilitated domestic violence raises a doctrinal difficulty that cannot be solved by adding more cybercrime provisions to existing legal systems. The central problem lies in the way law classifies harm. Digital abuse in intimate relationships may appear as fragmented conduct: repeated messages, access to cloud storage, location tracking, control over banking applications, threats to circulate intimate images, or the misuse of smart-home devices. Assessed separately, each act may look minor, technically ambiguous, or difficult to prove. Within an abusive relationship, however, those acts may operate as coercive control. This article uses normative legal research to examine how domestic violence law should recognise technology-facilitated coercive control while avoiding an overbroad criminal category. The analysis relies on primary legal materials, including the Serious Crime Act 2015, the Domestic Abuse Act 2021, the Domestic Abuse (Scotland) Act 2018, the Online Safety Act 2023, the EU Digital Services Act, Australia's Online Safety Act 2021, and selected coercive-control reforms in New South Wales. It also draws on recent journal literature concerning intimate partner violence, coercive control, image-based sexual abuse, digital evidence, and victim protection. The article argues that digital abuse should be legally treated as domestic violence where the conduct forms part of a pattern of domination, surveillance, intimidation, sexual coercion, economic restriction, or post-separation control. It further argues that digital evidence must be handled through a victim-centred protocol based on necessity, specificity, minimisation, and protected disclosure. A stronger legal model does not need to abandon due process. It needs to read digital facts in their relational setting.

INTRODUCTION

Domestic violence law was never designed for a world in which intimate control could be maintained through phones, cloud accounts, smart speakers, banking applications, vehicle-tracking systems, and children's devices. The old legal image of domestic abuse still carries a physical bias. Law more readily responds to bruises, assault, explicit threats, or visible property damage (Rogers et al., 2023). Digital abuse is less comfortable for legal reasoning because it often arrives through ordinary platforms and ordinary habits. A partner may ask for a password, insist on location sharing, monitor online status, or use a family subscription to access private information. None of these acts automatically constitutes domestic violence. Yet inside a relationship shaped by fear, prior threats, dependency, and unequal control, the same conduct may become a mechanism for surveillance and domination. The legal question is not whether technology creates a new form of intimacy. The harder question is whether law can recognise old coercive patterns when they are carried by digital tools (Leitão, 2021).

The global debate has moved beyond the simple claim that technology is being misused by abusive partners. Recent research has described technology-facilitated intimate partner violence as a continuum of behaviours, including monitoring, harassment, impersonation, image-based sexual abuse, threats, economic restriction, and post-separation stalking (Bailey et al., 2024) . A victim may leave the

shared home but remain reachable, traceable, and punishable through digital systems. This is one reason why separation no longer gives the same practical meaning to safety. A former partner may no longer have keys to the house, but may still have access to location history, shared photo storage, vehicle applications, school communication platforms, or a child's tablet (Storey & Pina, 2025). Legal systems that treat digital abuse as a set of unrelated cyber incidents risk missing the domestic character of the harm. The abuse is not merely "online". It is domestic control extended through networked infrastructure.

Coercive control provides a more accurate legal vocabulary, although it is not free from difficulty. The concept shifts attention from isolated incidents to a course of conduct that restricts autonomy through intimidation, isolation, degradation, surveillance, and rule-making. This shift matters because domestic abuse is often cumulative. A single message may not be threatening to an outsider. It may still make a victim change route, cancel work, delete a social media post, avoid a family gathering (Kadir, 2025), or comply with a demand because the message carries a history. Legal systems that have criminalised coercive or controlling behaviour, such as England and Wales under section 76 of the Serious Crime Act 2015 and Scotland under the Domestic Abuse (Scotland) Act 2018, have already accepted that domestic abuse cannot be reduced to physical assault (Brennan & Myhill, 2022). The unresolved issue is whether these legal categories can adequately capture digital tactics without becoming vague or dependent on police discretion (Myhill et al., 2023).

There is a need for some intellectual hesitation here. Expanding domestic violence law into digital conduct can strengthen victim protection, but it can also create definitional problems. Many intimate relationships involve shared devices, shared passwords, location-sharing arrangements, and emotionally messy communication. Criminal law cannot treat every jealous message, account check, or post-breakup argument as domestic violence. A careful doctrine must distinguish ordinary conflict, privacy violation, cyber harassment, and coercive domination. The distinction should not be based only on the technology used (Tolmie et al., 2024). It should be based on relational context, repetition, purpose, threat, vulnerability, prior abuse, and the actual restriction imposed on the victim's freedom. Without that restraint, legal reform may become broad in language but weak in practice (Hilton et al., 2023). It may also invite defensive arguments that coercive control law criminalises poor relationship behaviour rather than patterned domination.

