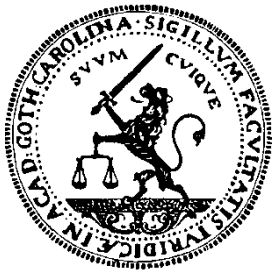

FACULTY OF LAW

LUND UNIVERSITY

Zubeyir Baghirzade

# Remote Coercive Control and the Limits of States' Positive Obligations under the European Court of Human Rights' Jurisprudence on Domestic Violence

JAMM07 Master Thesis

International Human Rights Law

30 higher education credits

Supervisor: Markus Gunneflo

Term of graduation: Spring 2026

# Table of contents

# Summary

This thesis examines whether the European Court of Human Rights (ECtHR) can adequately respond to technology-facilitated domestic abuse through its existing framework of States' positive obligations under the European Convention on Human Rights (ECHR). The study focuses specifically on 'remote coercive control', a specific form of abuse in which digital technologies are used to exercise ongoing surveillance, intimidation, control, and psychological pressure within intimate relationships without requiring physical proximity between the perpetrator and the victim. Examples include the use of spyware and monitoring applications, unauthorised access to email and social media accounts, GPS tracking, and other forms of digital surveillance.

The analysis begins from the observation that domestic violence has traditionally been understood through visible physical violence and separate incidents of harm. However, digital technologies such as smartphones, spyware, GPS tracking, social media platforms, and online communication tools have changed the conditions under which abuse occurs. Abuse may now continue remotely, continuously, and invisibly, even after physical separation.

The thesis analyses the ECtHR's domestic violence jurisprudence, particularly under Articles 3 and 8 of the ECHR, and examines recent judgments concerning technology-facilitated abuse (*Buturugă v Romania*, *Volodina v Russia (No. 2)*, and *M.Ş.D. v Romania*). It argues that the ECtHR's existing framework is formally capable of addressing remote coercive control, particularly through the flexibility of Articles 3 and 8. However, significant conceptual tensions emerge when traditional legal concepts are applied to digitally mediated abuse. The Court's framework remains largely structured around visible, physically proximate, and incident-based forms of violence, whereas remote coercive control operates through continuous, cumulative, and often invisible forms of psychological harm. Consequently, the thesis concludes that the principal issue is not the absence of legal protection, but the need for more context-sensitive interpretation of existing doctrinal concepts in response to evolving forms of digital abuse.

# Preface

This thesis marks the end of one of the most meaningful periods of my life. Although my time at Lund University is now coming to an end, the past two years have been profoundly formative. They have shaped me academically, socially, and personally in ways I could not have fully anticipated when I first arrived in Sweden. This period has not simply been a stage of study, but also an intense, demanding, and at the same time deeply rewarding experience. Looking back, I can confidently say that this period was never wasted; it was full of learning, growth, and unforgettable moments. I leave Lund with a strong sense that these years will remain with me for a long time.

I would first like to express my gratitude to Lund University for providing me with the academic environment and opportunity to pursue my studies in such a stimulating and international setting. I am also deeply grateful to the Swedish Institute Scholarship for making this journey possible. Being selected among many applicants was both an honour and a responsibility, and I have tried to make full use of the opportunity that was given to me.

I am especially grateful to my supervisor, Markus Gunneflo, for his guidance and great support during the entire process of writing this thesis. His feedback and encouragement were essential in shaping the direction of my work and in helping me maintain clarity and focus during the research process.

When I began writing this thesis, I had already received the result of my doctoral applications and had been admitted to a PhD in Law programme. This gave me a very different perspective while working on the thesis. Compared to my earlier research papers, I approached this work with greater academic experience, stronger research skills, and a more specialised perspective. My master's studies played an important role in preparing me for this next stage. Conducting extensive research and writing numerous research papers throughout these years helped me grow as a researcher and prepared me for doctoral-level studies. For this reason, I would like to thank all of my teachers and professors who contributed to my academic development. Particularly, I would like to express my special thanks to Karol Nowak and Matthew Scott for their support, guidance, and encouragement during my preparation for doctoral studies and for helping me further develop my research direction.

Finally, I would like to thank my family for always supporting me, encouraging me, and believing in me throughout every stage of my education. I am also especially grateful to my fiancée for being by my side during this entire process and for her constant love, patience, and support.

*"Though I'm past one hundred thousand miles, I'm feeling very still."*
— David Bowie, *Space Oddity*

# Abbreviations

| | |
|---|---|
| ECHR | European Convention on Human Rights |
| ECtHR | European Court of Human Rights |
| UN | United Nations |
| CoE | Council of Europe |
| HUDOC | ECtHR case-law database |
| GPS | Global Positioning System |

# 1 Introduction

## 1.1 The Problem

Domestic violence has traditionally been understood as physical violence causing visible harm through repeated incidents occurring under the same roof. Accordingly, legal and institutional responses focused on identifiable acts of violence, immediate threats, and observable escalation. However, digital technologies are increasingly integrated into everyday life, significantly changing the conditions under which abuse may occur. Smartphones, social media platforms, GPS tracking, spyware, online harassment, unauthorised access to digital accounts, and the dissemination of intimate images have allowed perpetrators to exercise control, surveillance, intimidation, and psychological pressure remotely and continuously. Importantly, such abuse may persist even after physical separation between the victim and the perpetrator. As a result, domestic abuse increasingly occurs within digitally mediated environments. This raises important questions for human rights law, particularly because existing legal frameworks were largely designed to address traditional forms of violence, which are physically proximate and incident-based. Consequently, it remains uncertain whether current human rights doctrine can effectively conceptualise and respond to technology-facilitated domestic abuse.

This problem is examined through the concept of remote coercive control in this thesis. The concept of coercive control, particularly articulated by Evan Stark, shifted understandings of domestic violence from isolated incidents to ongoing patterns of domination, surveillance, intimidation, and restriction within intimate relationships.[1] Based on this, contemporary scholarship increasingly explores how digital technologies facilitate coercive forms of abuse. Nevertheless, the terminology within the literature remains fragmented. Different scholars refer to 'digital coercive control', 'technology-facilitated coercive control', 'technology-facilitated stalking', and related concepts.[2] This thesis uses the term 'remote coercive control' because it best captures the distinctive conditions of digitally mediated coercive abuse. In particular, the term emphasises continuity, remoteness, persistence beyond physical proximity, and the ability of digital technologies to sustain coercive control beyond spatial boundaries. Correspondingly,

[1] Evan Stark, *Coercive Control: How Men Entrap Women in Personal Life* (2nd edn, Oxford 2024).

[2] Delanie Woodlock, Meagan McKenzie, Danielle Western and Bridget Harris, 'Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control' (2020) 73(3) *Australian Social Work* 368; Molly Dragiewicz, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P Suzor, Delanie Woodlock and Bridget Harris, 'Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms' (2018) 18(4) *Feminist Media Studies* 609; Delanie Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' (2017) 23(5) *Violence Against Women* 584.

remote coercive control refers to a form of technology-facilitated abuse in which digital technologies are used to exercise ongoing coercive control, surveillance, intimidation, and psychological domination within intimate relationships without physical proximity between the perpetrator and the victim.[3] The thesis further identifies four defining characteristics of remote coercive control: continuity, spacelessness, invisibility, and cumulative psychological harm.

## 1.2 Background

These developments raise significant concerns within the framework of the European Convention on Human Rights (ECHR or the Convention). Remote coercive control has direct effects on interests protected under the Convention, including privacy, psychological integrity, personal autonomy, dignity, and personal security.[4] A growing body of scholarship has been crucial in identifying and explaining the emerging harm of technology-facilitated abuse. Specifically, research in sociology, criminology, feminist theory, and media studies has shown how digital technologies extend coercive control, has mapped the gendered harms of online abuse and surveillance, and has expanded definitions of violence beyond physical injury.[5] This scholarship has been vital in making hidden harms visible and clarifying victims' experiences in digital environments. What this scholarship does not do, however, is address the legal challenges raised by technology-facilitated violence. In particular, it does not reinterpret States' positive obligations in digital contexts or provide concrete legal guidance capable of structuring judicial reasoning and thus State responsibility. In other words, from the perspective of human rights law, relatively limited attention has been given to the doctrinal structure of the European Court of Human Rights' (ECtHR or the Court) jurisprudence and, more specifically, to whether the Court's existing framework of positive obligations can adequately conceptualise and respond to remote coercive control in contemporary digital settings. Therefore, this thesis addresses a particular doctrinal gap by examining how existing Convention concepts operate when applied to technology-facilitated forms of coercive control in the digital age.

The thesis considerably focuses on the doctrine of States' positive obligations under the Convention and its application. Domestic violence jurisprudence before the ECtHR primarily operates through positive obligations requiring

[3] Dragiewicz et al., 'Technology Facilitated Coercive Control' 610–12.

[4] Elizabeth Coombs, 'Human Rights, Privacy Rights, and Technology-Facilitated Violence' in Jane Bailey, Asher Flynn and Nicola Henry (eds), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Emerald Publishing 2021) 482.

[5] Anastasia Powell, 'Technology-Facilitated Abuse: Intimate Partner Violence in Digital Society' in Karen Boyle and Susan Berridge (eds), *The Routledge Companion to Gender, Media and Violence* (Routledge 2023) 341–342; Dragiewicz et al., 'Technology Facilitated Coercive Control' 609; Heather Douglas, Bridget A Harris and Molly Dragiewicz, 'Technology-Facilitated Domestic and Family Violence: Women's Experiences' (2019) 59(3) *The British Journal of Criminology* 551.

States to take reasonable preventive and protective measures where authorities knew or ought to have known of risks to Convention rights.[6] Within this framework, Articles 3 and 8 particularly play a principal doctrinal role in addressing domestic violence. Article 3 covers severe forms of abuse involving inhuman or degrading treatment and protects both physical and psychological integrity, whereas Article 8 provides a broader framework protecting private life, autonomy, dignity, and non-physical forms of harm within relationships.[7] Together, these provisions structure the Court's response to domestic abuse.

In analysing positive obligations, the thesis focuses on three particular doctrinal concepts: risk, State knowledge, and seriousness of harm. The reason why they were specifically selected is that they determine how positive obligations arise and operate within the Court's jurisprudence. Risk triggers protective duties; State knowledge shapes foreseeability and State responsibility; and seriousness of harm establishes whether the threshold of the relevant provisions has been reached in a given case. Accordingly, the thesis argues that remote coercive control places conceptual pressure on each of these concepts in particular. This is because the Court's existing framework remains largely structured around traditional forms of abuse; this, in turn, complicates the clear determination of positive obligations and these key concepts in cases of digital violence.

## 1.3 Research Questions

Against this background, the central research question of the thesis is: To what extent can the ECtHR's existing framework of positive obligations adequately address remote coercive control as a form of technology-facilitated domestic abuse? In order to answer this question, the thesis addresses the following subsidiary questions: (i) How does remote coercive control challenge traditional understandings of domestic violence? (ii) How are positive obligations structured within the Court's domestic violence jurisprudence? (iii) How do the concepts of risk, State knowledge, and seriousness of harm operate in relation to remote coercive control? (iv) How has the ECtHR addressed technology-facilitated abuse in its recent case-law? (v) What doctrinal tensions emerge between the existing positive obligations framework and remote coercive control, and how might they be reconsidered? Therefore, the overall aim of the thesis is to examine whether the Court's existing doctrinal framework remains conceptually aligned with remote coercive control and, indirectly, evolving forms of technology-facilitated abuse.

[6] *Osman v United Kingdom* (App no 87/1997/871/1083) Judgment of 28 October 1998, para 116.

[7] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) arts 3 and 8.

## 1.4 Methodology

This thesis primarily adopts a doctrinal legal research approach. The research examines the jurisprudence of the ECtHR concerning domestic violence and States' positive obligations under the Convention. In doctrinal terms, the study proceeds through the analysis, ordering, and systematisation of judicial decisions and legal principles in order to identify the normative structure underlying the Court's case-law.[8] The thesis therefore focuses on how the Court interprets and applies the concepts of risk, State knowledge, and seriousness of harm within domestic violence jurisprudence, particularly under Articles 3 and 8 of the ECHR.

The research also includes a contextual analysis of selected ECtHR judgments concerning technology-facilitated abuse. In this regard, the thesis analyses how the Court understands and conceptualises domestic violence, coercive control, victim vulnerability, and State responsibility in digital contexts. This approach is particularly relevant because the contextual analysis of these cases helps to determine how the Court responds to the realities of digital abuse.

In addition, the thesis involves a conceptual analysis of the doctrinal framework of positive obligations. This aspect of the research examines whether legal concepts developed primarily in response to traditional forms of domestic violence remain fully adequate when applied to remote coercive control. Particular attention is given to potential tensions within the concepts of risk, State knowledge, and seriousness of harm when abuse occurs through continuous, remote, and technology-enabled conduct. The analysis does not seek to construct an entirely new doctrinal framework. By contrast, it evaluates the flexibility of the existing framework and examines how its concepts may require a more context-sensitive interpretation in light of changing technological and social conditions.[9]

As regards the Court's case-law, relevant judgments were identified through searches conducted within the HUDOC database using terms including 'domestic violence', 'cyberviolence', 'online harassment', 'digital abuse', and related terminology. Cases were then analysed individually in order to identify instances of technology-facilitated abuse within intimate relationships. Particular focus was placed on *Buturugă v Romania*, *Volodina v Russia (No. 2)*, and *M.Ş.D. v Romania* because these judgments explicitly address technology-facilitated abuse within domestic contexts and involve the application of Articles 3 and/or 8 of the ECHR.

This thesis made limited use of artificial intelligence-assisted language tools, specifically ChatGPT (OpenAI) and Grammarly, exclusively for language

[8] P Ishwara Bhat, *Idea and Methods of Legal Research* (Oxford 2020) 144–46.
[9] *Ibid* 148.

editing purposes, including orthographic correction, syntactic refinement, and lexical or stylistic improvement. All substantive analysis, legal argumentation, interpretation, structure, and conclusions are the independent work of the author.

