

Legal Responses to Algorithmic Harassment and Digital Coercion in Intimate Contexts

Loredana TEREĆ-VLAD¹, Edi-Marian TIMOFTE²

¹ Assistant Professor, PhD, Ștefan cel Mare University of Suceava, Romania, loredanaterec@gmail.com

² Assistant Professor, PhD Candidate, Ștefan cel Mare University of Suceava, Romania.

Abstract

Intimacy has become algorithmically disrupted in the digital era. The introduction of algorithmic companion suggestions, AI-powered surveillance in social interactions, and deeper transformations to connection have changed human interactions, power, manipulation, and harm. This paper examines an emerging, yet under-explored area of law: algorithmic harassment and digital coercion in intimate situations. Existing legal mechanisms for addressing intimate harm - broadly termed as physical and psychological abuse - are not sufficient to address the complex nature of silent intrusions of algorithmic manipulation - covert surveillance, nudging of behaviours, and personalization that strips away autonomy. Using literature from multiple disciplinary sources, this paper will provide a critical evaluation of the existing international legal mechanisms for addressing intimate harm and will argue that the complex nature of the harassments discussed requires a legal re-imagining in terms of algorithmic harassment and coercion as a distinct form of intimate harm that requires regulation and platform accountability and part of a the broader legal framework of rights-based protection. By shedding light on the absence of visibility regarding algorithmic abuse, this paper contributes to the areas where law, technology, and human vulnerability intersect, at a time where legal reform is needed, due, and obviously inescapable.

Keywords: algorithmic harassment, digital coercion, intimate partner abuse, AI and law, privacy rights.

How to cite: Terec-Vlad, L., & Timofte, E.M. (2025) Legal Responses to Algorithmic Harassment and Digital Coercion in Intimate Contexts. *Anuarul Universității "Petre Andrei" din Iași Fascicula: Asistență Socială, Sociologie, Psihologie*, 33, 290-301. <https://doi.org/10.63331/upasw/33/27>

1. Introduction

Technology no longer defines personal intimacy in terms of physical closeness or communication; it is now algorithmically defined, deconstructed, monitored, and ultimately exploited. Intimate relationships are conditioned by technological mediators: the smart device that tracks your movements and habits, social technologies that encourage choices, and algorithms that direct emotional activity and responses¹. As we integrate technology into personal aspects of human life, we normalize new possibilities for abuse that the law has hardly begun to recognize.

Algorithmic harassment and digital coercion are emerging as differentiated and novel forms of intimate partner abuse². Unlike conventional abuse, often visible or physically definable, the behaviors that define digital or cyber abuse are part of the very code that structures digital life. From automated content feeds that facilitate isolation, spyware for ubiquitous surveillance, to shared accounts, passwords, or cloud histories, perpetrators cause particular facets of digital infrastructure to reproduce coercive control in every crevice of the victim's being. These acts are not accidental or incidental uses of technology, but a major shift in how power and control demonstrate in relationships³.

Yet, while harms are becoming more complex and regular, our legal systems remain based on outdated models for understanding violence. Most legislative regimes are built on discrete acts - Assault, threats, stalking - and are unable to grasp the non-physical, diffused, and technologically mediated nuisances of algorithmic abuse. Additionally, laws impose binary logic of consent and harm, both of which cannot align with new grey areas of digital influence and behavioral manipulation⁴. Incredibly, a gap exists between the realities of digital coercion and protections afforded by the law. Some jurisdictions, such as New Zealand and the UK, have seen some progress to revise legislation on this emergent area; their inability to see beyond criminalization may leave the systemic and relational characteristics of coercive dynamics less understood⁵. Victims, particularly women and gender-diverse people, report feeling like they are managing legal remedies from a fragmented system, which ultimately re-traumatizes them, especially in processes that were not invented to understand algorithmic intrusion or non-consensual technological entanglement.

This paper makes three significant contributions. First, it frames algorithmic harassment and digital coercion as two independent legal categories demanding its own appreciation⁶. Second, it analyzes limitations of the current international legal responses to algorithmic harassment and digital coercion and identifies deficiencies in law, enforcement

¹ I. Apostu, *Female Management – Between Motherhood and Career*, in *Ecoforum* 6, no. 1 (2017): 1–36.

² P. P. Nistor and O.-A. Neagu, *Fear – an Essential Characteristic of Recent Times*, in *Logos Universality Mentality Education Novelty: Social Sciences* 13, no. 1 (2024): 38–49, <https://doi.org/10.18662/lumenss/13.1/100>

³ T. Kadri, *Networks of Empathy*, in *Utah Law Review* 1075, no. 4 (2020), <https://doi.org/10.26054/0D-QSHR-9WVA>

⁴ R. King, *Digital Domestic Violence: Are Victims of Intimate Partner Cyber Harassment Sufficiently Protected by New Zealand's Current Legislation?*, in *Victoria University of Wellington Law Review* 48, no. 4 (2017): 579–600.