Image-based sexual abuse makes the issue sharper. The creation, possession, threat, or distribution of intimate images can operate as sexual coercion, reputational punishment, or a way to prevent a victim from leaving. The threat may be more controlling than the eventual publication. A victim may remain silent during custody disputes, accept unwanted contact, or withdraw a complaint because an abusive partner holds intimate material. Deepfake technology adds further complexity because sexualised material can be fabricated and still produce real reputational, emotional, and legal harm (Henry et al., 2023). The Online Safety Act 2023 in the United Kingdom, the EU Digital Services Act, and Australia's Online Safety Act 2021 all matter here because platform responsibility, takedown mechanisms, and digital service governance influence whether the victim can regain practical control over the material. Criminal liability alone rarely solves the immediate harm of circulation, replication, and threat (KLucas, 2022).

The evidentiary problem is equally serious. Digital abuse produces records, but those records are fragile, incomplete, and sometimes dangerous for victims to disclose. Screenshots, logs, messages, metadata, account notifications, and device histories may support a complaint. At the same time, victims may be asked to hand over entire devices, private photos, health information, children's messages, legal correspondence, or communications with support services. A process designed to prove abuse can expose the victim to a new loss of privacy. The concern is not theoretical. Legal procedures may become part of continued control where perpetrators use disclosure requests, custody proceedings, or repeated complaints to exhaust and intimidate the victim (Gutowski & Goodman, 2023). In digital cases, that problem becomes more concrete because the victim's phone often contains the evidence and the victim's life at the same time.

This article argues that technology-facilitated domestic violence should be treated as domestic violence where digital conduct forms part of coercive control. The claim is deliberately narrower than saying that all digital harm in intimate relationships belongs to domestic violence law. The article develops two research objectives. The first objective is to analyse the legal character of technology-facilitated coercive control as a form of domestic violence rather than as a merely cyber or

communications offence. The second objective is to formulate a victim-centred normative model for protection, risk assessment, and digital evidence handling. These objectives respond to three research problems: how domestic violence law should conceptualise digital coercive control; why existing legal categories remain difficult to apply; and what model of protection can improve safety without weakening evidentiary fairness.

RESEARCH METHODS

This study uses normative legal research. The primary legal materials consist of statutes and legal instruments that directly regulate domestic abuse, coercive control, online harm, platform responsibility, and digital protection. The Serious Crime Act 2015 is used because section 76 criminalises controlling or coercive behaviour in an intimate or family relationship in England and Wales. The Domestic Abuse Act 2021 is used because it provides a statutory definition of domestic abuse and recognises controlling or coercive behaviour as part of abuse. The Domestic Abuse (Scotland) Act 2018 is used because it frames domestic abuse as a course of behaviour, including conduct intended to make a partner dependent, subordinate, isolated, controlled, frightened, humiliated, or punished. The Online Safety Act 2023, the EU Digital Services Act, Australia's Online Safety Act 2021, and New South Wales coercive-control reforms are used in the discussion because they provide legally relevant models for platform responsibility, online abuse responses, and course-of-conduct regulation in intimate relationships.

Secondary legal materials consist of recent peer-reviewed journal articles on technology-facilitated abuse, coercive control, intimate partner violence, image-based sexual abuse, deepfakes, legal abuse, policing, risk assessment, and technology-based interventions. The selection gives priority to articles published from 2021 onward, with some earlier works retained only where they remain conceptually central. The legal materials were collected through document study. The process involved identifying legal rules that speak directly to coercive or controlling conduct, locating digital-governance instruments that affect online abuse and intimate-image harms, and classifying journal literature according to its relevance to legal conceptualisation, evidentiary handling, victim protection, and doctrinal limitation. No empirical interviews or surveys were conducted because the purpose is not to measure prevalence. The inquiry is directed at whether legal concepts and procedures can properly account for digital coercion within domestic relationships.

The materials are analysed through conceptual, statutory, comparative, and prescriptive reasoning. Conceptual analysis is used to separate digital conflict, cyber misconduct, and coercive domestic abuse. Statutory analysis is used to test whether provisions on domestic abuse, online safety, and coercive control can address technologically mediated patterns of domination. Comparative analysis is used cautiously; foreign law is not treated as a model to be transplanted, but as a source of doctrinal options and warnings. Prescriptive reasoning is used to formulate a legal model based on recognition of digital coercive control, risk assessment, tailored protection orders, platform cooperation, and restrained evidence collection. The method is suitable because the central issue is normative: how law should classify conduct, allocate proof, and protect victims without producing vague or excessive liability.