## 1.5 Outline

The thesis is divided into an introduction, five substantive chapters, and a conclusion. The first substantive chapter establishes the conceptual framework of the thesis by examining the evolution of coercive control theory and defining remote coercive control. The second chapter addresses the doctrine of positive obligations within the ECtHR's domestic violence jurisprudence, with particular focus on the concepts of risk, State knowledge, and seriousness of harm under Articles 3 and 8. The following chapter applies this doctrinal framework to remote coercive control and identifies conceptual tensions arising from digitally mediated abuse. The subsequent chapter analyses the Court's relevant case-law concerning technology-facilitated abuse, focusing primarily on *Buturugă v Romania*, *Volodina v Russia (No. 2)*, and *M.Ş.D. v Romania*. The final substantive chapter explores the implications of these tensions for the future development of positive obligations doctrine and suggests how existing concepts might be reconsidered for more effective application. The thesis ends with the Conclusion consisting of doctrinal, conceptual, and institutional reflections, as well as broader implications for future research on technology-facilitated domestic violence within human rights law. Overall, the thesis argues that the ECtHR's current framework of positive obligations is capable of addressing technology-facilitated abuse to a certain extent, but conceptual tensions still expose the need for a more context-sensitive doctrinal interpretation in digitally mediated environments.

# 2 Framing the Problem

## 2.1 Domestic Violence and the Concept of Coercive Control

Domestic violence has historically been conceived mainly as physical violence between intimate partners. Early legal and policy frameworks tended to conceptualise domestic abuse as a series of incidents involving physical assaults and threats of bodily harm.[10] Within these frameworks, the focus was largely on visible injury, immediate danger, and discrete episodes of violence that could be clearly recognised and documented. As a result, domestic violence was often viewed as isolated acts occurring within the private sphere of family life. This perspective shaped both public views and institutional responses to domestic abuse for many years. However, over the years, scholarship and advocacy have increasingly challenged this narrow understanding. They began to observe that many abusive relationships involve more than just physical violence, including patterns of control that affect the victim's daily life.[11]

An important development in this evolving understanding was the introduction of the concept of 'coercive control', most notably developed by Evan Stark. Stark conceptualised domestic abuse not simply as a series of violent acts but as an ongoing pattern of domination, through which the abuser systematically limits the victim's autonomy and freedom.[12] Under this approach, the key aspect of abuse includes the strategies used to dominate and control the victim's behaviour, relationships, and daily life. Coercive control may involve many forms beyond physical violence, such as psychological manipulation, economic deprivation, intimidation, surveillance, and isolation from social support networks.[13] These behaviours usually occur repeatedly over time, forming an ongoing pattern through which the perpetrator maintains power in the relationship.

Three key features are particularly central to understanding the concept of coercive control. First, coercive control emphasises patterns rather than individual incidents. This approach does not focus on single acts of violence; instead, it highlights how abusive behaviour develops as a continuous and systematic pattern.[14] The importance of any individual act may be less about its immediate impact and more about its role within the wider pattern of domination. Second, coercive control involves the regulation of everyday life. Victims may face restrictions on their movement, communication, finances,

[10] Ronagh JA McQuigg, *Domestic Abuse and the European Court of Human Rights* (Routledge 2024) 3–11.
[11] *Ibid* 40.
[12] Stark, *Coercive Control* 243.
[13] *Ibid* 245.
[14] *Ibid* 248.

work, and social life.[15] Through these forms of control, the abusive partner gradually restricts the victim's autonomy and independence. Third, coercive control produces cumulative harm. The effects of abuse intensify over time, often resulting in serious psychological consequences such as fear, dependency, and a loss of personal control. Consequently, the concept of coercive control shifts attention from individual acts of violence to the broader patterns of power operating within abusive relationships.[16]

The concept of coercive control has significantly shaped the analysis and understanding of domestic violence across multiple disciplines. Within scholarship, this concept has helped develop a deeper understanding of abusive relationships, emphasising patterns of behaviour and the broader context in which violence occurs.[17] It has influenced policy discussions and advocacy work, highlighting non-physical forms of abuse and how coercive behaviours can undermine a victim's autonomy and safety even without visible injury. In certain jurisdictions, these insights have informed legal and policy reforms, including measures that recognise patterns of coercive and controlling behaviour in intimate relationships.[18]

More broadly, the concept of coercive control reflects a significant shift in the conceptualisation of domestic violence. Recent scholarship not only examines domestic violence from the perspective of physical assault but also increasingly understands it as a system of control through which perpetrators seek to dominate their partners and limit their freedom. This approach recognises that abuse may occur in various forms, including psychological, economic and social harm, and that the cumulative effects of such behaviours can be significantly harmful. By emphasising patterns of control within abusive relationships, the concept of coercive control provides a framework for recognising forms of abuse that may not involve physical violence but still undermine the victim's autonomy and well-being. However, the rise of contemporary technologies has presented new challenges in addressing coercive control. These technologies provide additional means through which such control may be exercised.

## 2.2 Defining Remote Coercive Control and its Distinctive Features

In recent years, developments in digital technology have introduced new dimensions to the dynamics of control. Technologies that are widely used in everyday life can also be misused within abusive relationships. As a result, perpetrators may increasingly rely on digital tools such as smartphones, social

[15] Stark, *Coercive Control* 245.

[16] *Ibid* 256–57.

[17] Evan Stark, 'Rethinking Coercive Control' (2009) 15(12) *Violence Against Women* 1509, 1510.

[18] McQuigg, *Domestic Abuse and the European Court of Human Rights* 40.

media platforms and location-based services to monitor, intimidate, and harass victims. This phenomenon is often described in scholarship and policy discussions as technology-facilitated violence or technology-mediated abuse.

Technology-facilitated abuse may occur in a variety of forms. In intimate relationships, the abusive partner may install spyware or monitoring applications on a mobile phone in order to gain access to the victim's messages, call logs or other personal data.[19] Global positioning systems (GPS) tracking functions may be used to monitor the victim's movements in real time, allowing the perpetrator to know the victim's location at any moment. In other cases, abusive partners may gain unauthorised access to email accounts, social media profiles and messaging platforms to read private communications or to impersonate the victim online.[20] Significantly, the growing role of digital technologies in enabling and facilitating different forms of abuse, particularly within intimate partner relationships, has been widely documented. These developments highlight how modern technologies can extend the reach of coercive behaviour beyond traditional forms of interpersonal interaction.

Within this broader context, the concept of remote coercive control can be understood as a particular form of technology-facilitated abuse. In this thesis, remote coercive control refers to patterns of coercive control that are exercised through digital technologies, allowing perpetrators to monitor, intimidate, or influence victims continuously and without requiring physical proximity.[21] While coercive control traditionally involved efforts such as isolation, surveillance, or intimidation within shared physical spaces, digital technologies now enable these acts to be carried out remotely. Without being physically present, perpetrators may engage in malicious acts by monitoring victims' activities, accessing personal communications, or tracking movements from anywhere. In this sense, technological devices serve as a means by which established patterns of coercive control are maintained and reinforced.

The definition mentioned consists of several elements. First and foremost, remote coercive control is facilitated through digital technologies. Devices such as smartphones, computers, and internet-connected applications enable harmful acts to be carried out. Second, these technologies mediate continuous forms of surveillance. Digital tools can allow perpetrators to repeatedly track victims' activities with minimal effort. Third, the abuse may operate

[19] Karlie E Stonard, 'Technology-Assisted Abuse within Intimate Relationships' in John Devaney, Caroline Bradbury-Jones, Rebecca J Macy, Carolina Øverlien and Stephanie Holt (eds), *The Routledge International Handbook of Domestic Violence and Abuse* (Routledge 2021) 357.

[20] Kathryn Brookfield, Rachel Fyson and Murray Goulden, 'Technology-Facilitated Domestic Abuse: An Under-Recognised Safeguarding Issue?' (2024) 54(1) *The British Journal of Social Work* 419, 423.

[21] Dragiewicz et al., 'Technology Facilitated Coercive Control' 610–12.

remotely, meaning that the perpetrator can exercise coercive control without being physically close to the victim. Finally, remote coercive control is part of broader patterns of coercive behaviour. The use of technology does not replace other forms of abuse but serves as one of several mechanisms for exercising control.

For the purposes of this thesis, it would be important to distinguish remote coercive control from the wider category of online harassment and digital abuse. Significantly, this concept does not encompass all forms of harmful online activity. Instead, attention is given specifically to situations in which digital technologies are used within intimate relationships as part of a broader pattern of coercive and controlling behaviour. In other words, remote coercive control refers to a technologically facilitated extension of coercive control rather than a completely separate form of abuse. Importantly, it should not be understood as a new and separate category of violence, nor as an alternative to offline abuse. Digital technologies do not create new violence, but they transform how domestic abuse is committed and perpetuated.[22] They make abuse more severe and enduring. As a result, control and domination within intimate relationships are reinforced through new tools.

In order to clearly understand the concept of remote coercive control, it is necessary to explore its several characteristics that distinguish it from other forms of technology-facilitated abuse. The first is the potential for continuous surveillance. This feature refers to the 'timeless' nature of technology-facilitated abuse.[23] Digital tools can enable perpetrators to continuously track a victim's location, communications, and online activities. Applications for location sharing, access to personal devices, or monitoring programmes can create an environment in which the victim's actions and interactions are perpetually observed. Such remote coercive control has no clear end-point; it is ongoing and escalating. Perpetrators may carry out further abusive acts against victims at any time, often unexpectedly. Consequently, this capacity for persistent observation may strengthen the perpetrator's control and further limit the victim's sense of privacy and independence.[24]

The second characteristic is the absence of physical proximity. In traditional forms of coercive control, the perpetrator's physical presence is often observed within the household and immediate environment. However, digital technologies allow abusive behaviour to occur even when the perpetrator and the victim are physically separated. As digital technologies are not limited by physical space, victims can be subjected to abuse wherever they use digital

[22] Adriane Van der Wilk, 'Protecting Women and Girls from Violence in the Digital Age: The Relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in Addressing Online and Technology-Facilitated Violence against Women' (Council of Europe, December 2021) 9.

[23] Karlie E Stonard, 'Technology-Assisted Abuse within Intimate Relationships' 357.

[24] Brookfield et al., 'Technology-Facilitated Domestic Abuse' 426.

devices or access online platforms, at any time.[25] Harm can be inflicted remotely through malicious practices, such as digital surveillance, GPS tracking, or unauthorised access to online accounts. Such conduct may cause significant psychological and emotional harm, even in the absence of physical violence. Thus, control and abuse can persist regardless of the perpetrator's location, yet remain deeply embedded within the intimate relationship and everyday life. This feature indicates the 'spaceless' nature of technology-facilitated abuse.

Third, remote coercive control reflects relative invisibility. Many forms of digital monitoring can occur without the victim's knowledge. Digital access allows perpetrators to maintain abusive conduct that leaves no visible traces and is often difficult to detect.[26] Spyware and monitoring applications may be installed covertly, and victims may not immediately realise that their communications and movements are being observed. Moreover, the perpetrator may be suspected but cannot be conclusively linked to the conduct because digital practices can easily conceal their identity even when the perpetrator is known in real life. Identifying and proving the presence of such technologies often requires technical expertise, which further complicates victims' and third parties' recognition of ongoing coercive control and its harmful effects.

Finally, remote coercive control often results in cumulative and psychological harm. The effects of persistent surveillance may extend beyond individual acts of harassment. Victims may experience ongoing anxiety about being monitored and tracked, leading them to censor their communications and limit their daily activities. This persistence can create a sense of omnipresence, with victims feeling that the perpetrator is present in every aspect of their lives.[27] Over time, continuous digital monitoring may reinforce feelings of fear, loss of autonomy, and psychological pressure within the relationship.

All together, these characteristics demonstrate how digital technologies can fundamentally transform the ways in which coercive control is exercised within abusive relationships and experienced by victims. In turn, this necessitates exploring the concept of remote coercive control from the perspective of international human rights law.

---

[25] Bridget A Harris, 'Technology and Violence Against Women' in Sandra Walklate, Kate Fitz-Gibbon, JaneMaree Maher and Jude McCulloch (eds), *The Emerald Handbook of Feminism, Criminology and Social Change* (Emerald Publishing 2020) 321.

[26] Alison J Marganski and Lisa A Melander, 'Technology-Facilitated Violence Against Women and Girls in Public and Private Spheres: Moving from Enemy to Ally' in Jane Bailey, Asher Flynn and Nicola Henry (eds), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Emerald Publishing 2021) 626.

[27] Woodlock et al., 'Technology as a Weapon in Domestic Violence' 372.

## 2.3 Why Remote Coercive Control Matters for Human Rights Law

Remote coercive control can significantly affect the lives of individuals who experience such conduct. While this form of abuse occurs within intimate relationships, its consequences extend beyond the private sphere and may involve interests which are commonly protected under human rights frameworks. By interfering with personal privacy, psychological integrity, and the ability to live free from intimidation and constant monitoring, remote coercive control can undermine fundamental aspects of individual autonomy and dignity.[28] Malicious practices such as continuous digital surveillance, persistent monitoring of a person's movements, and unauthorised access to private communications can substantially limit an individual's freedom to communicate, move, and interact with others. Additionally, ongoing monitoring and threats can create psychological pressure that affects a victim's sense of security and personal integrity. These harms indicate that remote coercive control is not just a private issue between two parties of an intimate relationship but raises broader concerns related to individual rights and freedoms.

In this regard, the concept of remote coercive control also reflects wider patterns that have long been recognised within discussions of violence against women. It has consistently been highlighted that domestic violence disproportionately affects women, and it is often embedded within unequal power relations between partners.[29] Technology-facilitated abuse, including remote coercive control, often reflects these same gendered patterns. International organisations have increasingly acknowledged the role of digital technologies in facilitating new forms of violence against women. For instance, materials produced by UN bodies and the Council of Europe have shown how digital technologies and online environments are used to harass, monitor, and threaten women within intimate relationships.[30] These developments highlight the significance of understanding technology-facilitated abuse within the broader context of gender-based violence.

As a specific form of technology-facilitated abuse, remote coercive control is particularly relevant in the context of human rights for understanding the evolution of domestic abuse within increasingly digitalised social environments. As digital technologies become deeply integrated into

[28] Coombs, 'Human Rights, Privacy Rights, and Technology-Facilitated Violence' 482.

[29] Russell P Dobash and Rebecca E Dobash, 'Violent Men and Violent Contexts' in Russell P Dobash and Rebecca E Dobash (eds), *Rethinking Violence against Women* (SAGE Publications 1998) 143–45.