⁵ H. Douglas, *Legal Systems Abuse and Coercive Control*, in *Criminology & Criminal Justice* 18, no. 1 (2018): 84–99, <https://doi.org/10.1177/1748895817728380>

⁶ P. P. Nistor and C. C. Achiței, *The Cultural Importance of Integrating Socially Assisted Vulnerable Groups within Society – The Case of the Roma Community*, in *Logos Universality Mentality Education Novelty: Philosophy & Humanistic Sciences* 11, no. 1 (sup1) (2024): 87–103, <https://doi.org/10.18662/lumenphs/11.1Sup1/81>

and interpretation⁷. This will demonstrate how the current reality demands a rethinking of any potential protective legislative process that goes beyond individual incidents of violence and considers the political nature of algorithmic violence in intimate contexts. Third, the paper proposes a new legal paradigm that considers relational autonomy, human rights and platform accountability. By framing digital abuse in intimate contexts not just as a technological aberration but as a failure of legal imagination and structural components, the paper calls for an urgent, interdisciplinary reform of current laws⁸.

2. Algorithmic Harassment: A Hidden Form of Intimate Violence

The growing presence of algorithmic systems in daily life has allowed for novel forms of control that often invisible to the ones being abused. When considered in the context of intimate relationships, algorithmic systems can be co-opted to surveil, manipulate, and harass a partner in ways that were once impossible or unrecognizable by law. Algorithmic harassment involves the use, or misuse, of automated digital systems to coerce, track behaviours, or provide algorithmic isolation by curating content, overseeing surveillance, and removing someone from digital social spaces. Algorithmic harassment differs from other forms of abuse and control not just by the use of technology, but through the automation logic. For instance, a partner might use algorithms on shared platforms to manipulate what the victim sees or is prevented from seeing; curating reality to reinforce dependency or fear. The algorithmic amplification of harmful content, the weaponization of recommendation engines, and the weaponization of location tracking and behaviour engagement are hardly innocuous ways of control. Freed et al. have noted that even very simple digital tools like GPS and shared calendars have become part of CBA's toolkit, rendering smartphones and applications to be tools of fear⁹.

In addition, various digital platforms that unknowingly support misuse, support those derogatory functions with design flaws. Many of these systems have adequate privacy granularity, audit log deficiency, or insufficient protection against modeling, oversurveillance or algorithm manipulation. In settings where AI has an active and foundational role in producing content, the possibility for algorithmically mediated harassment is amplified. This is because the victim can be issued targeted content (suggestive ads, reminders, threatening posts) as a result of an abuser's indirect but effective digital footprint - a vicious feedback loop that causes emotional destabilization¹⁰. Unlike a direct act of abuse where the abuser can be traced and targetable, algorithmic harassment challenges basic legal presumptions about intent and attribution. An abuser might "nudge" the system in one of many ways (liking specific content, manipulating keywords, or by pings requiring the display of geographic coordinates); once this occurs, platform algorithm processes a resulting pattern of harassment. This delegation of harm and abuse makes legal attribution or demonstration

⁷ A. Corsei and M.-A. Ștefănoaia, *Romania and Human Rights According to European Regulations*, in *Acta Universitatis Danubius. Juridica* 18, no. 2 (2022), <https://dj.univ-danubius.ro/index.php/AUDJ/article/view/1860>

⁸ N. Henry and A. Powell, *Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law*, in *Social & Legal Studies* 25, no. 3 (2016): 397–418, <https://doi.org/10.1177/0964663915624273>

⁹ D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell, *A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology*, in *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018): 1–13, <https://doi.org/10.1145/3173574.3174241>

¹⁰ W. O'Brien and M. H. Maras, *Technology-Facilitated Coercive Control: Response, Redress, Risk, and Reform*, in *International Review of Law, Computers & Technology* 38, no. 2 (2024): 174–194, <https://doi.org/10.1080/13600869.2023.2295097>

of malicious intent difficult because the algorithm did not do it intentionally based on what was typically "neutral" inputs¹¹.