RESULTS AND DISCUSSION

1. Reclassifying Digital Abuse as Coercive Domestic Violence

Technology-facilitated abuse should not be legally reduced to the misuse of devices. The device is only the instrument. The relevant legal harm lies in the way the instrument is used to organise control. A partner who accesses cloud storage without consent may commit a privacy violation. The same act becomes domestic abuse where it is part of a broader course of intimidation, humiliation, surveillance, or restriction. This distinction is important because domestic violence law is concerned with relational domination, not merely unlawful data access. Existing research has placed technology-facilitated abuse within the broader structure of intimate partner violence, with tactics ranging from surveillance applications and social media harassment to camera misuse and persistent monitoring (Rogers & Davis, 2024). The practical issue is that these acts often appear ordinary from outside the relationship. A court may see "messages". The victim may experience a command backed by years of punishment.

Section 76 of the Serious Crime Act 2015 offers a useful starting point because it criminalises repeated or continuous controlling or coercive behaviour between personally connected persons where

the behaviour has a serious effect. Its strength lies in course-of-conduct reasoning. Digital abuse can fit this structure where the perpetrator repeatedly monitors accounts, demands location sharing, threatens exposure, uses spyware, or contacts the victim through multiple platforms after separation. The limitation is that the provision does not itself provide a digital vocabulary. This can leave frontline actors to treat tech abuse as incidental unless statutory guidance, police practice, and prosecutorial assessment explicitly integrate digital tactics. The Domestic Abuse Act 2021 partly corrects this by defining domestic abuse to include controlling or coercive behaviour, economic abuse, psychological abuse, and threatening behaviour. Yet the statute still requires practical interpretation before conduct such as cloud-account control, smart-home manipulation, or intimate-image threats is recognised as domestic domination rather than miscellaneous online harm.

The Domestic Abuse (Scotland) Act 2018 is more analytically helpful because it treats domestic abuse as a course of behaviour and includes behaviour that makes a partner dependent or subordinate, isolates a partner, controls or monitors day-to-day activities, deprives freedom of action, or frightens, humiliates, degrades, or punishes. This formulation is better suited to technology-facilitated abuse because it does not depend on naming a specific device. A perpetrator who monitors a victim's location through a shared application, controls access to digital banking, or threatens to publish intimate material can be assessed through the effect of the conduct rather than the novelty of the tool. The statutory structure is still not perfect. A law that uses broad terms such as "monitoring" and "control" requires disciplined application. Without evidence of pattern, impact, and relational power, ordinary conflict may be overread. With too much caution, serious digital domination may be dismissed as immature communication.

The better legal test should combine four elements. First, there must be a current or former intimate or family relationship. Second, the conduct must be repeated, continuous, or linked to a broader abusive course of conduct. Third, the digital act must have a coercive function, such as surveillance, intimidation, humiliation, sexual leverage, economic restriction, isolation, or punishment. Fourth, the conduct must cause or risk serious interference with the victim's safety, autonomy, privacy, dignity, or freedom of action. This test avoids reliance on the technical label of the act. It also avoids the opposite mistake, namely treating every unwanted digital contact as domestic violence. The focus remains on the relational function of the conduct. That is where coercive control becomes legally useful and where it must be kept precise (Wilson & Fritz, 2023).

Digital coercive control also requires attention to consent. In intimate relationships, consent to digital access is often informal, fluid, and shaped by dependence. A password may have been shared voluntarily during the relationship. A location-sharing application may have been installed for convenience. A partner may have access to a family tablet or a shared cloud album. The legal error occurs when prior access is treated as permanent authorisation. Consent should be capable of withdrawal, and continued use after withdrawal may become coercive if it contributes to monitoring, threat, or restriction. Even before explicit withdrawal, "consent" may be legally thin where refusal would likely trigger anger, violence, abandonment, financial punishment, or sexual coercion. This is not an argument for presuming abuse in every digitally connected relationship. It is an argument for reading consent with attention to power, dependency, and the practical cost of refusal (Munro, 2025).