[30] UN Broadband Commission for Digital Development, *Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call* (2015); Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), *General Recommendation No 1 on the Digital Dimension of Violence against Women* (GREVIO(2021)20, 20 October 2021).

everyday life, they also create new ways through which coercive control can be exerted. Understanding these dynamics is an important step in analysing how legal and policy frameworks approach domestic abuse in modern digital contexts. Accordingly, exploring the nature and characteristics of remote coercive control provides the foundation for the subsequent analysis of how existing legal frameworks respond to forms of abuse that are increasingly mediated through digital technologies.

# 3 States' Positive Obligations in Domestic Violence Cases

This chapter explores the doctrinal framework of positive obligations under the Convention from a perspective of domestic violence. Its purpose is to identify the legal concepts and standards through which State responsibility is assessed, in particular the concepts of risk, State knowledge, and seriousness of harm. This framework provides the analytical basis for examining its application to remote coercive control in the following chapter.

These three concepts are specifically analysed throughout the thesis because they play a principal doctrinal role in determining how positive obligations arise and operate within the Court's domestic violence jurisprudence. Risk determines when protective duties are triggered; State knowledge shapes questions of foreseeability and State responsibility; and seriousness of harm establishes whether the threshold of Convention protection has been reached.[31] Correspondingly, the chapter focuses on Articles 3 and 8 of the Convention, as these provisions provide the primary legal foundation through which the Court addresses domestic violence.

## 3.1 Development of Positive Obligations

The ECHR was originally framed in terms of negative obligations. According to this traditional understanding, the role of the State was to refrain from interfering with the rights protected under the Convention.[32] In other words, States were required not to violate individual rights through their own actions. This classical approach framed human rights law as a protective model against State abuse.

However, over time, the Court's jurisprudence has developed beyond this 'negative obligations' framework. The Court has increasingly recognised that, in order to ensure the effective protection of Convention rights, States may also be required to take positive actions.[33] This development is based on Article 1 of the Convention, which requires States to secure to everyone within their jurisdiction the rights and freedoms set out in the Convention.[34] The notion of 'securing' rights has been interpreted by the Court as requiring

[31] Vladislava Stoyanova, 'Fault, Knowledge and Risk within the Framework of Positive Obligations under the European Convention on Human Rights' (2020) 33(3) *Leiden Journal of International Law* 601, 602, 612; *Opuz v Turkey* (App no 33401/02) Judgment of 9 June 2009, para 158.

[32] Laurens Lavrysen, *Human Rights in a Positive State: Rethinking the Relationship between Positive and Negative Obligations under the European Convention on Human Rights* (Intersentia 2016) 214.

[33] Jean-François Akandji-Kombé, *Positive Obligations under the European Convention on Human Rights: A Guide to the Implementation of the European Convention on Human Rights* (Council of Europe, Human Rights Handbooks No 7, January 2007) 5–6.

[34] European Convention on Human Rights art 1.

not only abstention from interference but also the adoption of measures to ensure that those rights are effectively protected in practice.[35]

Accordingly, the Court has recognised that State responsibility may arise even when the harm is caused by private individuals rather than State agents.[36] In such situations, the key issue is not whether the State directly caused the harm, but whether it fulfilled its obligation to take reasonable measures to prevent and respond to violations of Convention rights. This has led to the development of a framework of positive obligations that applies in so-called 'horizontal' contexts, where the relationship is primarily between private parties but may still engage State responsibility due to failures in protection.[37]

Significantly, the Court has shaped the structure of positive obligations through its jurisprudence, particularly in its articulation of the principles governing preventive duties. A key point in this context is the Court's formulation of the standard requiring that authorities 'knew or ought to have known' of a risk to an individual.[38] This element is closely linked to the requirement that the risk be both 'real and immediate,' meaning that it must be concrete and present, rather than hypothetical and remote. Where such a risk is identified, the State may be required to take reasonable measures within the scope of its powers that could be expected to prevent or reduce that risk.

The ECtHR has consistently stressed that positive obligations require States to prioritise taking adequate measures rather than achieving guaranteed outcomes; in other words, positive obligations are considered 'obligations of means and not of result'.[39] States are not obliged to prevent all harm or ensure absolute protection against violations of Convention rights. Instead, their responsibility is assessed based on due diligence: whether the authorities took reasonable measures within their authority to address a known or foreseeable risk.[40] This approach aims to balance protecting individuals with the practical challenges that State authorities face in responding to complex and evolving situations.

The development of positive obligations has been particularly significant in the context of domestic violence. As discussed in the previous chapter,

[35] Akandji-Kombé, *Positive Obligations under the European Convention on Human Rights* 8.

[36] *X and Y v Netherlands* (App no 8978/80) Judgment of 26 March 1985, para 23.

[37] Akandji-Kombé, *Positive Obligations under the European Convention on Human Rights* 14.

[38] *Osman v United Kingdom*, para 116.

[39] Vladislava Stoyanova, 'Framing Positive Obligations under the European Convention on Human Rights Law: Mediating between the Abstract and the Concrete' (2023) 23(3) *Human Rights Law Review* 27.

[40] *Kurt v Austria* (App no 62903/15) Judgment of 15 June 2021, paras 158–160.

domestic violence often occurs within intimate relationships, and it is characterised by patterns of abuse that may not always be immediately apparent, including forms of controlling behaviour that operate beyond isolated incidents. While such harm arises in the private sphere, the Court has emphasised that States may be held responsible if they fail to respond appropriately.[41]

In its case-law, the Court has increasingly prioritised the role of positive obligations in the context of domestic violence. In *Opuz v. Turkey*, the Court recognised that repeated incidents of domestic violence and threats can impose on the State an obligation to take protective and preventive action.[42] Similarly, in *Talpis v. Italy*, the Court examined whether the authorities responded adequately to complaints of domestic abuse and whether they took reasonable steps to prevent further harm.[43] More recently, in *Kurt v. Austria*, the Court further clarified the application of the 'real and immediate risk' standard in situations involving ongoing domestic violence.[44]

These cases highlight how the general framework of positive obligations operates in practice. They reflect that States may be required to act adequately where there are signs of escalating violence, repeated reports, or other risk factors affecting the individual. In this context, the authorities are expected to assess the situation, take preventive measures where necessary, and ensure that their response is effective in addressing the risk of harm.

Accordingly, the doctrine of positive obligations under the Convention provides the legal basis for treating domestic violence as an issue of State responsibility rather than simply private harm. At the same time, it shapes how such responsibility is assessed in practice.

## 3.2 Concepts of Risk, State Knowledge and Seriousness

Based on the general framework of positive obligations described above, the application of this doctrine depends on several key concepts. In particular, the concepts of risk, State knowledge, and seriousness of harm play an important role in determining when State responsibility is engaged in domestic violence.

According to the assessment of risk, the Court has consistently required that, for positive obligations to apply, there must be a real and immediate risk to the life or physical or psychological integrity of an individual.[45] This approach is inherently forward-looking, focusing on the likelihood of future

[41] McQuigg, *Domestic Abuse and the European Court of Human Rights* 58.
[42] *Opuz v Turkey*, paras 128–130.
[43] *Talpis v Italy* (App no 41237/14) Judgment of 2 March 2017, paras 107–131.
[44] *Kurt v Austria*, para 164.
[45] *Osman v United Kingdom*, para 116; *Opuz v Turkey*, para 129; *Eremia v Republic of Moldova* (App no 3564/11) Judgment of 28 May 2013, para 49.

harm rather than only on past events. In determining the existence of a risk, the Court takes certain factors into account, including prior incidents of violence, explicit threats, and patterns of behaviour indicating escalation.[46] In the context of domestic violence, this may involve repeated complaints to authorities, documented incidents of abuse, and indications of a progressively worsening situation. Through this approach, the Court assesses whether the circumstances, taken together, indicate a degree of risk requiring preventive measures. At the same time, the assessment of risk often depends on identifiable factors, such as specific threats and prior acts of violence, which help indicate how serious and immediate the situation is.[47]

The other significant factor is State knowledge, which is closely connected to the concept of risk. The Court differentiates between situations where authorities had actual knowledge of the risk and those where they had putative knowledge of the risk.[48] Actual knowledge may become apparent when victims report abuse to the police, file complaints, and seek protective measures. In such cases, since the authorities are fully aware of the circumstances, they are expected to respond appropriately. On the other hand, States may be held responsible in situations of putative knowledge, where the authorities ought to have known of a risk based on the information available to them.[49] This may involve police reports, prior interventions, and visible signs of escalating violence.[50] In this regard, the assessment of State knowledge is not confined to formal complaints but also considers the more comprehensive factual context. In other words, State responsibility depends on what the authorities knew or should have known at the time.

The third element in the Court's reasoning is the seriousness of the harm. Importantly, not all forms of harm fall within the scope of the Convention. The Court has consistently highlighted that a minimum level of severity must be reached in order to engage the protection of relevant articles.[51] In relation to Article 3, this threshold is relatively high, which requires a kind of treatment that qualifies as inhuman or degrading.[52] In contrast, Article 8 provides a distinct and broader framework, covering psychological integrity and personal autonomy.[53] In the context of domestic violence, the assessment of seriousness often considers factors such as the extent of physical injury, the presence of threats, and the overall intensity of the abusive conduct.[54]

---

[46] *Kurt v Austria*, para 198.

[47] McQuigg, *Domestic Abuse and the European Court of Human Rights* 71.

[48] *Osman v United Kingdom*, para 116.

[49] Stoyanova, 'Fault, Knowledge and Risk within the Framework of Positive Obligations' 604.

[50] *Kurt v Austria*, para 198.

[51] *Opuz v Turkey*, para 158; *Eremia v Republic of Moldova*, para 48.

[52] European Convention on Human Rights art 3.

[53] *Ibid* art 8.

[54] *Valiulienė v Lithuania* (App no 33234/07) Judgment of 26 March 2013, para 65.

## 3.3 Relevance of Articles 3 and 8

The doctrine of positive obligations is primarily applied through specific provisions of the Convention. This section focuses more closely on Articles 3 and 8, which are central to defining the scope and content of State responsibility in domestic violence cases.

Article 3 of the Convention prohibits torture and inhuman or degrading treatment or punishment.[55] It is an absolute right, which does not allow any exceptions or derogations, even in situations of emergency.[56] The Court has stressed that this provision requires States not only to refrain from ill-treatment as negative obligations, but also to take measures to prevent such treatment as positive obligations.[57] These obligations include duties to protect individuals from serious harm, to take preventive operational measures where a real and immediate risk exists, to conduct effective investigations into ill-treatment, and to provide effective remedies.[58]

In the context of domestic violence, Article 3 is generally engaged in situations involving serious physical violence and life-threatening conduct. The Court has stressed that repeated assaults, severe beatings, or credible threats to life may reach the threshold of inhuman or degrading treatment.[59] Once this threshold is reached, the State is required to act with particular diligence. This may involve measures such as the timely response to complaints, the protection of victims, and the effective intervention of law enforcement authorities.[60]

As regards Article 8 of the Convention, it provides a broader framework. It guarantees the right to respect for private and family life, home and correspondence.[61] Unlike Article 3, Article 8 is not limited to severe forms of harm. Instead, it encompasses a broad range of interests, including psychological integrity, personal autonomy, and the ability to develop relationships free from unjustified interference.[62]

The Court has held that Article 8 also imposes positive obligations on States to ensure effective respect for private life.[63] This includes the protection of individuals from interference by other private persons. In domestic violence

[55] European Convention on Human Rights art 3.

[56] European Court of Human Rights, *Guide on Article 3 of the European Convention on Human Rights: Prohibition of Torture* (31 August 2025), para 2.

[57] *Opuz v Turkey*, para 159.

[58] European Court of Human Rights, *Guide on Article 3*, para 4.

[59] *Ibid* paras 18, 22.

[60] *Volodina v Russia* (App no 41261/17) Judgment of 9 July 2019, paras 76–77.

[61] European Convention on Human Rights art 8.

[62] European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence* (31 August 2025), paras 86–87.

[63] *Bevacqua and S v Bulgaria* (App no 71127/01) Judgment of 12 June 2008, para 64; *Eremia v Republic of Moldova*, para 72.

cases, the severity of harm may not reach the threshold of Article 3 but can still affect the individual's well-being; in such situations, Article 8 plays a relevant role.[64] Situations involving harassment, intimidation, and other forms of non-physical abuse may fall within the scope of Article 8. In such cases, the State is required to take reasonable steps to prevent further interference and to ensure an adequate legal and institutional framework for protection.

Significantly, Article 8 provides a more comprehensive assessment of harm, as it covers forms of abuse that may not cause serious physical injury but can affect psychological integrity and personal autonomy. Consequently, it constitutes a crucial provision in the broader context of domestic violence, where harm can occur in diverse forms and degrees.

Together, Articles 3 and 8 provide the Court with the principal legal framework for articulating and applying positive obligations in domestic violence cases. Despite differences in severity and scope, they operate complementarily, allowing the Court to address a wide range of harmful conduct within intimate relationships.

While the ECtHR has developed a strong approach to positive obligations in domestic violence cases, its doctrines have primarily evolved in response to abuses identifiable through observable incidents and escalating patterns of harm, in short, traditional forms of abuse. The following chapter builds on this doctrinal framework to examine how it applies to remote forms of coercive control mediated by digital technologies.

[64] European Court of Human Rights, *Guide on Article 8*, paras 41, 127.

# 4 Doctrinal Test: Applying Existing Frameworks

## 4.1 Applying the Positive Obligations Framework to Remote Coercive Control

The doctrine of positive obligations under the Convention provides the central framework through which State responsibility is assessed in situations involving coercive control. However, where such abuse occurs in the digital sphere, it becomes significant to examine how this framework would operate when applied to remote coercive control.

In order to apply this framework, it is first necessary to analyse the characteristics of remote coercive control through the lens of legal concepts aligned with the Court's jurisprudence. As discussed earlier, remote coercive control consists of several features, in particular continuous surveillance, the absence of physical proximity, relative invisibility, and the production of cumulative psychological harm.

The element of continuous surveillance, characterised by the 'timeless' nature of the abuse, can be understood as an interference with the right to respect for private life under Article 8 of the Convention. The Court has recognised that the monitoring of an individual's communications, movements, or personal data may engage Article 8, particularly where such conduct affects the individual's ability to exercise autonomy and maintain personal relationships.[65] Accordingly, practices such as non-consensual access to digital accounts, GPS tracking, or persistent monitoring of online activity may be regarded as interferences with privacy and correspondence. Moreover, the repetitive and ongoing nature of such conduct may be interpreted as enhancing the severity of the interference, particularly when it impacts multiple aspects of the individual's daily life.

