Nordic Social Work Research

ISSN: 2156-857X (Print) 2156-8588 (Online) Journal homepage: www.tandfonline.com/journals/rnsw20

Digital technologies and economic abuse in intimate relationships: perceptions of clinical professionals who work with victim-survivors of violence in Finland

Anniina Kaittila, Sonja Tihveräinen, Johanna Hietamäki, Jarno Tuominen, Suvi Nipuli, Annamari Kangas-Kalinen, Leo Nyqvist & Marita Husso

To cite this article: Anniina Kaittila, Sonja Tihveräinen, Johanna Hietamäki, Jarno Tuominen, Suvi Nipuli, Annamari Kangas-Kalinen, Leo Nyqvist & Marita Husso (01 Jun 2026): Digital technologies and economic abuse in intimate relationships: perceptions of clinical professionals who work with victim-survivors of violence in Finland, Nordic Social Work Research, DOI: 10.1080/2156857X.2026.2677880

To link to this article: https://doi.org/10.1080/2156857X.2026.2677880

Published online: 01 Jun 2026.

NORDIC SOCIAL WORK RESEARCH
https://doi.org/10.1080/2156857X.2026.2677880

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Digital technologies and economic abuse in intimate relationships: perceptions of clinical professionals who work with victim-survivors of violence in Finland

Anniina Kaittila [a], Sonja Tihveräinen [b], Johanna Hietamäki [c], Jarno Tuominen [d], Suvi Nipuli [e], Annamari Kangas-Kalinen [a], Leo Nyqvist [a] and Marita Husso [b]

[a]Department of Social Research, University of Turku, Turku, Finland; [b]Faculty of Social Sciences, Tampere University, Tampere, Finland; [c]Finnish Institute for Health and Welfare (THL), Department of Social Sciences, University of Eastern Finland, Kuopio, Finland; [d]Department of Psychology and Speech-Language Pathology, University of Turku, Turku, Finland; [e]Finnish Institute for Health and Welfare (THL), Helsinki, Finland

ABSTRACT

In recent decades, the management of economic affairs has largely transitioned to digital platforms. Electronic identification and online money management have not only simplified individuals' daily lives but have also introduced new methods for financially harming one's partner or ex-partner. This study explores the various types of digitally facilitated economic abuse (DFEA) reported by clinical professionals who work with victim-survivors of violence. The data consist of 102 open-ended survey responses and four focus group interviews conducted with 15 participants. The findings suggest that DFEA can be categorized into two main types: digitally facilitated economic exploitation and digitally facilitated economic control. Digitally facilitated economic exploitation encompasses three distinct forms: The perpetrator (1) steals the victim's money, (2) uses the victim's identity to obtain financial benefits or (3) threatens to inflict financial harm. By contrast, digitally facilitated economic control involves 1) dominating victims of violence by taking control of their finances or 2) surveilling them through digital platforms, such as their online banking or loyalty card accounts. The motivation behind these actions differs from that of economic exploitation; it is not primarily for financial gain but rather a desire for control. Based on the findings of this study, there is a pressing need to critically examine digital practices and platforms to mitigate the potential for abuse. Preventing DFEA requires collaboration among a range of societal actors, including social and healthcare service providers, policymakers, law enforcement, prosecutors and financial and technology institutions.

ARTICLE HISTORY
Received 13 April 2025
Accepted 15 May 2026

KEYWORDS
Economic abuse; technology-facilitated domestic abuse; intimate partner violence; digital technologies

Introduction

In recent decades, the management of economic activities has largely shifted to digital platforms. In many countries, banking transactions are managed through online platforms, and money transfers between individuals are primarily conducted using digital services. Electronic identification is used to apply for benefits, access various official systems, verify identities across different services (including health services) and order a range of products and services for home delivery. However, electronic identification and online money management have not only simplified the

CONTACT Anniina Kaittila anniina.kaittila@utu.fi

daily lives of individuals but have also introduced new methods for financially harming someone, whether they are a close acquaintance or a stranger (Bellini et al. 2023). In this study, we refer to this phenomenon as *digitally facilitated economic abuse* (DFEA; Nyman, Evertsson, and Henrikson 2023) and explore it in the context of intimate partner violence. Particularly, the abuser is typically the victim-survivor's former or current partner.