A specific problem arises with post-separation abuse. The formal end of a relationship does not necessarily end digital access. Former partners may remain connected through shared parenting applications, school platforms, children's devices, vehicle subscriptions, home-security accounts, cloud storage, or financial arrangements. Protection orders that prohibit physical proximity may fail where surveillance and intimidation continue remotely. The Domestic Abuse Act 2021 and the Serious Crime Act 2015 are relevant because they recognise abuse between former partners, but the content of protective restrictions must be updated. A no-contact order should prohibit contact through fake accounts, shared applications, third-party accounts, payment notes, children's devices, and smart-home systems where those channels are used for control. A protection order that does not address digital routes of contact may look strong on paper while leaving the victim reachable every day.

The New South Wales coercive-control reforms are important because they demonstrate an attempt to criminalise abusive courses of conduct within intimate partner relationships while identifying patterns rather than isolated acts. The value of this approach lies in recognising that controlling conduct can include monitoring, restricting freedom, isolating, manipulating access to money, and threatening harm. Its challenge is similar to the challenge faced in England, Wales, and Scotland: the statute must

be applied by institutions that can distinguish coercive patterns from ordinary conflict. This is why digital indicators should be embedded in risk assessment and prosecutorial guidance. A perpetrator's use of technology may not be sophisticated. Less sophisticated methods, including social media, messaging, and video-call recording, can still produce substantial control, especially where the victim has limited resources to change devices, secure accounts, or leave shared digital arrangements (Reed et al., 2025).

Image-based sexual abuse confirms why domestic violence law should not rely only on cybercrime categories (Kadir, 2024). The harm is not exhausted by publication. Threats to distribute intimate images may discipline the victim's behaviour long before any upload occurs. In intimate relationships, such threats can force silence, compliance, continued contact, sexual submission, or withdrawal from legal proceedings. Deepfake sexual material deepens the problem because fabricated images may still be used to shame, extort, or discredit a victim (Henry et al., 2023). The Online Safety Act 2023, the EU Digital Services Act, and Australia's Online Safety Act 2021 become relevant here because they move part of the legal response from the perpetrator alone to the digital environment that enables circulation, reporting, removal, and preservation. Domestic violence law needs this connection. The victim's immediate need is often not only punishment of the perpetrator but rapid containment of the material and proof that the threat formed part of coercive control.

2. Digital Evidence, Victim Protection, and Procedural Restraint

Digital evidence can make domestic violence visible, but it can also make the victim more exposed. Screenshots, call logs, emails, voice notes, location records, application notifications, device access histories, and platform data may prove a pattern that witnesses never saw. This is valuable because coercive control often occurs in private and because perpetrators may deny or normalise their conduct. Yet the evidentiary benefit comes with procedural risk. A phone is not merely an evidence container. It may hold health records, legal messages, therapy notes, immigration documents, children's communications, bank information, intimate images, and contact with support services. A legal process that demands unrestricted device access can reproduce the same loss of privacy that digital abuse created.

The law of evidence should therefore move away from crude all-or-nothing thinking. Screenshots should not be automatically accepted as conclusive, but they should not be dismissed because they are not full forensic extractions. In domestic violence cases, proof is often cumulative. A screenshot may be supported by timestamps, phone numbers, account identifiers, platform records, witness testimony, call logs, bank records, metadata, device notifications, or evidence of prior incidents. Requiring perfect digital proof from the beginning may defeat the purpose of victim protection. Still, authenticity matters. A fair system should allow preliminary reliance on accessible digital materials while preserving the right to test reliability where the case moves toward criminal conviction. This is not a relaxation of proof. It is a recognition that domestic abuse evidence often becomes reliable through pattern, corroboration, and relational interpretation (Weissflog et al., 2025).

The Serious Crime Act 2015 and the Domestic Abuse (Scotland) Act 2018 both require attention to courses of conduct. That legal structure should shape evidence collection. Investigators should not ask only whether one message contains an explicit threat. They should ask how the message fits into the sequence of monitoring, punishment, apology, renewed access, sexual pressure, financial restriction, or post-separation pursuit (Mappaselleng & Kadir, 2025). This may require a chronology rather than a file of isolated screenshots. A victim's evidence may include small incidents that seem unimportant to outsiders: a login alert at night, a delivery note containing a private insult, a sudden change in a smart thermostat, a payment transfer with a threatening reference, or a child's device receiving messages meant for the victim. These details matter because coercive control is often administratively small and psychologically large.