As regards the absence of physical proximity, it does not exclude the applicability of the Convention. According to the Court's jurisprudence on domestic violence, harm occurring within the private sphere may still engage State responsibility if the authorities fail to provide effective protection.[66] In remote coercive control, the perpetrator's distance from a victim may be seen as a variation in the method of control rather than a fundamental change in the nature of the harm. Accordingly, acts conducted via digital technologies may still be evaluated under the framework of positive obligations, especially

[65] *Buturugă v Romania* (App no 56867/15) Judgment of 11 February 2020, para 74; *Volodina v Russia (No 2)* (App no 40419/19) Judgment of 14 September 2021, para 50.

[66] *Opuz v Turkey*, para 159.

when they affect the individual's psychological integrity and sense of security.

The next characteristic is relative invisibility of remote coercive control. From a legal perspective, this invisibility may be considered as a challenge in proving the facts and providing evidence.[67] Conduct, such as hidden surveillance and unauthorised access to devices, may leave limited visible traces, making it more challenging to detect and document the abuse. Within the Court's framework, this feature would be relevant to assessing State knowledge, specifically whether the authorities knew or ought to have known the risk.

Finally, the cumulative and psychological nature of harm arising from remote coercive control can be interpreted in terms of psychological integrity and personal autonomy, which are protected under Article 8. The Court has recognised that harm does not need to be physical in order to fall within the scope of the Convention.[68] Repeated acts of harassment, intimidation, and monitoring may collectively lead to a constant sense of the perpetrator's presence, reflecting a sense of omnipresence.[69] These harmful acts may interfere with an individual's private life by creating an environment of fear and restricting personal autonomy. Consequently, the cumulative effect of such conduct may become significant while assessing the seriousness of the harm and the need for protective measures.

In addition to the characteristics of remote coercive control, it is also necessary to consider how the *Osman* framework would operate in this context. This involves examining how the concepts of risk, State knowledge, and the seriousness of the harm would, in principle, be applied to cases of technology-facilitated coercive control.

Firstly, the key issue is whether remote coercive control would constitute a 'real and immediate risk' to the individual's rights. In the Court's case-law, the assessment of risk is usually grounded in identifiable signs, such as prior incidents, explicit threats, and patterns of escalating violence.[70] However, when it comes to remote coercive control, evidence of risk may appear in different forms. For example, repeated non-consensual access to personal accounts, persistent monitoring of communications, and ongoing digital harassment could be indicators of a continuing pattern of conduct. Such behaviour may indicate that the individual is experiencing sustained interference with their psychological integrity and autonomy. Therefore, risk

[67] Marganski and Melander, 'Technology-Facilitated Violence Against Women and Girls' 626.

[68] European Court of Human Rights, *Guide on Article 8*, para 41.

[69] Woodlock et al., 'Technology as a Weapon in Domestic Violence' 372.

[70] McQuigg, *Domestic Abuse and the European Court of Human Rights* 71.

assessment would depend on whether these behaviours collectively amount to a serious and immediate threat requiring prevention.

The other important issue concerns State knowledge. In cases of remote coercive control, authorities can become aware of harmful conduct through victim complaints, reports of digital harassment, or through evidence such as messages, account activity, and other digital records.[71] At the same time, the concept of putative knowledge would require assessing whether the authorities ought to have been aware of the situation given the information available to them. This may include previous reports of domestic abuse, patterns of controlling behaviour, or frequent interactions with law enforcement. Within the *Osman* framework, the key issue would be whether the information available to the authorities was sufficient to necessitate intervention.

Finally, the seriousness of the harm plays an important role in defining how remote coercive control would fall within the scope of Articles 3 and 8 of the Convention. As discussed before, Article 3 covers severe ill-treatment, including serious physical violence and conduct that threatens life. Accordingly, in cases of remote coercive control, when digital conduct is accompanied by threats of violence and severe psychological pressure, these extreme forms of abuse could engage Article 3. However, mostly, the harm arising from remote coercive control may not reach this high threshold. By contrast, Article 8 more closely aligns with the features of remote coercive control, as it provides a broader and more flexible framework. Interferences with privacy, correspondence, and psychological integrity, which are commonly observed in cases of remote coercive control, clearly fall within the scope of this provision.[72] Consequently, technology-facilitated abuse may be assessed as a violation of the right to respect for private life.

To conclude, the existing framework of positive obligations under Articles 3 and 8 enables the legal analysis of remote coercive control. At the same time, applying this framework to technology-facilitated abuse requires careful analysis of how these concepts function in contexts that differ from traditional forms of domestic violence.

## 4.2 Doctrinal Challenges in Applying Positive Obligations to Remote Coercive Control

Having applied the framework of positive obligations to remote coercive control in the previous section, it becomes necessary to examine more closely how its core elements operate in this new context. The previous section is primarily reconstructive: after reviewing the characteristics, it analyses remote coercive control through the concepts of risk, State knowledge, and

[71] *Buturugă v Romania*, para 74.
[72] Woodlock et al., 'Technology as a Weapon in Domestic Violence' 373.

seriousness of harm, and describes how the existing doctrinal framework could, in principle, be applied to patterns of technology-facilitated abuse. In doing so, it shows that remote coercive control can be brought within the conceptual scope of the Court's jurisprudence.

However, this section adopts a different approach. Instead of asking how the doctrine would apply, it seeks to evaluate how it functions in practice when applied to the specific characteristics of remote coercive control. While the framework may initially seem flexible enough to cover such forms of abuse, a more detailed analysis exposes certain tensions in its application. In particular, the concepts of risk, State knowledge, and seriousness of harm raise specific difficulties when applied to patterns of abuse that are continuous, remote, cumulative, and often invisible.

### 4.2.1 Limitations of the concept of risk

Within the framework of positive obligations, the notion of a 'real and immediate risk' plays an important role in determining the requirement of taking preventive operational measures. As mentioned before, this assessment typically depends on identifiable indicators, such as incidents of violence, explicit threats, and patterns of escalation. In the context of domestic violence, they often help authorities identify risks and take timely and appropriate action.

However, remote coercive control can challenge this concept. As this form of abuse has a continuous nature, it often occurs as an ongoing pattern of surveillance, monitoring, and psychological pressure.[73] As a result, the harm is not necessarily limited to a single identifiable incident, but instead develops gradually over time. Where the risk is persistent rather than moment-based, this raises doubts about the requirement of 'immediacy'.

In traditional domestic violence cases, the notion of 'immediacy' often covers an escalation, such as increasingly frequent and severe incidents, or the development of explicit threats.[74] These elements help connect the existing and known harm with the likelihood of future harm. Yet, in remote coercive control, escalation may not be clearly identifiable. Harmful behaviours, such as continuous monitoring and non-consensual access to digital accounts, can continue at a relatively constant level, without creating a specific moment that indicates an imminent danger.[75] In turn, this makes it difficult to define clear escalation points. Consequently, as there are no clear escalation points, this may hinder the assessment of whether a risk becomes sufficiently immediate to require intervention or not.

The cumulative nature of harm also complicates this assessment. Remote coercive control often impacts victims psychologically through ongoing surveillance and control, rather than through a single severe incident. Although each incident, for example accessing messages or tracking

[73] Powell, 'Technology-Facilitated Abuse: Intimate Partner Violence in Digital' 341–42.
[74] *Kurt v Austria*, para 175.
[75] Harris, 'Technology and Violence Against Women' 321.

locations, may be seen as relatively minor separately, they may collectively cause significant damage to the individual's personal autonomy and integrity.[76] However, under the existing framework, risk assessment generally relies on discrete factors that can be examined individually.[77] Since the harm from remote coercive control is inherently cumulative and diffuse, a tension arises when attempting to evaluate it.

Overall, these characteristics demonstrate that while the concept of 'real and immediate risk' can be applied to remote coercive control in principle, it becomes more complex in practice. They may create difficulties for authorities in determining when the threshold has been reached. Therefore, the existing concept of risk does not fully respond to the features of remote coercive control.

### 4.2.2 Limitations of the concept of State knowledge

The assessment of 'State knowledge' in the context of remote coercive control also reveals a challenge. State knowledge can be actual or putative: actual knowledge arises where authorities are directly informed of a risk, whereas putative knowledge arises where they ought to have known of a risk based on the information available.[78] In domestic violence cases, this assessment often consists of factors, including victim complaints, previous police interventions, or visible signs of harm.

However, remote coercive control challenges these assumptions. Due to the 'anonymous' nature of such abuse, digital surveillance, unauthorised access to personal accounts, or GPS tracking may leave no clear traces for immediate recognition.[79] In many cases, particularly where spyware and covert tracking devices are used, even victims themselves may not be fully aware of the perpetrator's identity and the extent of the surveillance.[80] Consequently, this raises a key question: how can authorities acquire knowledge of a risk that may not be apparent even to the person affected?

On the other hand, in situations where victims are aware of digital abuse and able to report it, the assessment of knowledge may still present certain problems. In traditional domestic violence cases, physical violence usually results in observable injuries and tangible evidence, whereas malicious acts within remote coercive control are often more difficult to document and interpret. This is because digital evidence, such as account activity, messages, metadata, or used devices, may demand specialised technical expertise to analyse.[81] As a result, even when the authorities receive information about the abuse, assessing its significance may be challenging. This may make it

[76] Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' 598; Powell, 'Technology-Facilitated Abuse: Intimate Partner Violence in Digital Society' 341.

[77] Stoyanova, 'Fault, Knowledge and Risk within the Framework of Positive Obligations' 609.

[78] *Ibid* 604.

[79] Marganski and Melander, 'Technology-Facilitated Violence Against Women and Girls' 632.

[80] *Ibid* 626.

[81] Dragiewicz et al., 'Technology Facilitated Coercive Control' 618.

harder to recognise this information as a sign of a risk that requires intervention.

When it comes to the notion of putative knowledge, another problem appears. In traditional domestic violence cases, authorities may be expected to have putative knowledge where there are repeated reports, visible injuries, and other indications of escalating violence.[82] However, in the context of remote coercive control, such indications may be less visible or entirely absent. Where the harmful conduct is invisible, ambiguous, or diffuse, it becomes more difficult to ascertain what the authorities ought reasonably to have known.[83]

Finally, the reliance on victim reporting should be examined in this context. Unless the abuse is externally visible, the authorities' awareness of the situation may depend heavily on the victim's report; this, in turn, depends on the victim's ability to recognise and report the harm. However, the cumulative and psychological nature of remote coercive control may itself affect the victim's perception of and response to the abuse.[84] Accordingly, this reveals a gap between the existence of harm and the State's capacity to acquire knowledge of it.

### 4.2.3 Limitations of the concept of seriousness

The seriousness of the harm plays a central role in determining whether conduct falls within the scope of Article 3 or Article 8 of the Convention. As noted earlier, Article 3 requires a relatively high level of severity, typically linked to serious physical violence or treatment causing significant suffering. By contrast, Article 8 provides a broader framework, involving interferences with private life, psychological integrity, and personal autonomy.

In the context of remote coercive control, the assessment of seriousness raises particular difficulties. This form of abuse is mainly psychological and often non-physical, and it does not necessarily cause visible injury and immediate physical harm. As a result, it may be challenging to determine whether such conduct reaches the threshold of severity required under Article 3. At the same time, the cumulative nature of the harm challenges this assessment. The impact of remote coercive control often develops gradually, with repeated acts that weaken the individual's autonomy and personal security. The cumulative effect of repeated conduct may be significant, but applying this approach to patterns of digital abuse may demand a more nuanced evaluation of how harm develops over time.

As regards Article 8, at first sight, it may be seen more readily applicable to remote coercive control due to its broader scope. Interferences with privacy, correspondence, and psychological integrity align more closely with

[82] Stoyanova, 'Fault, Knowledge and Risk within the Framework of Positive Obligations' 610.

[83] Marganski and Melander, 'Technology-Facilitated Violence Against Women and Girls' 632.

[84] Woodlock et al., 'Technology as a Weapon in Domestic Violence' 375; Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' 591.

the characteristics of remote coercive control. Nevertheless, the seriousness of such interference remains uncertain even within the framework of Article 8. In particular, the absence of visible harm and the hidden nature of digital control can complicate the determination of the threshold which is necessary for State intervention. Also, without a clearly identifiable incident, assessing the seriousness of the conduct may be more difficult. In traditional domestic violence cases, the severity of harm depends on identifiable acts, such as physical assaults or explicit threats. Yet, in remote coercive control, the harm is not necessarily confined to a single moment but is instead distributed across a pattern of behaviour. In other words, it consists of multiple malicious acts which collectively constitute a pattern of remote coercive control.[85] Accordingly, as this form of abuse does not involve more concrete and observable indicators, it becomes more challenging to assess the seriousness of the harm, and, consequently, a tension between remote coercive control and the traditional framework emerges.

In conclusion, on the one hand, the analysis of risk, State knowledge, and seriousness demonstrates that the existing framework of positive obligations can, in principle, be applied to remote coercive control. On the other hand, the specific characteristics of this form of abuse raise challenges for each of these concepts. These challenges do not undermine the framework itself, yet they highlight that its application in the context of technology-facilitated abuse may require a more careful interpretation.

## 4.3 Systematisation of Doctrinal Limitations

In the previous section, the doctrinal tensions that emerge when applying the positive obligations framework to remote coercive control were demonstrated. These tensions were analysed through the concepts of risk, State knowledge, and seriousness of harm within the Court's jurisprudence. First, the concept of risk reveals an immediacy problem. In remote coercive control, clearly identifiable points are less distinct, as harm evolves gradually rather than occurring at specific moments. As a result, it becomes difficult to ascertain a real and immediate risk. Second, the concept of State knowledge exposes a visibility problem. When digital abuse is hidden and hard to detect, determining both actual and putative State knowledge becomes more challenging. Third, the concept of seriousness raises a threshold problem. In the context of remote coercive control, harm is mostly psychological, diffuse, and cumulative, complicating the determination of when it reaches the required threshold of severity. Overall, these are not isolated difficulties; rather, they reflect a broader tension between the doctrinal assumptions of positive obligations and the distinctive characteristics of remote coercive control.

[85] Powell, 'Technology-Facilitated Abuse: Intimate Partner Violence in Digital Society' 341.