In some circumstances, the acts of harassment can be indirect, depending on algorithmic gaslighting to confuse a target's sense of realness: the victim's experience could be undermined by suppression of viewed content, by manipulating threads of memory (e.g., by deleting previous digital conversations), or by repeated exposure of threatening associations. The point made by Dragiewicz et al., is that "technology-facilitated coercive control" incorporates the system, as a form of coercive control using design of the platform itself, likely offering few if any trails of conventional proof¹². Legal approaches to algorithmic harassment to date have been reactive and patchwork, where jurisdictions may classify the behaviour to a larger social problem such as cyberstalking or another broader category of harassment, and legal consequences or even legal appeal does not account for algorithmic harassment as structural harassment that cannot be seen, but that has consequences and therefore changes the framing of these actions. The absence of clearly defined considerations for algorithmic harassment has important effects: courts may dismiss legal actions or say that the action is not intentional, because there were no "proof" or evidence shows there was also no "physical harm". It is illogical for courts to expect victims to understand the complex mechanism of algorithmic harassment, as courts are not the best places for determining (and therefore adjudicating) cause and effect in a computational process, or situational abuse perpetrated through a platform-mediated process. Moreover, the very terms of law also bring barriers understanding of lived experience surrounding algorithmic harassment; with harassers continuing their harassment, and sometimes putting up barriers that seem impossible to break (constructing the experience around constancy, inescapability, and biochemical erosion of mental and emotional autonomy). In rural and remote experiences, as Harris et al. have noted, it is compounded by geographical isolation such as when relying completely on the devices or platform that forced them to withdraw¹³. Claustrophobic control connects to physical, digital, intimate, structural types of control that can potentially lead to irremediable harms. In this chapter, I am making the case that we understand algorithmic harassment as a new and qualitatively different experience, not just an evolution of abuse; that fundamentally changes the architectural relations around control in intimate life. Understanding algorithmic harassment as a new form of abuse is important for future legal responses. Legal systems need to evolve to address the conditions of algorithmic abuse; not only the consequences, but the architecture of how systems are created, who is empowered by them, and how these can be held to accountability. Without this new legal framing, victims will continue to form patterns of algorithmic harm and abuse

¹¹ A. Koshiyama, E. Kazim, P. Treleaven, P. Rai, L. Szpruch, G. Pavey, G. Ahamat, F. Leutner, R. Goebel, A. Knight, J. Adams, C. Hitrova, J. Barnett, P. Nachev, D. Barber, T. Chamorro-Premuzic, K. Klemmer, M. Gregorovic, S. Khan, E. Lomas, A. Hilliard, and S. Chatterjee, *Towards Algorithm Auditing: Managing Legal, Ethical and Technological Risks of AI, ML and Associated Algorithms*, in *Royal Society Open Science* 11, no. 5 (2024): 1–34, <https://doi.org/10.1098/rsos.230859>

¹² M. Salter, M. Dragiewicz, J. Burgess, and A. Matamoros-Fernandez, *Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms*, in *Feminist Media Studies* 18, no. 3 (2018): 609–625, <https://doi.org/10.1080/14680777.2018.1447341>

¹³ B. Harris and D. Dragiewicz, *Digital Coercive Control: Insights From Two Landmark Domestic Violence Studies*, in *British Journal of Criminology* 59, no. 3 (2019): 530–550, <https://doi.org/10.1093/bjc/azy052>

that are ultimately imperceptible to a law that remains anchored in the language of bruises and threats, instead of algorithms and code¹⁴.

3. Digital Coercion and Consent under Algorithmic Influence

For a long time, consent has been a central feature of legal norms regulating intimate relationships. However, in the world of algorithm effect and digital monitoring, classic definitions of consent - independently developed, informed and reusable - are being reduced. Digital coercion cannot always take the form of overating hazards or demands. Instead, it may appear through control of ongoing monitoring, underlying pressure, algorithm elbow, and digital spaces that erase a partner's ability to act as an autonomous agent. In intimate places, force can take the form of unauthorized access to equipment, social media or cloud storage; Forced space sharing; Or using tracking or monitor software that is secretly installed on a partner's phone. The nature of this control is at times presented as "care", or "concern", making it more difficult to identify and resist. As Woodlock writes, "Technology use in domestic violence is not just a convenience for abusers, but an intentional method of extending abusive control over a victim"¹⁵.

Furthermore, consent manipulation can occur without the need for direct communication. Abusers might draw upon expectations around "password-sharing", or "digital openness", in relationships to normalize insidious practices. In this space, asking for access sometimes becomes unnecessary; surveillance is unchecked and refusal is guilt-laden. Unfortunately, the law is still bound to narrow interpretations of consent, concentrating on yes or no consensuality and ignoring the incremental, compounding erosion of agency due to digital reliance and fear of punishment that occurs over time. Newer technologies exacerbate this situation as AI-driven features of personalization, smart devices for home and health that passively capture data, create additional avenues for coercion. As an example, under "tracking health" a partner could monitor realtime reports of heart rate variability, sleep activity, +/-variances from the daily resting location. In many cases, through silence or insinuation, these reports may act as a primary normalizing follow-up to behaviour. As Harris and Dragiewicz outline, algorithmic transparency renders escape to a greater extent; even physical separation may not equal privacy or psychological safety to persons subject to intimate partner violence¹⁶.