Procedural restraint is essential. A victim-centred evidence protocol should rest on four principles: necessity, specificity, minimisation, and protected disclosure. Necessity requires investigators to explain why a particular category of data is needed. Specificity requires requests to be limited by account, date, platform, device, or issue. Minimisation requires irrelevant data to be excluded from copying, review, and disclosure. Protected disclosure requires strict limits on intimate images, children's data, health information, legal communications, counselling records, and support-service contact. These principles should apply at police, prosecutorial, and court stages. They also fit ordinary

due process. The accused should have access to relevant evidence, but relevance should not become a justification for rummaging through the victim's life.

Legal abuse complicates digital evidence further. Abusive partners may use court proceedings, disclosure requests, custody disputes, or complaints to continue control. The problem is not that defendants should be denied procedural rights. The problem is that legal procedures can be weaponised where courts lack sensitivity to coercive control (Gutowski & Goodman, 2023). In digital cases, the risk is heightened because disclosure may reveal current location, new phone numbers, safe contacts, refuge services, therapy records, or communications with lawyers. A protective model should allow judicial filtering, redaction, sealed exhibits, independent digital review, and restricted access to intimate material. The accused can challenge the evidence without receiving unnecessary access to data that increases danger.

The Online Safety Act 2023, the EU Digital Services Act, and Australia's Online Safety Act 2021 are also relevant to evidence because platform data may be necessary to prove account ownership, publication, impersonation, takedown history, threat, or repeated contact. A platform may hold logs that a victim cannot access. In image-based sexual abuse, hash values, upload records, reporting histories, or removal actions may support proof without requiring repeated circulation of the image in open files. In stalking or harassment cases, platform cooperation may help identify fake accounts or preserve content before deletion. Legal reform should require preservation pathways that are fast enough for safety and careful enough for privacy. It should also prevent abusive misuse of platform reporting systems, where perpetrators falsely report victims' accounts to silence or isolate them.

The handling of intimate images requires special protection. Requiring a victim to repeatedly display, transmit, or describe intimate material can become a form of institutional harm. A better approach uses sealed evidence, limited viewing, technical descriptions, hash matching, expert summaries, and protective directions. The core legal fact is not always the visual content itself. It may be the possession, threat, fabrication, distribution, or coercive use of the material. In deepfake cases, the law should avoid requiring victims to prove that the image is "real" before recognising harm. A fabricated image may be false and still coercive. It may be used to threaten employment, family standing, custody, immigration security, or personal safety. The harm lies partly in the perpetrator's ability to mobilise sexualised reputational damage (Sorochinski & Varvaro, 2023).

Counter-allegations must be handled carefully. In some cases, both parties may exchange hostile messages or access shared digital spaces. A domestic violence analysis should not simply count incidents. It should examine directionality, purpose, fear, dependency, injury, social power, prior abuse, and practical effect. A victim who records conversations, saves screenshots, or checks a shared account to understand how surveillance is occurring is not automatically equivalent to a perpetrator who installs spyware to control movement. This distinction does not excuse unlawful conduct by victims. It prevents legal analysis from flattening self-protection and domination into "mutual conflict". Coercive control doctrine becomes weak where it cannot tell the difference between resistance, documentation, retaliation, and primary aggression (Lucas et al., 2022).

Risk assessment should treat digital tactics as possible escalation indicators. Repeated unwanted contact across platforms, threats involving intimate images, tracking after separation, account compromise, impersonation, monitoring through children's devices, smart-home manipulation, and attempts to block support networks may indicate more than online harassment. They may indicate that the perpetrator is trying to maintain access after the victim has reduced physical contact. This is where the Domestic Abuse Act 2021 and the Domestic Abuse (Scotland) Act 2018 should be read together with practical protection-order design. A no-contact rule should be translated into digital terms. It should prohibit direct contact, indirect contact, surveillance, account access, location tracking, impersonation, intimate-image threats, and use of shared platforms for intimidation. Without that translation, a protection order may ban the front door while leaving the digital door open.

3. Toward a Victim-Centred Normative Model

A victim-centred model should begin with statutory recognition. Domestic violence law should expressly recognise technology-facilitated abuse as part of coercive or controlling conduct where digital systems are used to monitor, harass, intimidate, humiliate, impersonate, isolate, economically restrict, sexually coerce, or punish a current or former intimate partner. The wording should avoid naming only current technologies. Stalkerware, GPS tags, cloud accounts, smart speakers, and artificial-intelligence

tools will change. The legal definition should focus on conduct and function. Guidance can provide examples, but the statute should remain technology-neutral. This approach is consistent with the course-of-conduct logic of the Serious Crime Act 2015 and the Domestic Abuse (Scotland) Act 2018, while filling the interpretive gap left by general domestic abuse definitions.