Whereas this section focuses on the systematisation of these doctrinal limitations. They can be systematised into four broader patterns. Each of them reflects a structural feature of the existing framework and its interaction with the distinctive characteristics of remote coercive control.

The first pattern of limitation concerns the continuity of remote coercive control. Within this form of abuse, harm is not limited to specific events. It occurs as an ongoing pattern of surveillance, monitoring, and psychological pressure, and there is often no clear beginning or ending point.

This directly impacts the assessment of risk. While the existing doctrine expects harm to escalate through identifiable incidents, continuous patterns of abuse may prevent the determination of clear signs that signal immediacy. Consequently, the legal assessment of risk may be unclear. Similarly, the continuous nature of abuse also affects the assessment of seriousness. Although in the traditional framework the Court's analysis often relies on discrete and identifiable incidents, in remote coercive control harm is not easily divided into separate components. It gradually continues to develop, consisting of individual malicious acts. Each of these acts, even though their combined effect is severe, may be seen as minor when assessed separately.[86] Therefore, this may challenge the assessment of the seriousness of continuous harm.

The second pattern concentrates on the spaceless nature of remote coercive control. Typically, this form of abuse occurs remotely, without physical proximity. Digital technologies enable perpetrators to exercise coercive control regardless of location, allowing harmful conduct to continue even after the physical separation of the parties.[87]

This nature affects the assessment of risk. Unlike traditional cases where removing physical proximity reduces the risk and likelihood of harm, harm in remote contexts may persist uninterrupted despite physical separation. As a result, this weakens the importance of spatial factors within the assessment of risk. Moreover, protective measures designed for traditional domestic violence cases are often conceived as means of containing physical proximity and interrupting the abuse. However, when it comes to remote coercive control, such measures become less effective, since the digital environment allows abuse to occur without physical proximity.

The third pattern of limitation centres on the relative invisibility of remote coercive control. Many forms of digital abuse, such as covert surveillance, non-consensual access to personal accounts, and GPS tracking, are usually hidden, leaving no visible traces. Even where evidence exists, it may be

[86] Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' 598; Powell, 'Technology-Facilitated Abuse: Intimate Partner Violence in Digital Society' 341.

[87] Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' 592.

uncertain, and its detection and interpretation may require technologically specialised expertise.[88]

This, in turn, has a significant effect on the concept of State knowledge. Actual knowledge becomes harder to establish when victims themselves are uncertain about the existence of the abuse and cannot report it to the authorities. Similarly, putative knowledge can be affected, as the absence of visible signs complicates the determination of what authorities ought reasonably to have known. Furthermore, the anonymous nature of the abuse influences the assessment of the seriousness of harm. When harm is hidden, it becomes more challenging to recognise its severity. Psychological harm, especially when it develops gradually, may not be immediately apparent to legal authorities. Therefore, the invisibility of the abuse undermines an effective response to remote coercive control.

The fourth and last pattern of limitation addresses the cumulative nature of harm experienced in remote coercive control. This form of abuse causes a persistent condition of anxiety, fear, and restricted personal autonomy. Victims may gradually adapt their actions to remote coercive control by limiting their communication, movement, and personal expression.[89] Over time, this can create a sense of omnipresence.

Significantly, this cumulative impact challenges the existing doctrinal framework in several respects. In terms of seriousness, when harm develops gradually, it can be harder to measure its severity, as existing thresholds for assessing harm often emphasise forms of suffering that are immediately observable. Similarly, in relation to risk, the cumulative nature of such harm makes it harder to identify a point at which the situation becomes sufficiently urgent to require intervention. Consequently, cumulative psychological harm reveals the limits of a framework that does not fully consider how the victim's experience evolves over time.

Overall, these challenges reflect broader structural patterns within the framework of positive obligations. Together, they reveal how the doctrine is shaped by assumptions that do not fully align with the characteristics of remote coercive control.

Importantly, this analysis should not be understood as indicating a failure of the existing doctrinal framework. The Court's jurisprudence is sufficiently flexible to accommodate evolving forms of harm, including those facilitated

[88] Dragiewicz et al., 'Technology Facilitated Coercive Control' 618.

[89] Woodlock et al., 'Technology as a Weapon in Domestic Violence' 375; Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' 591.

through digital technologies.[90] However, the analysis highlights that this flexibility faces certain tensions when applying the doctrine to new contexts.

Therefore, these systematised limitations indicate that the application of positive obligations to remote coercive control places the existing doctrinal framework under conceptual strain. In doing so, they raise broader questions about how harm, risk, and State responsibility are understood within the Court's jurisprudence.

[90] Ronagh JA McQuigg, 'The Evolving Jurisprudence of the European Court of Human Rights on Domestic Abuse' in Philipp Czech, Lisa Heschl, Katrin Lukas, Manfred Nowak and Gerd Oberleitner (eds), *European Yearbook on Human Rights 2022* (Intersentia 2022) 224.

# 5 Analysis of Relevant ECtHR Case-Law

European human rights case law has long been an influential force for positive change with respect to domestic violence.[91] At the same time, it increasingly reflects the challenges posed by technological mediation in domestic violence cases. As the leading human rights court in Europe and a thought-leader in human rights practice more generally, the ECtHR has gradually developed a jurisprudence that recognises technology-facilitated conduct as a part of domestic violence. It has increasingly acknowledged that domestic violence can occur online and through technology, and that States may be held accountable for failing to respond effectively. This development reflects an attempt to apply existing domestic violence standards to digital contexts. This jurisprudence demonstrates both important advances and ongoing limitations in addressing digital harm.

The Court has addressed technology-facilitated abuse in depth through its significant cases of *Buturugă v Romania*, *Volodina v Russia (No. 2)* and *M.Ş.D. v Romania*. The selection focuses on cases that explicitly examine technology-facilitated conduct in domestic and intimate relationship settings and engage in Articles 3 and 8 of the ECHR. It includes both landmark and recent judgments, highlighting the Court's evolving stance.

Overall, this chapter examines how the Court applies its existing doctrinal framework to technology-facilitated abuse, and it assesses to what extent the Court's jurisprudence indirectly captures the dynamics of remote coercive control.

## 5.1 Analysis of *Buturugă v Romania*

This case concerns a context of intimate partner violence during and after the applicant's marriage. The applicant reported repeated physical assaults, death threats, and intimidation by her former husband, particularly during divorce proceedings.[92] Alongside physical violence, she alleged that he had accessed her private electronic accounts, including her Facebook account, and copied personal communications and data.[93] Despite filing complaints and requesting investigative measures, including a forensic examination of digital devices, the authorities did not extend beyond physical incidents and dismissed the relevance of digital interference. Criminal proceedings were discontinued, and the alleged breach of correspondence was not substantively investigated.

[91] McQuigg, *Domestic Abuse and the European Court of Human Rights* 101–06.
[92] *Buturugă v Romania*, para 6.
[93] *Ibid* para 11.

The case was examined under Articles 3 and 8 of the Convention. The central legal issue was whether the Romanian authorities fulfilled their positive obligations to protect the applicant from domestic violence and to conduct an effective investigation into her allegations.[94] This included both physical violence and the alleged breach of the secrecy of correspondence. The Court assessed whether the State adequately responded to a situation involving risks to the applicant's physical and psychological integrity, and whether the investigative framework sufficiently addressed all relevant aspects of the abuse.[95]

The Court identified risk mainly by relying on specific incidents of physical violence and explicit threats. It emphasised the applicant's reports of assault and death threats, supported by a forensic medical certificate.[96] While it acknowledged the seriousness of domestic violence as a phenomenon, the assessment of risk remained limited to identifiable acts and evidence of harm. The Court did not conceptualise risk as arising from ongoing patterns of coercion, but instead framed it through discrete events capable of demonstrating immediate harm.

State knowledge was based on the applicant's complaints to the authorities and supporting evidence, including medical documentation and witness statements. The Court considered that the authorities had actual knowledge of the risk, given that the applicant had formally reported the incidents within a reasonable time frame.[97] It rejected the Government's argument that delays undermined the investigation and stressed that psychological factors must be taken into account in domestic violence cases. However, the Court also highlighted deficiencies in the authorities' response, particularly their failure to gather sufficient evidence and to investigate the case as one involving domestic violence.[98]

The seriousness of the harm is based on the assessment of the case under both Articles 3 and 8, which reflects the dual nature of the harm. Physical violence and threats fell within the scope of Article 3, whereas issues concerning private life and correspondence were examined under Article 8. The Court determined that the harm reached the threshold of seriousness under Article 3, especially considering the applicant's vulnerability as a victim of domestic violence.[99] At the same time, it emphasised that domestic violence also encompasses psychological harm and other non-physical forms of abuse.[100]

[94] *Buturugă v Romania*, paras 43–44.
[95] *Ibid* para 79.
[96] *Ibid* para 66.
[97] *Ibid* para 69.
[98] *Ibid* para 68.
[99] *Ibid* para 60.
[100] *Ibid* para 74.

However, the assessment of seriousness remained closely linked to the presence of physical injury and identifiable incidents.

A significant feature of the judgment is its recognition of digital interference as a part of domestic violence. The Court explicitly acknowledged that harmful actions such as unauthorised access to electronic communications, monitoring, and data extraction may constitute relevant forms of abuse within intimate relationships.[101] It also accepted that cyberviolence, including intrusions into cyberprivacy and cybersurveillance, can form an essential component of domestic violence.

However, despite this recognition, the treatment of technology remains structurally limited. From a doctrinal perspective, digital abuse was not analysed distinctly, but rather as an element considered together with physical violence. In fact, technology-facilitated violence, in itself, is not understood as a new and separate category of violence, nor as an alternative to offline abuse; digital technologies do not create new violence, but they transform how abuse is committed and perpetuated.[102] Nonetheless, doctrinally, it may require distinct attention, as it alters how harm operates. In this context, the Court criticised the domestic authorities for failing to investigate the applicant's allegations of digital intrusion, emphasising that such conduct should have been examined on the merits.[103] Yet, it did not develop a distinct framework for assessing the impact of technological abuse.

As a result, technology appears as an extension of existing categories of harm rather than as a phenomenon requiring conceptual adaptation. The Court includes digital elements in the broader understanding of domestic violence, but does not fully articulate their specific characteristics, such as persistence, invisibility and psychological effects.

In conclusion, this landmark judgment represents an important step by recognising technology-facilitated abuse within the scope of domestic violence. It reflects the Court's willingness to interpret existing doctrinal frameworks to address new forms of harm.[104] On the other hand, the reasoning indicates a potential challenge in fully capturing the nature of such abuse.

In particular, the focus on identifiable incidents and physical violence as main signs of risk and seriousness may confine the capacity of the doctrine to address forms of harm that are less visible and more continuous.[105] The

[101] *Buturugă v Romania*, para 74.

[102] Van der Wilk, 'Protecting Women and Girls from Violence in the Digital Age' 9.

[103] *Buturugă v Romania*, paras 75–76.

[104] Adaena Sinclair-Blakemore, 'Cyberviolence Against Women Under International Human Rights Law: *Buturugă v Romania* and *Volodina v Russia (No 2)*' (2023) 23(1) *Human Rights Law Review* 27.

[105] *Ibid* 24–25.

Court's analysis does not sufficiently engage with the distinct impacts of such conduct on victims. Overall, this highlights a tension between the framework's adaptability to new forms of harm and its underlying assumptions.

## 5.2 Analysis of *Volodina v Russia (No. 2)*

According to the facts of this case, the applicant had previously been in an abusive relationship involving physical violence, threats, and coercive behaviour.[106] After the relationship ended, the abuse continued in digital form. The perpetrator hacked her social media account, published intimate photographs, and created fake profiles using her identity.[107] He also sent repeated death threats via online platforms and tracked her movements using a GPS device.[108] The applicant reported these incidents multiple times, providing evidence such as screenshots and account data. However, the authorities delayed opening a criminal investigation, failed to take protective measures, and ultimately the proceedings were discontinued due to the statute of limitations.[109]

The case of *Volodina (No. 2)* was assessed under Article 8 of the Convention, focusing on the State's positive obligations to protect the applicant's private life and psychological integrity. The key legal question was whether the authorities fulfilled their obligations to provide an adequate legal framework, take preventive measures against a known risk of abuse, and conduct an effective investigation into repeated acts of technology-facilitated violence.[110] Thus, the case tests how the positive obligations framework operates when harm is primarily digital, cumulative, and less immediately visible than physical violence.

As regards the reasoning, the Court recognised that the applicant faced a real and ongoing risk to her psychological integrity.[111] Importantly, risk was not tied to a single imminent physical incident but to a pattern of conduct, including surveillance, impersonation, and threats.[112] The Court identified risk through a series of individual acts, including the publication of intimate images, the creation of fake profiles, GPS tracking, and threats, all of which intensified the applicant's distress and insecurity.[113] Significantly, the Court criticised the domestic authorities for failing to take a 'global view' of the situation.[114] This reflects a partial recognition that risk develops through ongoing repetition and escalation, rather than through discrete events.

[106] *Volodina v Russia (No. 2)*, para 5.
[107] *Ibid* para 6.
[108] *Ibid* paras 11, 17.
[109] *Ibid* para 20.
[110] *Ibid* para 33.
[111] *Ibid* para 57.
[112] *Ibid* paras 48, 50, 56, 66.
[113] *Ibid* paras 50, 56, 57.
[114] *Ibid* para 66.

Nevertheless, the doctrinal framing remains grounded in identifiable incidents; this, in turn, reflects an approach that still prioritises immediacy over the ongoing nature of digital abuse.[115]

State knowledge was mainly based on repeated complaints by the applicant. She reported the hacking, impersonation, threats, and tracking device to the authorities, often providing supporting evidence.[116] The Court considered this sufficient to trigger actual knowledge, highlighting that the authorities were aware of the interference with her rights but did not act promptly and effectively.[117] Furthermore, the Court also hinted at putative knowledge, given the seriousness and persistence of the allegations. It explicitly stated that its findings from the first *Volodina* case regarding the 'known risk of recurrent violence' were directly 'applicable in the circumstances of the present case'.[118] By referencing the previous case, the Court highlighted that the authorities were already on notice regarding the perpetrator's behaviour and ought to have known that the cyberviolence was a continuation of that same pattern of abuse.