Perhaps one of the more troubling developments is in the use of deep fake technology, and image-based sexual coercion (IBSC). Targeted victims are threatened with the release of synthetic or manipulated photographs or videos, even where there is no original image. The weaponizing of intimate data – real or faked (primed or unprimed) – robs a person of dignity, and the ability to define and control their own body and story. Often there are limited mechanisms for legal systems to address, since establishing falsified or malicious intention can be almost impossible when the materials produced are algorithmically generated. Proof is difficult if not impossible due to the complex interference associated with fabricated evidence such as fraud, impersonation, identity crime, or revenge

¹⁴ L. Vlad, *The Family Where To? From the "Solid" Perspective to "Liquid" Perspective*, in *Postmodern Openings* 8, no. 1 (2017): 67–80.

¹⁵ D. Woodlock, *The Abuse of Technology in Domestic Violence and Stalking*, in *Violence Against Women* 23, no. 5 (2017): 535–558, <https://doi.org/10.1177/1077801216646277>

¹⁶ N. Henry, N. Gavey, and K. Johnson, *Image-Based Sexual Abuse as a Means of Coercive Control: Victim-Survivor Experiences*, in *Violence Against Women* 29, no. 6–7 (2022): 1206–1226, <https://doi.org/10.1177/10778012221114918>

porn¹⁷. Legal definitions of coercion may create challenges for victims who fundamentally engage (or disconnect) from their legal rights and responsibilities with respect to consent. In her analysis of New Zealand's legal approach, King captures the fears of victims and whether the digital trace/reality will be legitimized, misunderstood or worse still, utilized to bring legal action. The definitional invisibility of coercion, assurance that there is no forensic evidence, and the legal system and its definition of digital manipulation creates institutional gas lighting and provides evidence of secondary victimization¹⁸.

This chapter maintains that legal narratives about consent must distance themselves from a binary of yes or no and endpoint on its own as a definitional basis, particularly in digitally mediated relationships. Lawmakers must acknowledge the spectrum of coercion via relentless digital presence, the imbalanced power dynamics of technology in intimate relationships, and the inability in algorithmic contexts to decipher between preference and obligation or coercion. For individuals with relationships within the trajectory of dominance and abuse to obtain legal or appropriate rights that protect their interest in the digital age, a more contextualized, informed (of technology) and continuous understanding (of consent) is needed.

4. Legal Responses and Gaps in International Frameworks

While technology is changing the ways that intimate abuse occurs, legal frameworks across the globe are shackled to antiquated assumptions, fragmented interpretations, and reactive rather than preemptive approaches. Some jurisdictions have recognized technology facilitated violence (TFV) as an emergent issue, with a few developing a comprehensive and coherent response to algorithmic harassment and digital coercion specifically in the context of intimate relationships. Legal reform has usually not kept pace with both the rate of technological change and the practical behaviours of perpetrators.

At the international level, there are some significant instruments, including the Istanbul Convention and Convention on Cybercrime (Budapest Convention), that partially contain protections. The Istanbul Convention recognizes psychological violence and stalking, which can encompass some digital coercion, but lacks measures to address algorithmic abuse or control through AI; it recognizes the importance of psychological abuse and stalking, that may be theoretically relevant but does not have specific legal protections for some types of coercive digital exploitation. The Budapest Convention specifically recognizes unauthorized access and data breaches but does not address ways in which lawful access is manipulably used in domestic environments. This creates a significant legal blind spot: many of the harms associated with coercion through an its algorithmic nature does not constitute illegality per se, but involves the misuse of legal digital affordances in order to exert control.

At the national level, legal systems betray similar deficiencies. For example, the offence of controlling or coercive behaviour in England and Wales is a significant milestone which was introduced in 2015. However, as Wiener shows, it remains limited when the coercion is algorithmically diffused and technologically embedded. The justice system

¹⁷ C. Wiener, *From Social Construct to Legal Innovation: The Offence of Controlling or Coercive Behaviour in England and Wales*, in M. McMahon and P. McGorrrery (eds.), *Criminalising Coercive Control* (Singapore: Springer, 2020), 159–175, https://doi.org/10.1007/978-981-15-0653-6_8

¹⁸ E. Pavan and A. Lavorgna, *Promises and Pitfalls of Legal Responses to Image-Based Sexual Abuse: Critical Insights from the Italian Case*, in A. Powell, A. Flynn, and L. Sugiura (eds.), *The Palgrave Handbook of Gendered Violence and Technology* (Cham: Palgrave Macmillan, 2021), https://doi.org/10.1007/978-3-030-83734-1_27

typically struggles to assign responsibility when abusers act by exercising a digital means that seems passive and/or indirect¹⁹. From my experience, having to prove both that they have a "serious effect" on the victim and that there is a "pattern of behaviour" typically foils any ability they have to pursue justice in the case of algorithmic harassment, where the evidence is apposite, ephemeral and rarely understood by judicial actors.