The second element is digital risk assessment. Police, prosecutors, courts, and support services should treat digital conduct as part of the safety picture from the first report. A victim who reports repeated login alerts, unknown tracking, threats involving images, or contact through children's devices should not be told merely to block the perpetrator. Blocking may help in some cases. In others, it may escalate danger or cut off evidence. Risk assessment should ask whether the perpetrator has physical access to devices, technical skill, shared accounts, control over money, access to children's technology, knowledge of the victim's routines, or a history of post-separation threats. Technology-based abuse frequently overlaps with offline abuse, and the overlap should guide protection rather than remain a separate technical question (Boxall et al., 2025).

The third element is protection-order design. Orders should be written in terms that victims, police, and courts can actually apply. A prohibition on contact should include contact through fake accounts, third-party accounts, payment references, shared subscriptions, work platforms, gaming platforms, parenting applications, school accounts, and automated notifications where used abusively. A prohibition on surveillance should include location tracking, spyware, cloud access, smart-home monitoring, vehicle applications, and children's devices. An order may also require device return, account transfer, password reset, removal from shared subscriptions, disabling of trackers, deletion of unauthorised access credentials, and non-interference with support-service communications. These measures are not technical luxuries. In many cases, they determine whether separation creates safety.

The fourth element is platform responsibility. The Online Safety Act 2023, the EU Digital Services Act, and Australia's Online Safety Act 2021 demonstrate different ways of involving digital services in harm reduction. Domestic violence law should connect with these regimes because intimate abuse often depends on platform architecture. Reporting tools, account recovery systems, privacy settings, location-sharing defaults, takedown procedures, and evidence-preservation rules can either help or harm victims. A platform that removes abusive content without preserving proof may frustrate prosecution. A platform that sends safety notifications to a shared account may alert the perpetrator. A reporting pathway that demands complex forms may be unusable for a victim under active surveillance. Legal duties should require safety-sensitive design, rapid response to protection-order breaches, and preservation of relevant data under proper safeguards.

The fifth element is digital evidence governance. A statutory or judicial protocol should regulate how police and prosecutors request, copy, store, review, and disclose victim data. Whole-device extraction should be exceptional, justified, documented, and reviewable. Targeted extraction should be preferred. Intimate images should be sealed or technically represented where possible. Children's data should receive heightened protection. Support-service communications should be treated with particular care. Defence access should be controlled by relevance and protective conditions. This model protects victims, but it also protects the quality of criminal process. Evidence obtained through overbroad and poorly documented extraction is vulnerable to challenge. Evidence obtained through specific, necessary, and accountable procedures is more defensible.

The sixth element is institutional training, but training must be practical rather than symbolic. Police and prosecutors need to recognise ordinary forms of digital abuse: shared iCloud access, SIM swapping, fake social media profiles, AirTag-type tracking, smart-doorbell monitoring, banking-app control, non-consensual screen recording, location sharing through children's devices, and coercive use of intimate images. Judges need to understand why a short message may carry coercive force where there is prior abuse. Legal aid lawyers and victim advocates need enough technical knowledge to preserve evidence without increasing risk. Social workers and domestic violence services need referral pathways to digital security support. The point is not to turn every legal actor into a forensic expert. The point is to prevent digital ignorance from becoming doctrinal minimisation (Williams et al., 2025).

The seventh element is doctrinal restraint (Emezue et al., 2022). A strong legal model should be able to say that some digital conduct is abusive, some is unlawful but not domestic violence, and some is painful but not properly criminal. This matters because intimate relationships contain ordinary conflict, poor judgment, emotional dependency, and privacy mistakes. The threshold for coercive domestic violence should require pattern, relational power, coercive function, and serious effect or risk.

Civil protection may operate earlier than criminal conviction, but it should still require credible evidence of safety, autonomy, privacy, dignity, or freedom being threatened. This restrained approach is not hostile to victims. It strengthens legal protection by making the category harder to dismiss as vague.