However, the reasoning reveals a reliance on formal visibility. Specifically, knowledge is gained through explicit reports and tangible evidence. The authorities dismissed threats as not 'real' and delayed investigative steps; their reluctance to act shows that digital abuse may be underestimated when it does not meet traditional evidentiary requirements.[119] The Court criticised delays, jurisdictional confusion, and the failure to promptly collect digital evidence, noting that these shortcomings undermined the effectiveness of the investigation and ultimately led to impunity.[120]

In the case of *Volodina v Russia (No. 2)*, the seriousness of the harm concerns Article 8. The Court assessed it under Article 8, framing it as an interference with the applicant's private life and psychological integrity. It explicitly recognised that cyberviolence, including the non-consensual dissemination of intimate images, impersonation, and online threats, can cause 'anxiety, distress and insecurity'.[121]

Despite recognising the seriousness of the harm, the Court did not find that it reached the threshold of Article 3. This suggests that psychological harm, even when severe and persistent, is more readily addressed under Article 8.[122]

---

[115] Sinclair-Blakemore, 'Cyberviolence Against Women Under International Human Rights Law' 23.

[116] *Volodina v Russia (No. 2)*, para 56.

[117] *Ibid* paras 50, 68.

[118] *Ibid* para 61.

[119] *Ibid* para 66.

[120] *Ibid* paras 63, 64, 67, 68.

[121] *Ibid* para 50.

[122] Ronagh JA McQuigg, 'The European Court of Human Rights and Domestic Violence: Volodina v Russia' (2021) 10(1) *International Human Rights Law Review* 155, 164.

At the same time, the Court emphasised that the acts were sufficiently serious to require a criminal-law response, particularly given their humiliating and degrading nature.[123] The failure to ensure accountability was seen as undermining deterrence and public confidence in the rule of law.[124] Thus, seriousness is recognised, but its doctrinal placement within Article 8 suggests a continued differentiation between physical and primarily psychological forms of harm.[125]

In comparison with the case of *Buturugă*, this one provides a more explicit and comprehensive engagement with technology-facilitated abuse. It expands on the principles established in *Buturugă* to address a wider spectrum of digital harms. In addition to identifying cyberviolence as a form of domestic violence, the case of *Volodina (No 2)* clearly encompasses behaviours such as online harassment, malicious impersonation, and digital surveillance within the concept of technology-facilitated abuse.[126] At the same time, the Court reiterates that online violence is not a separate category but a 'facet of the complex phenomenon of domestic violence'.[127] This aligns with the understanding that technology does not create new forms of violence, but transforms how existing patterns of control and abuse are exercised.[128]

However, the Court's reasoning also exposes an implicit limitation. Although it acknowledges the seriousness and variety of digital abuse, it does not develop a distinct analytical framework that captures its specific characteristics, as in the *Buturugă* case. Accordingly, technology is regarded as both central and conceptually underdeveloped. It plays a central role in the factual background and in identifying harm, but it still remains embedded within existing doctrinal categories without conceptual refinement. The Court recognises cumulative harm to some extent, particularly by criticising the authorities' failure to adopt a 'global view'.[129] However, it ultimately analyses the case through discrete incidents.[130] This results in an approach that acknowledges digital abuse as a core component of domestic violence while only partially engaging with its transformative impact on the nature of harm and control.[131]

---

[123] *Volodina v Russia (No. 2)*, para 57.

[124] *Ibid* para 67; Niels Hedlund, 'The ECHR and the Positive Obligation to Criminalise Domestic Psychological Violence' (2024) 24(3) *Human Rights Law Review* 8.

[125] Róisín Á Costello, 'Volodina v Russia (No 2): Intimate Images, Domestic Violence and the Positive Obligations of Member States under Article 8 ECHR' (2021) 7 *European Data Protection Law Review* 614, 619.

[126] *Volodina v Russia (No. 2)*, para 48.

[127] *Ibid* para 49.

[128] Van der Wilk, 'Protecting Women and Girls from Violence in the Digital Age' 9.

[129] *Volodina v Russia (No. 2)*, para 66.

[130] Sinclair-Blakemore, 'Cyberviolence Against Women Under International Human Rights Law' 25.

[131] Costello, 'Volodina v Russia (No 2)' 619.

In conclusion, the Court's reasoning in the judgment of *Volodina (No. 2)* demonstrates a significant step forward in recognising technology-facilitated abuse within the framework of positive obligations. Its acknowledgment of cyberviolence as part of domestic violence, and its emphasis on the need for a comprehensive investigative response, reflect an evolving understanding of the phenomenon. Nevertheless, the analysis indicates a potential challenge in adequately addressing such cases within the current doctrinal structure. There is still reliance on incident-based reasoning and formal indicators of risk and State knowledge, and it does not align well with patterns of digital abuse that are cumulative, diffuse, and often invisible.

## 5.3 Analysis of *M.Ș.D. v Romania*

This case deals with a young woman who was the victim of technology-facilitated abuse by her former partner following the end of their relationship. The applicant, an eighteen-year-old student, began a brief relationship with her partner through social media, during which they exchanged intimate images.[132] Following their separation, the perpetrator engaged in a pattern of digital abuse: he created fake social media profiles impersonating the applicant, disseminated her intimate photographs to relatives, and posted them on escort websites alongside her personal details, leading to sustained harassment by third parties.[133] He also issued threats and displayed offline aggression. Although the applicant submitted complaints and provided digital evidence, the authorities delayed investigative measures and ultimately undermined the seriousness of the conduct, framing it as consensual and lacking criminal relevance: the applicant had willingly sent the intimate photos, and there was no public interest in pursuing the computer-related forgery case.[134]

As with previous cases, this one falls under Article 8 of the Convention, concerning the State's positive obligation to protect the applicant's private life against interference by private individuals. The central legal question was whether Romania fulfilled its positive obligations by providing an adequate legal framework capable of addressing the non-consensual dissemination of intimate images and by conducting a prompt, thorough, and effective investigation into the applicant's allegations of online harassment and impersonation.[135]

The Court clearly recognised the existence of a serious and ongoing risk to the applicant's psychological integrity. This risk was identified both in the initial acts of dissemination and in their consequences, particularly exposure to harassment by unknown individuals, reputational harm, and long-term

[132] *M.Ș.D. v Romania* (App no 28935/21) Judgment of 3 December 2024, para 5.
[133] *Ibid* paras 6–10.
[134] *Ibid* paras 11–70.
[135] *Ibid* paras 99, 127.

psychological damage.[136] Importantly, the Court highlighted that the perpetrator acted out of revenge and with the purpose of publicly humiliating and degrading the applicant.[137] However, the Court articulated risk by focusing largely on individual incidents rather than considering it as a continuous pattern of abuse. While it noted that the perpetrator continued his behaviour after the complaint and explicitly refused to stop, the analysis does not fully conceptualise the situation as an escalating course of conduct. Therefore, the immediacy of risk is determined by harm that has already occurred, rather than by considering the likelihood of future harm.

State knowledge was clearly confirmed through the applicant's detailed complaint, which consisted of incriminating evidence and explicit references to ongoing harassment; this is why the authorities had actual knowledge of both the conduct and the risk of its continuation.[138] Nevertheless, the Court highlighted significant delays and omissions. The investigation was opened only after six months, and the suspect was questioned nearly two years after the complaint.[139] During this period, the authorities failed to gather digital evidence. Moreover, they did not take protective measures, even though the applicant had explicitly warned that the perpetrator would continue his actions.[140] Furthermore, the Court emphasised inappropriate conduct within the investigative process, including elements of victim-blaming and dismissiveness.[141] Such negligence reflects a deeper issue in how harm is interpreted and addressed.

When it comes to the seriousness of the harm, the Court unequivocally considered the acts to reach the threshold of Article 8. It stressed that the non-consensual dissemination of intimate images, particularly when intended to humiliate, degrade, and expose the victim to public harassment, amounts to a serious interference with private life.[142] Crucially, the Court found that the seriousness of the harm required a criminal-law response, rejecting the argument that civil remedies would be sufficient.[143] The psychological consequences, such as long-term trauma and social isolation, played a central role in this assessment.[144] Nonetheless, the domestic authorities had failed to reflect this seriousness in practice. They interpreted legal provisions narrowly, dismissed certain charges, and allowed others to expire under the statute of limitations.[145] The resulting lack of accountability undermined the deterrent function of the legal system, leading the Court to conclude that the

[136] *M.Ş.D. v Romania*, para 123.
[137] *Ibid*.
[138] *Ibid* para 140.
[139] *Ibid* para 139.
[140] *Ibid* para 140.
[141] *Ibid* para 147.
[142] *Ibid* para 121.
[143] *Ibid* para 125.
[144] *Ibid* para 123.
[145] *Ibid* para 146.

State had failed to meet its positive obligations under Article 8 of the Convention.[146]

As regards the Court's treatment of technology, it explicitly situates malicious digital acts within its broader jurisprudence on technology-facilitated abuse, recognising them as forms of online harassment and cyberviolence. It acknowledges that digital elements, such as fake social media accounts, dissemination of images, and online impersonation, are capable of producing serious psychological harm.[147]

Nevertheless, a similar limitation arises in this case as well: the Court does not fully theorise the specific characteristics of technology-facilitated abuse. On the one hand, it touches on them to a certain extent by recognising that online abuse can intensify harm, particularly through scale, anonymity, and persistence. On the other hand, the Court does not provide a detailed explanation of these features and only briefly addresses them in its reasoning. Technology is regarded mainly as an instrument of harm, rather than as a factor capable of reshaping the nature of the harm itself. Moreover, the Court characterises the authorities' failure to secure digital evidence as a procedural domestic issue, rather than as indicative of a broader institutional limitation in dealing with technology-facilitated harm. As a result, while technology appears central in fact, it remains underdeveloped in doctrine, limiting the Court's ability to fully address the specific dynamics of technology-facilitated domestic violence.

This case shows in particular that the reliance on incident-based reasoning suggests a challenge in conceptualising technology-facilitated abuse as a continuous and cumulative process. This reflects a potential disconnection between the doctrinal framework and the reality of digital abuse. Overall, the case demonstrates that although the framework can include technology-facilitated violence, it does so inconsistently and under conceptual tension.

## 5.4 Remote Coercive Control Through the Lens of Analysed Judgments

The three cases analysed above reflect the ECtHR's increasing attention to technology-facilitated domestic violence. In all three cases, digital conduct is recognised as a significant element, forming part of the factual and legal assessment. The Court explicitly acknowledges cyberviolence, online harassment, and the dissemination of intimate images as capable of violating Convention rights. At the same time, this engagement still relies on the existing doctrinal framework of positive obligations. As a result, while the Court encounters circumstances involving remote coercive control, it addresses them by using concepts and assumptions that were mainly designed

[146] *M.Ş.D. v Romania*, paras 156, 158.
[147] *Ibid* para 123.

for more traditional forms of domestic violence. This section synthesises this limited connection between the Court's approach in its jurisprudence on technology-facilitated abuse and the characteristics of remote coercive control, which challenge the existing framework.

First and foremost, the tension between the feature of continuity and the Court's reasoning emerges across these cases. In all three judgments, the Court recognises that abuse may consist of multiple acts committed over time. In *Volodina (No. 2)*, for example, it criticises the authorities for failing to take a 'global view' of the applicant's situation.[148] Similarly, in *M.Ş.D.*, the Court affirms that the dissemination of intimate images produced ongoing consequences, particularly repeated harassment and long-term psychological harm.[149] Despite these reasonable observations, the Court largely relies on discrete incidents in its analytical structure. In other words, it separates individual incidents within a continuous pattern of abuse and gives room to each separately. For instance, risk is identified through specific acts such as the publication of images, threats, and unauthorised access. Yet it could instead be considered as arising from the continuous condition created by them. This is because the legal assessment fragments the abusive situation into isolated incidents, making it harder to recognise the persistent and escalating nature of the harm.[150] This can delay and weaken intervention, given that no single act may appear sufficiently urgent when viewed in isolation, even though their combined effect, more precisely, their overall pattern generates a serious and ongoing risk.[151] Accordingly, this reveals that the Court does not fully conceptualise abuse as a continuous process. By contrast, remote coercive control operates through continuity, where harm arises from its persistent nature.

A further tension arises when the existing framework encounters the nature of remoteness. In traditional domestic violence cases, risk is often closely linked to physical proximity and immediate danger. However, technology-facilitated abuse challenges this assumption, as in the cases analysed above, where harm frequently occurs after the end of the relationship and without physical proximity. In these cases, the abuse continues remotely through technology-facilitated and malicious actions, such as impersonation, dissemination of images, and online threats. The Court recognises that such acts can generate fear, distress, anxiety, and insecurity equivalent to offline violence.[152] Nevertheless, assumptions that are applied to the remoteness of digital abuse remain embedded within the existing doctrine. Risk assessment

[148] *Volodina v Russia (No. 2)*, para 66.

[149] *M.Ş.D. v Romania*, para 123.

[150] Sinclair-Blakemore, 'Cyberviolence Against Women Under International Human Rights Law' 23.

[151] Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' 598; Powell, 'Technology-Facilitated Abuse: Intimate Partner Violence in Digital Society' 341.

[152] *Buturugă v Romania*, para 74; *Volodina v Russia (No. 2)*, paras 49, 50; *M.Ş.D. v Romania*, paras 121, 123.

still tends to depend on immediacy, which aligns more easily with situations involving physical danger. As a result, situations of ongoing digital abuse may not be regarded as posing a sufficiently real and immediate risk, even where the harm is persistent and escalating, thereby reducing the likelihood of timely protective measures.[153] Overall, remote coercive control disrupts the relevance of physical proximity, but the doctrinal structure does not fully adapt to this transformation.

Thirdly, invisibility causes the tension of State knowledge. Across all three cases, the Court affirms the establishment of State knowledge primarily through victim complaints and the submission of evidence. In *Buturugă*, knowledge is based on reports of violence and requests for forensic examination; in *Volodina (No. 2)* and *M.Ș.D.*, it derives from repeated complaints together with digital material such as screenshots and account data.[154] This reflects a reliance on formal visibility: once harm is reported and substantiated, authorities are expected to act. However, the cases also reveal the limits of this approach. Digital abuse, including remote coercive control, may be difficult to detect, interpret, and even regard as harmful.[155] For instance, in *M.Ș.D.*, the authorities not only failed to gather digital evidence but also misinterpreted the legal significance of the conduct, treating the applicant's sending of the intimate photos as consensual and finding no public interest in pursuing the computer-related forgery case.[156] This suggests a further and deeper difficulty: even when evidence exists, its meaning may not be adequately understood. Remote coercive control, which may occur in hidden and ambiguous ways, exposes this gap between the requirement of visibility and the reality of digital abuse.