Attempts to legislate against image-based abuse (e.g., revenge porn) are necessary, but utilise limited horizons about coercion. Pavan et al note that even with legally symbiotic responses like, "Red Code" law in Italy, it remains unclear how effectively they operate on the ground because they reduce violations into isolated events, which fail to address how they are tactics in a wider pattern of control used in intimate partnerships²⁰.

The challenge of addressing and understanding abuse through law is compounded by structural and epistemic issues faced by law enforcement and the courts. Powell et al note that police and frontline services have limited awareness and training to identify, document and prosecute cases of TFV²¹. Victims of algorithmic abuse express significant concerns about their credibility and often report to police about the police experience being dismissed or laughed at, particularly when they cannot provide a detailed account of how abusers operated with "invisible" algorithms or how abusers initiated subtle alterations of their content, devices or platforms. This procedural blindness reinforces the structural sanctuary of impunity for perpetrators, while amplifying the ineffective adaption of justice systems to respond to society's techno-societal advancement.

There are repeated tensions in legal considerations about the boundaries of freedom of expression, technological neutrality, and the protection of victims. O'Brien and Powell articulate the reliance on criminal law can yield unpredictable results, including the broad proliferation of censorship by the platforms, surveillance creep, and the punitive backlash. O'Brien and Powell are firm supporters of proposing and operationalising instead a multi-level legal ecology approach which, in practical terms, means creating responses to algorithmic behaviours through a more comprehensive and inclusive, criminal, civil, regulatory and/or administrative responses that are contextualised in internationally recognised human rights norms²².

A related concern is the absence of cooperative and aligned digital abuse protections. Chikwe et al demonstrate that the absence of a unified conceptual and legal framework for addressing TFV causes a form of fragmented protections and jurisdictional dead zones²³. Given that many online and cloud powered technologies are allied, the ramifications of these legal incompatibilities and decisions exacerbate the equivocal terrains where victims cannot pursue effective harm reduction responses, especially in the context of cross border cases.

¹⁹ A. Powell and N. Henry, *Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Service Sector Perspectives*, in *Police Practice and Research* 28, no. 3 (2016): 291–307, <https://doi.org/10.1080/10439463.2016.1154964>

²⁰ C. F. Chikwe, N. E. Eneh, and C. U. Akpuokwe, *Conceptual Framework for Global Protection Against Technology-Enabled Violence Against Women and Girls*, in *International Journal of Science and Research Archive* 11, no. 2 (2024): 279–287, <https://doi.org/10.30574/ijrsra.2024.11.2.0415>

²¹ N. Henry and A. Powell, *Technology-Facilitated Domestic and Sexual Violence: A Review*, in *Violence Against Women* 26, no. 3–4 (2020): 182–200, <https://doi.org/10.1177/1077801219888021>

²² N. Henry and A. Powell, *Beyond the 'Sext': Technology-Facilitated Sexual Violence and Harassment Against Adult Women*, in *Journal of Criminology* 48, no. 1 (2014): 104–118, <https://doi.org/10.1177/0004865814524218>

²³ S. Walklate, K. Fitz-Gibbon, and J. McCulloch, *Is More Law the Answer? Seeking Justice for Victims of Intimate Partner Violence Through the Reform of Legal Categories*, in *British Journal of Criminology & Criminal Justice* 18, no. 1 (2017): 115–131, <https://doi.org/10.1177/1748895817728561>

Legal systems need to first recognise that data-driven coercion and algorithmic harassment cannot be viewed as marginal issues, this is a significant and responsible shift in framing the history of people abuse and interpersonal violence moving forward in the digital age. It is therefore crucial that legal definitions are clarified to facilitate the recognition of the abuse, but importantly, the contextual architecture and operational logics driving digital coercion. It should clearly articulate the instances of consent being vitiated through the use of digital coercion; defining harms as not only physical injuries, but also psychological and relational harms by algorithms; and obliging platforms to take great care in their pieces of digital artefact design, which rely on algorithmic choices which could lead to abuse.