DFEA combines technology-facilitated domestic abuse (TFDA) with economic abuse (EA). TFDA is a form of abuse in which perpetrators exploit networked technologies and online resources to monitor, harass and control their intimate partners (Afrouz 2023; Woodlock 2017; Ybarra et al. 2017). As a form of intimate partner violence, EA involves behaviours in which an abuser controls a victim-survivor's ability to use, acquire and maintain economic resources (Adams et al. 2020; Postmus et al. 2012).

Research on intimate partner violence has increasingly focused on TFDA and EA, but only a handful of studies have explored DFEA. Significant gaps remain in understanding how digital platforms are used to inflict financial harm on victim-survivors, what forms DFEA may take and what its impacts are on victim-survivors and their families. Consequently, targeted and robust research on the characteristics of DFEA is needed for service systems and legislation to recognize its presence and forms and to improve outcomes for affected individuals.

This study aims to examine and analyse the different manifestations of DFEA reported by clinical professionals working with victim-survivors of violence. Using an inductive analytical approach, the study asks which forms of DFEA professionals encounter in their work. By drawing on the insights of professionals who regularly encounter these cases, we aim to provide a nuanced understanding of how digital technologies are leveraged for economic control and coercion.

Finland provides a particularly relevant context for this study, as it ranks among the leading European countries in online banking usage (Eurostat 2025; Fonseca 2014) while also reporting high rates of intimate partner violence (FRA, Eige and Eurostat 2024; Statistics Finland 2023).

Intersections of economic- and technology-facilitated abuse

EA involves various forms of harm. For example, in The Revised Scale of Economic Abuse SEA2 (Adams et al. 2020), EA has been conceptualized and classified into two overarching categories: economic exploitation and economic control. Economic exploitation includes situations in which an abuser spends existing funds or commits acts that create debt or damage the victim-survivor's credit. Economic control refers to situations in which the abuser has control over the individual's income, spending or bank account. In addition, a third category – employment sabotage – is often included as a distinct form of EA. Employment sabotage refers to behaviours that prevent the victim-survivor from obtaining or maintaining employment (Stylianou, Postmus, and McMahon 2013). EA also frequently continues after divorce (Bruno, Strid, and Ekbrand 2024; Kaittila, Hakovirta and Kainulainen 2024).

Three primary TFDA tactics have been identified: omnipresence, isolation, and punishment and humiliation (Woodlock 2017). Omnipresence refers to the use of digital devices and platforms for constant contact and surveillance, with the intent of making the victim-survivor feel that they lack privacy, safety or security. Isolation occurs when digital technologies are used directly or indirectly to reinforce the victim-survivor's dependence on the abuser, determine how the victim-survivor uses their time and prevent them from seeking help or social support. In this context, punishment and humiliation often involve public shaming and the distribution of intimate or otherwise sensitive material with the intent to defame the victim-survivor among their friends, family and community members (Woodlock 2017).

Although EA and TFDA have distinct characteristics, they intersect in several ways. First, victim-survivors of these forms of violence frequently experience other types of domestic violence as well (Marganski and Melander 2018, Shrap-Jeffs 2016; Temple et al. 2016). Research indicates that both forms, EA and TFDA, are closely associated with coercive control – a type of intimate partner violence in which the abuser aims to control their partner and effectively restrict their autonomy (Dutton and Goodman 2005; Stark 2007). Coercive control is particularly harmful, as it can make the victim-survivor dependent on the abuser (Stylianou 2018) and frequently occurs alongside other forms of intimate partner violence, such as sexual, physical and psychological abuse (e.g. Adams, Beeble, and Gregory 2015; Stylianou 2018).