Finally, the cumulativeness of digital harm reveals a further tension. In all three cases, the Court acknowledges that technology-facilitated abuse can cause serious psychological consequences. In *Volodina (No. 2)* and *M.Ș.D.*, it explicitly refers to anxiety, distress, and long-term psychological impact, and emphasises that such harm may require a criminal-law response.[157] However, the doctrinal framework continues to assess seriousness by reference to defined thresholds, which are more easily met in cases involving immediately observable harm. This creates a specific difficulty in cases of remote coercive control, where harm develops gradually over time. Significantly, cumulative harm results in a persistent condition of fear, anxiety, and restricted autonomy.[158] It does not emerge as a clearly identifiable moment of severity. Victims may progressively adapt their behaviour in response to the perceived

[153] Dragiewicz et al., 'Technology Facilitated Coercive Control' 610–11.

[154] *Buturugă v Romania*, para 66; *Volodina v Russia (No. 2)*, para 56; *M.Ș.D. v Romania*, para 139.

[155] Marganski and Melander, 'Technology-Facilitated Violence Against Women and Girls' 626.

[156] *M.Ș.D. v Romania*, paras 36, 140, 146.

[157] *Volodina v Russia (No 2)*, para 57; *M.Ș.D. v Romania*, para 121.

[158] Woodlock et al., 'Technology as a Weapon in Domestic Violence' 372.

omnipresence of the perpetrator, for example, by limiting communication, altering daily routines, or censoring personal expression.[159] In this sense, the harm can potentially reshape the victim's lived experience over time. However, within a framework based on thresholds of seriousness, this gradual impact is less visible. Gradually developing harm can be harder to evaluate in terms of severity, given that existing thresholds often focus on immediately observable forms of suffering.[160] As a result, cumulative psychological harm may be recognised in principle, but in doctrinal terms, it may remain difficult to fully capture. It complicates the assessment of seriousness by making it harder to identify when harm reaches a sufficiently severe threshold. It also hinders the assessment of risk by obscuring when the situation becomes urgent enough to trigger intervention. This shows a structural limitation: the framework does not adequately address how harm evolves and becomes more severe over time.

Taken together, this indicates that the Court's jurisprudence is in a process of adaptation. The cases reflect not only an increasing judicial sensitivity to technology-facilitated abuse, but also an openness to interpreting existing standards through the lens of new forms of harm. On the other hand, the Court's adaptation remains limited in its underlying doctrinal assumptions. In fact, these specific characteristics do not prevent the Court from addressing technology-facilitated abuse, but they shape how such abuse is understood and evaluated. Accordingly, the Court's case-law reveals not a failure, but a structural limitation. The Court already encounters situations that closely resemble remote coercive control, and it partially captures their dynamics through existing concepts. However, it does not yet fully conceptualise these situations as a distinct form of harm. Therefore, the result is a jurisprudence that is both evolving and limited: recognising new realities, but still confined within an inadequate framework.

[159] Woodlock et al., 'Technology as a Weapon in Domestic Violence' 375; Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' 591.

[160] Sinclair-Blakemore, 'Cyberviolence Against Women Under International Human Rights Law' 23.

# 6 Reconsidering Positive Obligations in the Context of Remote Coercive Control

As demonstrated previously, remote coercive control is not external to the Strasbourg Court's jurisprudence, but is already indirectly embedded within it, though not fully articulated. The analysis has revealed that the existing framework of positive obligations is capable of addressing technology-facilitated abuse, but it faces significant conceptual difficulties.

Based on this background, this chapter shifts the focus from analysis to implications. Notably, it neither proposes a new legal framework, nor does it aim to reconstruct the existing framework of positive obligations developed by the Court. Instead, it explores what follows from the tensions identified. In particular, it examines how these tensions may contribute to a more refined understanding of the Court's existing approach, and what this can suggest for its future development.

## 6.1 From Doctrinal Tension to Doctrinal Reconsideration

The preceding chapters expose not isolated shortcomings, but a structural misalignment between the Court's doctrinal assumptions and the operational logic of remote coercive control. This misalignment does not amount to a lack of protection. On the contrary, it reflects a series of conceptual pressure points within the existing framework of positive obligations. The purpose of identifying these pressure points is not simply to restate the doctrinal tensions analysed in previous chapters; instead, it is to clarify where the existing framework experiences conceptual strain when applied to remote coercive control. In doing so, these pressure points provide the basis for considering how the Court's existing doctrine might be interpreted more contextually in future cases.

First, the concept of risk highlights a pressure on the 'immediacy' model. The Court's established requirement of 'a real and immediate risk' assumes that harm becomes legally relevant at identifiable moments of escalation. However, in the context of remote coercive control, harm tends to develop as a continuous condition rather than as a series of discrete incidents. This does not make the concept of risk inapplicable to remote coercive control, but it puts pressure on a temporal framework that prioritises imminence over persistence.[161]

[161] Sinclair-Blakemore, 'Cyberviolence Against Women Under International Human Rights Law' 23.

Second, the assessment of State knowledge reveals pressure on assumptions of visibility. The Court's reasoning continues to rely considerably on formal indicators that establish State knowledge, such as complaints, tangible evidence, and clearly articulated threats.[162] By contrast, remote coercive control carries a risk of invisibility. It frequently operates through forms of conduct that are covert, ambiguous, and technologically complex. Accordingly, the issue is not just whether authorities have sufficient information, but whether the framework adequately recognises how such information becomes identifiable.

Third, the concept of seriousness places pressure on the establishment of thresholds. The Court has demonstrated an increasing willingness to acknowledge psychological harm, particularly under Article 8.[163] Nonetheless, its assessment often remains embedded in identifiable acts and their immediate severity. In cases of remote coercive control, harm arises gradually from the combined effect of individually minor acts. This places strain on a threshold-based model that struggles to account for the gradual intensification of harm.

Taken together, these tensions show that the framework continues to rely heavily on event-based forms of reasoning. Even when addressing forms of abuse that are continuous, diffuse, and evolving, the doctrinal framework continues to approach harm through discrete events. This, in turn, gives rise to a tension between the event-based logic of legal reasoning and the continuous nature of remote coercive control.

Overall, these dynamics should not be understood as a failure of the Court's protective function. In fact, the jurisprudence shows that existing legal categories are capable of accommodating emerging forms of harm. However, when it comes to conceptualisation, limitations exist. Significantly, the framework is not incapable of addressing remote coercive control, but it is still not fully aligned with its defining characteristics. In light of this, if the framework is not incapable but strained, the question is not whether it should be replaced, but how it might be revised.

## 6.2 Reconsidering Positive Obligations for Remote Coercive Control

Reconsideration of positive obligations refers to how the Court's current doctrine might be adapted in response to the characteristics of remote coercive control. More precisely, the issue concerns how the Court's approach to defining the concepts of risk, State knowledge, and seriousness

[162] *Buturugă v Romania*, para 66; *Volodina v Russia (No. 2)*, para 56; *M.Ş.D. v Romania*, para 139.

[163] *Buturugă v Romania*, para 74; *Volodina v Russia (No. 2)*, para 50; *M.Ş.D. v Romania*, para 123.

of harm should operate so that they remain effective and do not create conceptual tensions when applied to technology-facilitated abuse.

A first area of possible reconsideration concerns the concept of risk. The pressure placed by remote coercive control on the 'immediacy' model suggests that the Court may reconsider the existing standard by prioritising the 'continuity' of harm. According to the Court's jurisprudence, positive obligations commonly arise where authorities knew or ought to have known of a 'real and immediate' risk of harm.[164] Traditionally, this formulation has been applied in situations that involve identifiable incidents, escalating threats, and physical proximity.[165] However, remote coercive control complicates this logic. Harm often develops gradually through continuous monitoring, digital surveillance, repeated intrusion, and psychological pressure. In such situations, the risk may arise not from the imminence of a single violent act, but from the continuous nature of the abusive environment.[166] Thus, the solution may not require rejecting the notion of 'real and immediate' risk, but rather adapting the understanding of 'immediacy' to continuous forms of abuse.

In this respect, this prioritises emphasising the continuity of harm, more precisely, the overall pattern of coercive control, over assessing every single identifiable incident. In practical terms, the Court's assessment could focus on whether the overall pattern of conduct creates an ongoing situation that significantly undermines the victim's psychological integrity, autonomy, and sense of security. Within such an approach, individual malicious acts would not be regarded as isolated incidents, but as indicators of a continuous environment of coercive control. Consequently, the requirement of 'immediacy' would not disappear; instead, 'immediacy' would be reconsidered through the continuous presence of harm.

This approach would still align with the Court's existing doctrine, particularly because the jurisprudence already demonstrates partial recognition of patterns and cumulative contexts. In the case of *Volodina v Russia (No. 2)*, the Court criticised the authorities' failure to adopt a 'global view' of the applicant's situation.[167] This reflects an emerging awareness that harm may become legally significant through continuity and repetition rather than isolated escalation alone.[168]

Second, the concept of State knowledge should be reconsidered. The pressure on assumptions of visibility reveals that the challenge of State knowledge is

[164] *Osman v United Kingdom*, para 116.

[165] *Kurt v Austria*, para 175; McQuigg, *Domestic Abuse and the European Court of Human Rights* 71.

[166] Powell, 'Technology-Facilitated Abuse: Intimate Partner Violence in Digital Society' 341–42.

[167] *Volodina v Russia (No. 2)*, para 66.

[168] Costello, 'Volodina v Russia (No 2)' 619.

not simply evidentiary, but interpretative. As described previously, remote coercive control is often hidden, technologically complex, and difficult to interpret.[169] This, in turn, challenges the establishment of State knowledge, which traditionally relies on visible indicators of abuse.[170] In this context, the notion of interpretative responsibility becomes significant. In the present discussion, this notion is not intended as a specific doctrinal term, but as a broader interpretative idea. It refers to the obligation of authorities not only to receive information passively, but also to recognise, contextualise, and properly interpret patterns of harm reflected in the information available to them.[171] Accordingly, in cases of remote coercive control, authorities should not passively receive evidence; they must also be capable of recognising and interpreting the dynamics of technology-facilitated abuse. As in cases such as *M.Ş.D. v Romania* and *Volodina v Russia (No. 2)*, the problem was not simply a lack of information, but was the authorities' failure to understand the significance of the information already given to them.[172] Online threats and digital harassment were regarded as minor and not sufficiently serious, and ongoing patterns of abuse were fragmented into separate incidents without contextual significance.[173]

This proves that the assessment of State knowledge may require a broader understanding of putative knowledge in cases of digital abuse. What authorities 'ought to have known' should not depend only on explicit evidence of imminent violence. Instead, the assessment may need to give priority to contextual factors, patterns of controlling behaviour, victim narratives, and the cumulative nature of reported conduct. Overall, such an approach reflects that remote coercive control changes how warning signs appear and how they must be interpreted.

A third area of reconsideration addresses the seriousness of harm. The pressure placed on the threshold-based assessment of seriousness further indicates the need for a more cumulative understanding of psychological harm. Such an assessment often remains connected to identifiable acts which are assessed individually. However, remote coercive control challenges this model. This is because the harm often develops cumulatively, and individually minor acts may collectively produce severe psychological consequences.[174] In fact, the Court's approach already entails elements that support a more cumulative perspective. In its judgment of *Volodina v Russia*

[169] Marganski and Melander, 'Technology-Facilitated Violence Against Women and Girls' 626.

[170] Stoyanova, 'Fault, Knowledge and Risk within the Framework of Positive Obligations' 610.

[171] *Ibid* 607.

[172] *M.Ş.D. v Romania*, paras 36, 140, 146; *Volodina v Russia (No. 2)*, paras 61, 66.

[173] Sinclair-Blakemore, 'Cyberviolence Against Women Under International Human Rights Law' 25.

[174] Woodlock, 'The Abuse of Technology in Domestic Violence and Stalking' 598; Powell, 'Technology-Facilitated Abuse: Intimate Partner Violence in Digital Society' 341.

*(No. 2)*, it explicitly highlighted that authorities should have assessed the situation globally, and its position reflects that seriousness cannot always be adequately evaluated through isolated incidents alone.[175] Therefore, the assessment of seriousness may require a shift in focus: from discrete minor incidents to their combined effect.

Importantly, such a reconsideration would necessitate a deeper understanding of how harm evolves in technology-facilitated environments. This may be significant specifically for Article 8, where cumulative psychological harm is already increasingly recognised.[176] On the other hand, it may also extend the application of Article 3 to especially severe cases. In particular, the Court may be required to consider whether prolonged exposure to digitally facilitated abuse can reach the minimum level of severity required under Article 3, even in the absence of sustained physical violence.[177] In this respect, severity would arise not only from the seriousness of individual acts, but also from their duration, repetition, and combined impact on the victim's mental autonomy and psychological integrity. The key point is not that all forms of remote coercive control should automatically fall within the threshold of Article 3. On the contrary, severity itself may need to be assessed through persistence and cumulative impact, instead of focusing primarily on immediately visible and physically violent acts.

Finally, it would be useful to consider the role of technology itself in a broader conceptual shift. At present, digital technologies are generally regarded as instruments which facilitate the perpetration of abuse. However, this approach risks underestimating the transformative effect of technological environments on coercive control.[178] Importantly, remote coercive control shows that technology reshapes the conditions under which control is exercised. Digital technologies enable the persistence of harm after physical separation, create conditions of omnipresence through constant connectivity, and expand the scale and permanence of abusive conduct. Accordingly, technology should not be understood simply as a tool of harm, but also as an environment shaping the nature, continuity, and intensity of abuse itself. Recognising this would not require the Strasbourg Court to create a completely new doctrinal framework. Instead, it would encourage a more context-sensitive interpretation of existing concepts within the framework of positive obligations. This approach would allow the Court to analyse

[175] *Volodina v Russia (No. 2)*, para 66.

[176] *Buturugă v Romania*, para 74; *Volodina v Russia (No. 2)*, para 50; *M.Ş.D. v Romania*, para 123.

[177] Sinclair-Blakemore, 'Cyberviolence Against Women Under International Human Rights Law' 23.