A final issue concerns inclusivity. Domestic violence is gendered in its prevalence, consequences, and social structure, but technology-facilitated abuse can affect women, men, LGBTQ+ victims, disabled victims, migrants, older adults, and adolescents (Kadir, 2026). A victim-centred model should recognise gendered patterns without making protection inaccessible to victims who do not match the most familiar profile. Digital abuse may have specific forms in queer relationships, including threats of outing, control over online identity, or disclosure of sexual material to family or community (Løkkeberg et al., 2024). Migrant victims may face threats involving immigration documents and transnational family networks. Disabled victims may be controlled through assistive technologies. The legal model should remain attentive to those variations while preserving the central idea: technology becomes legally relevant when it is used to control a person's practical freedom within an intimate or family relationship (Powell & Stockley, 2026).

CONCLUSION

Technology-facilitated domestic violence exposes a classification problem in contemporary law. Digital abuse is often processed as cyber harassment, privacy invasion, communications misconduct, or platform harm, while the domestic structure of control remains under-analysed. A better legal reading treats technology as the medium, not the essence, of the abuse. The relevant question is whether digital conduct forms part of coercive control through surveillance, intimidation, humiliation, sexual leverage, economic restriction, isolation, or post-separation domination. The Serious Crime Act 2015, the Domestic Abuse Act 2021, the Domestic Abuse (Scotland) Act 2018, New South Wales coercive-control reforms, the Online Safety Act 2023, the EU Digital Services Act, and Australia's Online Safety Act 2021 each offer partial tools. None is sufficient alone. Domestic violence law must connect course-of-conduct reasoning with digital-risk awareness, platform governance, and careful protection-order drafting.

The most defensible model is victim-centred but procedurally restrained. It recognises digital coercive control, incorporates digital indicators into risk assessment, updates protection orders for networked abuse, requires platform cooperation, and regulates evidence collection through necessity, specificity, minimisation, and protected disclosure. This model does not treat every unpleasant online interaction as domestic violence. It asks whether the conduct restricts the victim's autonomy in a relational pattern of domination. That distinction is legally important. It protects victims whose abuse has moved from the home into devices, while keeping criminal law anchored in proof, proportionality, and fair process.

REFERENCES

Bailey, L., Hulley, J., Gomersall, T., Kirkman, G., Gibbs, G., & Jones, A. D. (2024). The networking of abuse: Intimate partner violence and the use of social technologies. *Crime & Delinquency.*

Boxall, H., Lawler, S., & Morgan, A. (2025). Unpacking Variation in Technology-Facilitated Intimate Partner Violence: A Conceptual and Empirical Analysis. *Journal of Family Violence*. https://doi.org/10.1007/s10896-025-00928-8

Brennan, I., & Myhill, A. (2022). Coercive Control: Patterns in Crimes, Arrests and Outcomes for a New Domestic Abuse Offence. *The British Journal of Criminology*, *62*(2), 468–483. https://doi.org/10.1093/bjc/azab072

Emezue, C., Chase, J. D., Udmuangpia, T., & Bloom, T. L. (2022). Technology-based and digital interventions for intimate partner violence: A systematic review and meta-analysis. *Campbell Systematic Reviews*, *18*(3). https://doi.org/10.1002/cl2.1271

Gutowski, E. R., & Goodman, L. A. (2023). Coercive Control in the Courtroom: the Legal Abuse Scale (LAS). *Journal of Family Violence*, *38*(3), 527–542. https://doi.org/10.1007/s10896-022-00408-3

Henry, N., Gavey, N., & Johnson, K. (2023). Image-Based Sexual Abuse as a Means of Coercive Control: Victim-Survivor Experiences. *Violence Against Women*, *29*(6–7), 1206–1226. https://doi.org/10.1177/10778012221114918

Hilton, N. Z., Eke, A. W., Kim, S., & Ham, E. (2023). Coercive control in police reports of intimate partner violence: Conceptual definition and association with recidivism. *Psychology of Violence*, *13*(4), 277–285. https://doi.org/10.1037/vio0000457

Kadir, Z. K. (2024). Psychoanalytic and Crime: Is Freud's Theory Still Applicable in Criminological Research? *Media Keadilan: Jurnal Ilmu Hukum*, *15*(2), 95–110.

Kadir, Z. K. (2025). Memecah Siklus Kematian Keluarga: Analisis Kebijakan Kriminal Jepang terhadap Familicide di Masyarakat Urban. *Konsensus: Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi*, *2*(1), 88–109.