Second, EA and TFDA have highly negative consequences for the victim-survivors. Intimate partner violence contributes to diminished psychological well-being, leading to anxiety, depression and post-traumatic stress disorder (Harris and Woodlock 2022b; Johnson et al. 2022; Leitão 2021). Furthermore, EA has been linked to economic hardship, including debt and credit damage, and may also result in the victim's financial dependence on the abuser (Johnson et al. 2022). TFDA can lead to social isolation, avoidance of the use of social media and digital devices, and persistent fear and entrapment (Afrouz 2023; Harris and Woodlock 2022b; Leitão 2021).

Third, a characteristic shared by EA (Postmus et al. 2020; Wilson et al. 2024) and TFDA (Harris and Woodlock 2019; Husso et al. 2024) is that both victim-survivors and professionals find it challenging to acknowledge these forms of abuse as constituting violence. This difficulty stems in part from the societal perception that intimate partner violence is predominantly physical (Sharp-Jeffs 2016). Acknowledging EA is particularly challenging due to cultural norms that characterize financial matters as private, which makes it difficult for individuals to discuss these topics openly (Corrie and McGuire 2013). In many cases, considerable time passes before an individual recognizes that what they are experiencing constitutes abuse. Additionally, victim-survivors of EA often find themselves in precarious situations due to debt and a lack of financial resources, which are frequently accompanied by feelings of shame and anxiety. These emotions often prevent victim-survivors from disclosing their circumstances to professionals. Regarding TFDA, research highlights how offline/online dichotomies shape societal perceptions of the severity and consequences of technology-facilitated violence (Dragiewicz et al. 2018; Harris & Woodlock, 2022b; Killean, McAlinden, and Dowds 2022; Piippo et al. 2026). In addition, these concepts are relatively new to society in general and to many victim-survivors themselves.

Fourth, EA and TFDA are frequently reported in studies involving both victim-survivors of abuse and professionals who work with these clients. In an Australian survey of frontline domestic violence practitioners, almost all respondents (99.3%) stated that they worked with clients who had experienced technology-facilitated stalking and abuse (Woodlock, Bentley, et al. 2020b). Similarly, studies conducted with people who seek help for intimate partner violence have revealed that 76%–99% report experiencing EA (Adams et al. 2008, 2015; Postmus et al. 2012; Stylianou, Postmus, and McMahon 2013). TFDA and EA can transcend physical boundaries, enabling abusers to perpetrate intimate partner violence across geographic distances and to continue the abuse after separation, thereby complicating the process of leaving the relationship (Harris and Woodlock 2022a; Stylianou 2018; Stylianou, Postmus, and McMahon 2013).

In summary, as a concept and as a form of abusive behaviour, DFEA is situated within both EA and TFDA. However, it is also analytically distinct from either of them. Whereas EA captures tactics that restrict, exploit or damage a victim-survivor's economic resources, and TFDA captures the use of digital platforms and tools to surveil, harass or coerce, DFEA refers specifically to financial harms that are enabled or substantially amplified by digital financial infrastructures.

Earlier research on digitally facilitated economic abuse

Despite the urgency to better understand, map and address this topic, research into DFEA has been scarce. Three recent publications present findings directly related to DFEA. In Sweden, Nyman, Evertsson, and Henrikson (2023) highlighted how the use of online banking, payment and identification services poses significant risks for victim-survivors of DFEA. The women interviewed revealed that a common form of abuse involves the abuser taking control of the woman's smartphone, thereby restricting her access to money and financial services. Additionally, abusive partners demanded information about the victim-survivors' financial matters, accessed their bank accounts without permission and misused their electronic identification for personal gain. The study noted that Swish was frequently mentioned as a digital platform that abusers exploit to demand money from their partners.