As long as legal systems remain tethered to analog logics of harm, causality, and intent, they will remain structurally incapable of confronting a digital architecture of abuse that thrives precisely in the absence of visibility, linearity, and human volition.

5. Rethinking Regulation: Towards a Rights-Based Digital Intimacy Framework

The insufficiency of existing legal responses to algorithmic harassment or digital coercion in relational contexts is not merely an enforcement issue. It is an issue of legal imagination. To tackle this issue requires more than tinkering with existing types of harm or expanding the criminal code. It requires a rupture: moving from event-based regulation to structural accountability, from individual blame to systems blame, and from remedial justice to preventative protection. A rights based regulatory framework ultimately needs to recognize relational autonomy as a priority legal interest. The traditional legal conception of autonomy is concerned primarily with the individual as free from obstruction, and in the case of digital coercion, autonomy can be compromised through ongoing digital manipulation, especially in a socially and emotionally entangled context. There are a number of interesting issues at play regarding gray areas where collaborative projects, actively engaged by users in abuse and where systems themselves enable or advance abusive relational dynamics. The law needs to recognize these new facets of 'coercion-by-design' to ensure platforms are liable not just for content, but for the design attributes that enable surveilling, controlling, and limiting²⁴.

A critical aspect of reform is design justice - requiring that digital platforms can engage with protective features for users considered vulnerable in relational contexts, such as granular privacy settings, algorithmic explainability, and features that help users identify and report coercive behaviours. As Henry et al. observe in their systematic review of technology-enabled domestic violence, the majority of systems were created on the assumption there will always be goodwill from users in using or managing abuse-related features. A regulatory architecture that grounds itself in user protection would establish obligations that would not only require accountability from users, but designers, developers, and service providers too.

Moreover, the way that consent is understood - legally - needs to be reformulated, incorporating conditions of freedom, power, and context along with affirmative acts. The power asymmetries attached to a user's digital dependence can cause the semblance of a choice to be indistinguishable from coercion. On that note, feminist legal scholars have asserted contexts for consent for a long time - a recognition that I now argue should also be

²⁴ E. Farries and T. Sturm, *Feminist Legal Geographies of Intimate-Image Sexual Abuse: Using Copyright Logic to Combat the Unauthorized Distribution of Celebrity Intimate Images in Cyberspaces*, in *Environment and Planning A: Economy and Space* 51, no. 5 (2019): 1145–1165, <https://doi.org/10.1177/0308518X18786964>

applied in the area of algorithmic use, where the array of influence is customizable, persistent, and often invisible.

Platform responsibility is a critical second element. The law should regard platforms not as neutral channels of knowledge transfer but as distinct agents of design authority and social responsibility. Platforms that permit clandestine tracking, unseen surveillance, and permanently retained data, have a responsibility to govern the standards of duty of care, data minimization, and transparency of impact. This includes creating reporting pathways, some form of ethical auditing of algorithms, and providing real-time victim support within its services.

Finally, alignment which focuses on international considerations is necessary. Fragmented legal regimes create opportunities for perpetrators who can exploit jurisdictions to culpably avoid accountability. One rationale for a standardized, transnational, and legislative regulatory regime offered by human rights norms, would provide minimum protections for people regardless of their sphere of influence. As Farries highlights through the lens of copyright reasoning applied to intimate images, novel forms of protection can still be realized with odd legal devices if they work from a perspective of victimization and digital possibility.

This chapter proposes that digital intimacy should not be considered a secondary legal consideration any longer. It is a primary site of autonomy, dignity, and privacy that is affirmed - or denied. A rights-based regulatory architecture requires anticipatory, intersectional, and adaptive measures based on the premise that technological abuse is a characteristic of systems allowed to run unchecked, rather than an exception. Only then, can the law reflect the depth of harm that it wishes to ameliorate. If the law continues to view harm through the narrow lens of physicality and intention, while algorithms orchestrate control through invisibility and indifference, we risk sanctioning a future in which intimacy itself becomes the most vulnerable frontier of digital colonization - unregulated, unprotected, and algorithmically exploited.

6. Conclusion: Protecting the Intimate Self in the Age of Algorithms

While there are many ways we can conceptualize our analysis of algorithmic harassment and digital coercion in intimate contexts - harassment that is technologically savvy, socially contextualized, and legally undeveloped - this article has focused on these forms of abuse that are not necessarily violent, but emerge through the unseen or perfunctory actions we call "norms," such as surveillance, manipulation through platforming, datafied intimacy, and the nonchalant weaponization of code. What makes these forms of abuse particularly menacing is not only their invisibility, but their normalization - texting instead of calling, being monitored by your data, adduced as reminders or even convenience rather than infringements, tenderness rather than malice, even algorithmic necessity.