Kadir, Z. K. (2026). Uji Klasifikasi Yudisial dalam Pembunuhan terhadap Gender: Honor Killing dan Intimate Partner Femicide. *RISOMA : Jurnal Riset Sosial Humaniora Dan Pendidikan*, *4*(1), 313–326. https://doi.org/10.62383/risoma.v4i1.1506

Leitão, R. (2021). Technology-Facilitated Intimate Partner Abuse: a qualitative analysis of data from online domestic abuse forums. *Human–Computer Interaction*, *36*(3), 203–242. https://doi.org/10.1080/07370024.2019.1685883

Lucas, D. S., Fuller, C. S., & Packard, M. D. (2022). Made to be Broken? A Theory of Regulatory Governance and Rule-Breaking Entrepreneurial Action. *Journal of Business Venturing*, *37*(6).

Lucas, K. T. (2022). Deepfakes and Domestic Violence: Perpetrating Intimate Partner Abuse Using Video Technology. *Victims & Offenders*, *17*(5), 647–659. https://doi.org/10.1080/15564886.2022.2036656

Munro, N. A. R. (2025). Should Medical Experts Giving Evidence in Criminal Trials Adhere to EFNSI Forensic Guidelines in Evaluative Reporting. *Forensic Sciences*, *5*(1), 13. https://doi.org/10.3390/forensicsci5010013

Myhill, A., Hohl, K., & Johnson, K. (2023). The 'officer effect' in risk assessment for domestic abuse: Findings from a mixed methods study in England and Wales. *European Journal of Criminology*, *20*(3), 856–877. https://doi.org/10.1177/14773708231156331

Powell, A., & Stockley, C. (2026). A Continuum of Tactics: Technology Facilitated Abuse in Family Violence Crisis Contexts. *Australian Social Work*, 1–14. https://doi.org/10.1080/0312407X.2026.2640928

Reed, L. A., Brown, M. L., Kappas Mazzio, A., Messing, J. T., Grimm, K., Wachter, K., Jiwatram-Negrón, T., & Gonzalez-Pons, K. (2025). Patterns of Technology-Based Abuse Among Adult Intimate Partner Violence Survivors and Associations with Offline Abuse. *Journal of Interpersonal Violence*, *40*(13–14), 3284–3306. https://doi.org/10.1177/08862605241268782

Rogers, E. M., & Davis, J. (2024). The Research Utility of the National Violent Death Reporting System for Understanding Homicide Trends. *Journal of Contemporary Criminal Justice*, *40*(1), 26–47. https://doi.org/10.1177/10439862231189985

Rogers, M. M., Fisher, C., Ali, P., Allmark, P., & Fontes, L. (2023). Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review. *Trauma, Violence, & Abuse*, *24*(4), 2210–2226. https://doi.org/10.1177/15248380221090218

Sorochinski, M., & Varvaro, J. (2023). Technology facilitated sexual violence and abuse: exploring the what, who, where, why, when, and how of the 21 st century interpersonal crime. *Contemporary Justice Review*, *26*(1), 111–121. https://doi.org/10.1080/10282580.2023.2216717

Storey, J. E., & Pina, A. (2025). Technology-Facilitated Intimate Partner Violence: An Examination of Prevalence, Perpetration Type and Methods and the Impact of COVID-19. *Journal of Interpersonal Violence*. https://doi.org/10.1177/08862605251391169

Tolmie, J., Smith, R., & Wilson, D. (2024). Understanding Intimate Partner Violence: Why Coercive Control Requires a Social and Systemic Entrapment Framework. *Violence Against Women*, *30*(1), 54–74. https://doi.org/10.1177/10778012231205585

Torp Løkkeberg, S., Ihlebæk, C., Brottveit, G., & Del Busso, L. (2024). Digital Violence and Abuse: A Scoping Review of Adverse Experiences Within Adolescent Intimate Partner Relationships. *Trauma, Violence, & Abuse*, *25*(3), 1954–1965. https://doi.org/10.1177/15248380231201816

Weissflog, M., Ham, E., Jung, S., Kim, S., Eke, A. W., Campbell, M. A., & Hilton, N. Z. (2025). Measuring coercive control from police reports of intimate partner violence. *Journal of Criminal Justice*, *99*, 102442. https://doi.org/10.1016/j.jcrimjus.2025.102442

Williams, K. E. G., Votruba, A. M., & Eagle, R. S. (2025). Why Motive Matters: The Appraisal of Criminal Aims. *Behavioral Sciences*, *15*(9), 1244. https://doi.org/10.3390/bs15091244

Wilson, K. D., & Fritz, P. A. T. (2023). Psychometric Properties of the Coercion in Intimate Partner Relationships Scale. *Assessment*, *30*(2), 448–457. https://doi.org/10.1177/10731911211025628