[178] María Elósegui, 'The Case Law of the European Court of Human Rights on Violence Against Women and the Intimate Image Abuse' in Gian Marco Caletti and Kolis Summerer (eds), *Criminalizing Intimate Image Abuse: A Comparative Perspective* (Oxford 2024) 71.

technology-facilitated abuse through the altered conditions of vulnerability, exposure, and persistence created by digitally mediated environments.

Overall, these considerations reflect that the challenges posed by remote coercive control do not necessarily require the European Court of Human Rights to abandon its existing positive obligations framework. By contrast, they call for a more context-sensitive interpretation of concepts that were largely developed in response to traditional forms of domestic violence. Therefore, the issue concerns whether the Court's existing conceptual assumptions are sufficiently responsive to the evolving nature of harm in digitally mediated environments, not whether its jurisprudence is capable of addressing technology-facilitated abuse. In this regard, remote coercive control does not demonstrate the failure of the framework; it highlights the circumstances that may require future doctrinal adaptation.

# 7 Conclusion

Domestic violence has increasingly evolved within digital environments, transforming how coercive control operates within intimate relationships. This thesis examined whether the ECtHR's framework of positive obligations under the Convention can adequately respond to remote coercive control as a form of technology-facilitated domestic violence. It argued that, although the Strasbourg framework remains formally capable of addressing such abuse through Articles 3 and 8, remote coercive control exposes significant conceptual tensions within a doctrinal structure largely developed in response to traditional forms of abuse, which involve visible, physically proximate, and incident-based forms of harm.

Initially, the thesis highlighted that domestic violence cannot be understood only through physical violence and discrete incidents of abuse. Through the development of coercive control theory, particularly the work of Evan Stark, the analysis demonstrated that domestic abuse frequently operates through ongoing patterns of domination, surveillance, intimidation, and restriction. Building on this, the thesis defined remote coercive control as a technology-facilitated extension of coercive control characterised by continuity, remoteness, invisibility, and cumulative psychological harm. Digital technologies such as smartphones, spyware, GPS tracking, and social media platforms alter the operational conditions of abuse by enabling constant monitoring and control without requiring physical proximity between perpetrator and victim.

Against this background, the thesis examined the positive obligations framework under the ECtHR's domestic violence jurisprudence. It described that Articles 3 and 8 provide the principal doctrinal framework through which domestic violence is addressed, particularly through the concepts of risk, State knowledge, and seriousness of harm. This doctrine does not formally exclude technology-facilitated abuse, and its concepts remain sufficiently flexible to be applied to such situations. However, the analysis further demonstrated that remote coercive control places significant pressure on the assumptions underlying the doctrine. The Court's traditional understanding of 'real and immediate risk' is uneasily applicable to forms of abuse that operate continuously rather than through identifiable moments of escalation. Similarly, assumptions of visibility challenge assessments of State knowledge in situations involving hidden and technology-enabled surveillance. Establishing the seriousness of harm also becomes more complicated where harm develops cumulatively through individually minor acts rather than through immediately observable and severe violence.

Furthermore, the analysis of the Court's jurisprudence in *Buturugă v Romania*, *Volodina v Russia (No. 2)*, and *M.Ş.D. v Romania* illustrated both the adaptability and limitations of the existing framework. These judgments

demonstrate that the Court increasingly recognises cyberviolence, digital surveillance, online harassment, and image-based abuse as forms of domestic violence. At the same time, however, it continues to rely largely on doctrinal assumptions structured around traditional forms of abuse, characterised by visibility, physical proximity, and discrete incidents of harm. Consequently, the thesis concluded that the principal issue is not the absence of legal protection, but instead the emergence of conceptual strain within an event-based doctrinal framework confronted with continuous and technology-facilitated forms of abuse.

From a doctrinal perspective, the thesis does not argue that a completely new legal framework is required. On the contrary, the ECtHR's doctrine of positive obligations already contains significant interpretative flexibility. Nevertheless, remote coercive control demonstrates that existing concepts may require more context-sensitive interpretation in digitally mediated contexts. Risk may need to be understood through continuity rather than solely imminence; State knowledge may require greater emphasis on deeper contextual interpretation rather than formal visibility alone; and seriousness may need to more comprehensively capture cumulative psychological harm developing over time. Therefore, the issue is more one of interpretative refinement than doctrinal replacement.

As regards institutional reflections, digital forms of abuse are increasingly confronted by courts, police authorities, prosecutors, and domestic institutions. In this context, the challenge is not limited to legal classification, but also concerns institutional recognition and interpretation. Technology-facilitated abuse is often covert, persistent, and psychologically embedded, making it difficult to detect and contextualise within traditional evidentiary frameworks. Thus, effective protection may depend less on entirely new legislation and more on improving the ability of authorities to understand and apply existing legal frameworks in more context-sensitive and technologically informed ways.

Finally, the thesis finds it significant to reflect on broader scholarly discussions concerning the relationship between human rights law, domestic violence, and digital technologies. Future research could further examine evidentiary standards in cases of technology-facilitated abuse, the implications of spyware and AI-assisted surveillance, comparative approaches across regional human rights systems, and the interaction between human rights law, platform governance, and digital regulation. Future research may also explore the gender-based aspects of remote coercive control and the broader relationship between technological development and coercive power within intimate relationships. It is undeniable that domestic violence continues to evolve within digital environments. As long as legal concepts remain primarily responsive to physical forms of harm, they will

probably face continuing pressure, requiring ongoing doctrinal adaptation, institutional responsiveness, and scholarly engagement.

# Bibliography

## I. Academic literature


Akandji-Kombé, Jean-François, *Positive Obligations under the European Convention on Human Rights: A Guide to the Implementation of the European Convention on Human Rights* (Council of Europe, Human Rights Handbooks No 7, January 2007). https://www.refworld.org/reference/research/coe/2007/67106, accessed 22 May 2026.

Bhat, P Ishwara, *Idea and Methods of Legal Research* (Oxford University Press 2020). https://doi.org/10.1093/oso/9780199493098.001.0001, accessed 22 May 2026.

Brookfield, Kathryn, Rachel Fyson and Murray Goulden, 'Technology-Facilitated Domestic Abuse: An Under-Recognised Safeguarding Issue?' (2024) 54(1) *The British Journal of Social Work* 419–436. https://doi.org/10.1093/bjsw/bcad206, accessed 22 May 2026.

Coombs, Elizabeth, 'Human Rights, Privacy Rights, and Technology-Facilitated Violence' in Jane Bailey, Asher Flynn and Nicola Henry (eds), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Emerald Publishing 2021) 475–491. https://doi.org/10.1108/978-1-83982-848-520211036, accessed 22 May 2026.

Costello, Róisín Á, '*Volodina v Russia (No 2)*: Intimate Images, Domestic Violence and the Positive Obligations of Member States under Article 8 ECHR' (2021) 7 *European Data Protection Law Review* 614. https://ssrn.com/abstract=4168085, accessed 22 May 2026.

Dobash, R Emerson and Russell P Dobash (eds), *Rethinking Violence against Women* (SAGE Publications 1998). https://doi.org/10.4135/9781452243306, accessed 22 May 2026.

Douglas, Heather, Bridget A Harris and Molly Dragiewicz, 'Technology-Facilitated Domestic and Family Violence: Women's Experiences' (2019)

59(3) *The British Journal of Criminology* 551–570. https://doi.org/10.1093/bjc/azy068, accessed 22 May 2026.

Dragiewicz, Molly, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P Suzor, Delanie Woodlock and Bridget Harris, 'Technology-Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms' (2018) 18(4) *Feminist Media Studies* 609–625. https://doi.org/10.1080/14680777.2018.1447341, accessed 22 May 2026.

Elósegui, María, 'The Case Law of the European Court of Human Rights on Violence against Women and Intimate Image Abuse' in Gian Marco Caletti and Kolis Summerer (eds), *Criminalising Intimate Image Abuse: A Comparative Perspective* (Oxford University Press 2024; online edn, Oxford Academic, 22 February 2024). https://doi.org/10.1093/oso/9780198877813.003.0004, accessed 22 May 2026.

Harris, Bridget A, 'Technology and Violence Against Women' in Sandra Walklate, Kate Fitz-Gibbon, JaneMaree Maher and Jude McCulloch (eds), *The Emerald Handbook of Feminism, Criminology and Social Change* (Emerald Publishing 2020) 317–336. https://doi.org/10.1108/978-1-78769-955-720201026, accessed 22 May 2026.

Hedlund, Niels, 'The ECHR and the Positive Obligation to Criminalise Domestic Psychological Violence' (2024) 24(3) *Human Rights Law Review*, ngae019. https://doi.org/10.1093/hrlr/ngae019, accessed 22 May 2026.

Lavrysen, Laurens, *Human Rights in a Positive State: Rethinking the Relationship between Positive and Negative Obligations under the European Convention on Human Rights* (Intersentia 2016). https://doi.org/10.1017/9781780685311, accessed 22 May 2026.

Marganski, Alison J and Lisa A Melander, 'Technology-Facilitated Violence against Women and Girls in Public and Private Spheres: Moving from Enemy to Ally' in Jane Bailey, Asher Flynn and Nicola Henry (eds), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Emerald Publishing 2021) 623–641. https://doi.org/10.1108/978-1-83982-848-520211046, accessed 22 May 2026.

McQuigg, Ronagh J A, *Domestic Abuse and the European Court of Human Rights* (Routledge 2024). https://doi.org/10.4324/9781003493068, accessed 22 May 2026.

McQuigg, Ronagh J A, 'The Evolving Jurisprudence of the European Court of Human Rights on Domestic Abuse' in Philipp Czech, Lisa Heschl, Katrin Lukas, Manfred Nowak and Gerd Oberleitner (eds), *European Yearbook on Human Rights 2022* (Intersentia 2022) 205–224. https://doi.org/10.1017/9781839703447.008, accessed 22 May 2026.

McQuigg, Ronagh J A, 'The European Court of Human Rights and Domestic Violence: *Volodina v Russia*' (2021) 10(1) *International Human Rights Law Review* 155–167. https://doi.org/10.1163/22131035-01001002, accessed 22 May 2026.

Powell, Anastasia, 'Technology-Facilitated Abuse: Intimate Partner Violence in Digital Society' in Karen Boyle and Susan Berridge (eds), *The Routledge Companion to Gender, Media and Violence* (Routledge 2023) 337. https://doi.org/10.4324/9781003200871-38, accessed 22 May 2026.

Sinclair-Blakemore, Adaena, 'Cyberviolence Against Women under International Human Rights Law: *Buturugă v Romania* and *Volodina v Russia (No 2)*' (2023) 23(1) *Human Rights Law Review*. https://doi.org/10.1093/hrlr/ngac033, accessed 22 May 2026.

Stark, Evan, *Coercive Control: How Men Entrap Women in Personal Life* (2nd edn, Oxford University Press 2024; online edn, Oxford Academic, 23 November 2023). https://doi.org/10.1093/oso/9780197639986.001.0001, accessed 22 May 2026.

Stark, Evan, 'Rethinking Coercive Control' (2009) 15(12) *Violence Against Women* 1509–1525. https://doi.org/10.1177/1077801209347452, accessed 22 May 2026.

Stonard, Karlie E, 'Technology-Assisted Abuse within Intimate Relationships' in John Devaney, Caroline Bradbury-Jones, Rebecca J Macy, Carolina Øverlien and Stephanie Holt (eds), *The Routledge International Handbook of Domestic Violence and Abuse* (Routledge 2021) 356. https://doi.org/10.4324/9780429331053-27, accessed 22 May 2026.

Stoyanova, Vladislava, ‘Fault, Knowledge and Risk within the Framework of Positive Obligations under the European Convention on Human Rights’ (2020) 33(3) *Leiden Journal of International Law* 601–620. https://doi.org/10.1017/S0922156520000163, accessed 22 May 2026.

Stoyanova, Vladislava, ‘Framing Positive Obligations under the European Convention on Human Rights Law: Mediating between the Abstract and the Concrete’ (2023) 23(3) *Human Rights Law Review* 1–34. https://doi.org/10.1093/hrlr/ngad010, accessed 22 May 2026.

Woodlock, Delanie, Meagan McKenzie, Danielle Western and Bridget Harris, ‘Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control’ (2020) 73(3) *Australian Social Work* 368–380. https://doi.org/10.1080/0312407X.2019.1607510, accessed 22 May 2026.

Woodlock, Delanie, ‘The Abuse of Technology in Domestic Violence and Stalking’ (2017) 23(5) *Violence Against Women* 584–602. https://doi.org/10.1177/1077801216646277, accessed 22 May 2026.

## II. Legal instruments

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (opened for signature 4 November 1950, entered into force 3 September 1953).

Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) (adopted 18 December 1979, entered into force 3 September 1981).

## III. Jurisprudence

*X and Y v Netherlands* (app no 8978/80) 26 March 1985

*Osman v United Kingdom* (app no 87/1997/871/1083) 28 October 1998

*Bevacqua and S v Bulgaria* (app no 71127/01) 12 June 2008

*Opuz v Turkey* (app no 33401/02) 9 June 2009

*Valiulienė v Lithuania* (app no 33234/07) 26 March 2013

*Eremia v Republic of Moldova* (app no 3564/11) 28 May 2013

*Talpis v Italy* (app no 41237/14) 2 March 2017

*Volodina v Russia* (app no 41261/17) 9 July 2019

*Buturugă v Romania* (app no 56867/15) 11 February 2020

*Kurt v Austria* (app no 62903/15) 15 June 2021

*Volodina v Russia (No. 2)* (app no 40419/19) 14 September 2021

*M.Ş.D. v Romania* (app no 28935/21) 3 December 2024

## IV. Official documentation

European Court of Human Rights, *Guide on Article 3 of the European Convention on Human Rights: Prohibition of Torture* (31 August 2025).

European Court of Human Rights, *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence* (31 August 2025).

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), *General Recommendation No 1 on the Digital Dimension of Violence against Women* (GREVIO(2021)20, 20 October 2021). https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147, accessed 22 May 2026.

Van der Wilk, Adriane, 'Protecting Women and Girls from Violence in the Digital Age: The Relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in Addressing Online and Technology-Facilitated Violence against Women' (Council of Europe, December 2021). https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3, accessed 22 May 2026.

UN Broadband Commission for Digital Development Working Group on Broadband and Gender, *Cyber Violence against Women and Girls: A Worldwide Wake-Up Call* (International Telecommunication Union 2015).