The law, with its ideas of bodily harm, overt threats, and linear accomplishment, struggles against these ambient and systemic forms of destruction. It has to ask for evidence where there is only a pattern. It asks for intent where there is only influence. It operates under the assumption of agency where there is only digital subsidy. Therefore, the legal system has the potential to appear complicit - not maliciously, but as a function of historical thoughtlessness. Absent an update in legal spirit, algorithmic abuses risk continuing to flourish in veiled forms beneath the threshold of formal recognition: remaining legally uncontained zones of abuse and unregulated relationships, unacknowledged by courts or regulators who deny such forms of accountability or remedy.

An effective response requires more than legal adjustment; it requires a re-evaluation of violence, consent, and measures of harm within technologically saturated relationships. First, legal definitions that enhance relational vulnerability must become a discriminating factor within networked intimacies. Second, the conception that users engage with technology as free, informed agents, blurs the realities of redress for abuses engaged in asymmetries of knowledge, control, and emotional codependence.

Second, the legal gaze must turn away from content and forward towards the logic of the architecture inhospitable to human vulnerabilities - for example, how platforms ideologically expose users through their design, discourage technical engagement through defaults, proliferate application of control through purportedly "neutral" or automated alterations, and, in turn, reveal their power asymmetries in intimate spaces. It should not necessarily conclude that platforms are only liable for user content; we must also hold software responsible for enabling their signifiers toward violence over interpersonal engagements. We need a new digital duty of care and responsibility, especially in intimate spaces where stakes are more than reputational or economic, but psychological or emotional to the people involved.

Third, there must be a shift toward international legal harmonization of algorithmic coercion as gendered violence. Most victims engaging in digital domestic abuse, as well as traditional domestic abuse, are female or identify as gender diverse; to ignore this reality reinforces a degree of structural injustice. Legal development is not the only epistemological space - I suggest we meaningfully enhance legal innovation on acceptable usages of feminist jurisprudence for restorative digital practices, digital ethics, and human rights towards participatory legal grammar that we can articulate what existing codes have not yet seen.

Fourth, we need a legal diagnosis of legal futurism! Law needs to do more than respond to harm; it must think ahead to how harms, systemic domination and power relationships exist, and anticipate them through design standards, algorithmic audits, and interdisciplinary conversations between engineers, ethicists, survivors, and communities. Jurisprudence needs to now evolve at the speed of code or alternatively risk becoming a trusted witness to the commencement of the new age of violence.

If we do not unshake our vision of harm from a focus on physicality and intention and allow algorithms to orchestrate the pliability of control through invisibility and indifference, we risk institutionalizing a future in which intimacy itself is our most defenseless arena of digital colonization - unmonitored, unprotected, and algorithmically exploited.

References

- Apostu, I. 2017. "Female Management – Between Motherhood and Career." *Ecoforum* 6, no. 1: 1–36.
- Chikwe, C. F., N. E. Eneh, and C. U. Akpuokwe. 2024. "Conceptual Framework for Global Protection Against Technology-Enabled Violence Against Women and Girls." *International Journal of Science and Research Archive* 11, no. 2: 279–287. <https://doi.org/10.30574/ijjsra.2024.11.2.0415>
- Corsei, A., and M.-A. Ștefănoaia. 2022. "Romania and Human Rights According to European Regulations." *Acta Universitatis Danubius. Juridica* 18, no. 2. <https://dj.univ-danubius.ro/index.php/AUDJ/article/view/1860>
- Douglas, H. 2018. "Legal Systems Abuse and Coercive Control." *Criminology & Criminal Justice* 18, no. 1: 84–99. <https://doi.org/10.1177/1748895817728380>

- Farries, E., and T. Sturm. 2019. "Feminist Legal Geographies of Intimate-Image Sexual Abuse: Using Copyright Logic to Combat the Unauthorized Distribution of Celebrity Intimate Images in Cyberspaces." *Environment and Planning A: Economy and Space* 51, no. 5: 1145–1165. <https://doi.org/10.1177/0308518X18786964>
- Freed, D., J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell. 2018. "A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology." In *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–13. <https://doi.org/10.1145/3173574.3174241>
- Harris, B., and D. Dragiewicz. 2019. "Digital Coercive Control: Insights From Two Landmark Domestic Violence Studies." *British Journal of Criminology* 59, no. 3: 530–550. <https://doi.org/10.1093/bjc/azy052>
- Henry, N., and A. Powell. 2014. "Beyond the 'Sext': Technology-Facilitated Sexual Violence and Harassment Against Adult Women." *Journal of Criminology* 48, no. 1: 104–118. <https://doi.org/10.1177/0004865814524218>
- Henry, N., and A. Powell. 2016. "Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law." *Social & Legal Studies* 25, no. 3: 397–418. <https://doi.org/10.1177/0964663915624273>
- Henry, N., and A. Powell. 2020. "Technology-Facilitated Domestic and Sexual Violence: A Review." *Violence Against Women* 26, no. 3–4: 182–200. <https://doi.org/10.1177/1077801219888021>
- Henry, N., N. Gavey, and K. Johnson. 2022. "Image-Based Sexual Abuse as a Means of Coercive Control: Victim-Survivor Experiences." *Violence Against Women* 29, no. 6–7: 1206–1226. <https://doi.org/10.1177/10778012221114918>
- Kadri, T. 2020. "Networks of Empathy." *Utah Law Review* 1075, no. 4. <https://doi.org/10.26054/oD-QSHR-gWVA>
- King, R. 2017. "Digital Domestic Violence: Are Victims of Intimate Partner Cyber Harassment Sufficiently Protected by New Zealand's Current Legislation?" *Victoria University of Wellington Law Review* 48, no. 4: 579–600.
- Koshiyama, A., E. Kazim, P. Treleaven, P. Rai, L. Szpruch, G. Pavey, G. Ahamat, F. Leutner, R. Goebel, A. Knight, J. Adams, C. Hitrova, J. Barnett, P. Nachev, D. Barber, T. Chamorro-Premuzic, K. Klemmer, M. Gregorovic, S. Khan, E. Lomas, A. Hilliard, and S. Chatterjee. 2024. "Towards Algorithm Auditing: Managing Legal, Ethical and Technological Risks of AI, ML and Associated Algorithms." *Royal Society Open Science* 11, no. 5: 1–34. <https://doi.org/10.1098/rsos.230859>
- Nistor, P. P., and O.-A. Neagu. 2024. "Fear – an Essential Characteristic of Recent Times." *Logos Universality Mentality Education Novelty: Social Sciences* 13, no. 1: 38–49. <https://doi.org/10.18662/lumenss/13.1/100>
- Nistor, P. P., and C. C. Achiței. 2024. "The Cultural Importance of Integrating Socially Assisted Vulnerable Groups within Society – The Case of the Roma Community." *Logos Universality Mentality Education Novelty: Philosophy & Humanistic Sciences* 11, no. 1 (sup1): 87–103. <https://doi.org/10.18662/lumenphs/11.1Sup1/81>
- O'Brien, W., and M. H. Maras. 2024. "Technology-Facilitated Coercive Control: Response, Redress, Risk, and Reform." *International Review of Law, Computers & Technology* 38, no. 2: 174–194. <https://doi.org/10.1080/13600869.2023.2295097>
- Pavan, E., and A. Lavorgna. 2021. "Promises and Pitfalls of Legal Responses to Image-Based Sexual Abuse: Critical Insights from the Italian Case." In *The Palgrave Handbook of*

- Gendered Violence and Technology*, edited by A. Powell, A. Flynn, and L. Sugiura. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-83734-1_27
- Powell, A., and N. Henry. 2016. "Policing Technology-Facilitated Sexual Violence Against Adult Victims: Police and Service Sector Perspectives." *Police Practice and Research* 28, no. 3: 291–307. <https://doi.org/10.1080/10439463.2016.1154964>.
- Salter, M., M. Dragiewicz, J. Burgess, and A. Matamoros-Fernandez. 2018. "Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms." *Feminist Media Studies* 18, no. 3: 609–625. <https://doi.org/10.1080/14680777.2018.1447341>
- Vlad, L. 2017. "The Family Where To? From the 'Solid' Perspective to 'Liquid' Perspective." *Postmodern Openings* 8, no. 1: 67–80.
- Walklate, S., K. Fitz-Gibbon, and J. McCulloch. 2017. "Is More Law the Answer? Seeking Justice for Victims of Intimate Partner Violence Through the Reform of Legal Categories." *British Journal of Criminology & Criminal Justice* 18, no. 1: 115–131. <https://doi.org/10.1177/1748895817728561>
- Wiener, C. 2020. "From Social Construct to Legal Innovation: The Offence of Controlling or Coercive Behaviour in England and Wales." In *Criminalising Coercive Control*, edited by M. McMahon and P. McGorrery, 159–175. Singapore: Springer. https://doi.org/10.1007/978-981-15-0653-6_8
- Woodlock, D. 2017. "The Abuse of Technology in Domestic Violence and Stalking." *Violence Against Women* 23, no. 5: 535–558. <https://doi.org/10.1177/1077801216646277>