Bellini (2023) recently conducted a study in the United States on how abusers exploit technology-facilitated attacks and deceptive strategies to financially harm victim-survivors. The study data comprised reports from survivors of intimate partner violence and interviews with financial advocates. The methods employed by abusers extended far beyond conventional online banking infrastructure, encompassing employers, benefit providers, online shopping platforms, credit bureaus, investment managers and more. The study identified several distinct types of abusive acts, some of which overlap with those documented by Nyman, Evertsson, and Henrikson (2023).

Beyond exerting control over victim-survivors and seeking financial gain, DFEA perpetrators may engage in deliberate acts of harassment and sabotage. Abusers may make nonconsensual upgrades to subscription tiers to luxury or premium versions – for example, with entertainment services – that cost more money. They may cancel grocery shopping orders or delete digital assets that survivors purchased through subscription sites, including music libraries or digital photo albums. Additionally, in cases in which victim-survivors owned businesses, abusers crafted multiple fake profiles to leave significant amounts of negative feedback, a tactic known as *review bombing*. Some abusers also disseminated the victim-survivor's financial data, such as their authentication details and social security number, on public forums. Bellini's (2023) study indicates that, as with TFDA (Harris and Woodlock 2022b) and EA (Cook et al. 2024), DFEA does not necessarily cease when a relationship ends; it may continue or even escalate after the separation.

Woodlock, Bentley, et al. (2020b) published a report from Australia examining how professionals working with victim-survivors of domestic violence identified manifestations of DFEA. These included monitoring individuals' locations using information provided in online banking applications and restricting women's access to their banking services. The study highlighted that restricting women's access to banking and finances is a common response when a woman attempts to leave an abusive relationship – it exemplifies an act that often forces her to return to her abuser. For example, an abuser may withdraw funds from a joint account, making it impossible for the woman to meet her basic needs.

The vast majority of research on EA (Postmus et al. 2020) and TFDA (Afrouz 2023) has been conducted with women. Therefore, there is a clear need for studies that include victim-survivors of all genders and sexual orientations to better understand the broader dynamics of DFEA.

In summary, previous research has indicated that abusers employ a broad range of tactics and digital platforms to harm their victims. Studies have reported common findings, including actions involving control over online banking or misuse of the victim-survivor's electronic identification information to inflict harm. Each study has contributed unique insights into DFEA. Research has also shown how the prevalence and forms of violence, as well as the possibilities for intervention and help seeking, vary depending on whether a victim-survivor lives in an urban, rural or remote area – geographical dynamics that also shape how technology is used in acts of violence, as captured by the concept of *landscapes of violence* (George and Harris 2014; Harris and Woodlock 2022a). We argue that these landscapes of violence can also be digital. They differ across countries and are shaped by factors such as the degree of public sector digitalization and the availability of communication and online services, including those provided by public authorities, civil society organizations, banking and retail. Furthermore, we argue that these nationally specific digital landscapes influence the forms and manifestations of violence that can occur within them. Our research draws on this premise to examine the specific forms of DFEA enabled by the Finnish digital environment.

Post-digital society and digital financial services in Finland

The context within which Finnish couples and ex-couples navigate their everyday lives can be characterized by the concept of a post-digital society, which describes how digital technologies are deeply integrated into daily life – often invisibly. While the digital transformation era focuses on the adoption and adaptation of digital tools (see Cramer 2015), the post-digital society is characterized by the seamless integration of technology into all facets of human activity, including intimate relationships and financial matters. Feenberg (2019) highlighted how the seamless integration of online and offline worlds and dependence on digital devices, such as mobile phones, make people vulnerable to abuse and exploitation. For instance, electronic identification methods can be easily misused. Consequently, differentiating online actions from their real-world consequences becomes challenging, illustrating the profound influence of the digital realm on daily life (Feenberg 2019).

Financial technologies play a significant role in people's lives globally. According to the World Bank, approximately $1.3 billion in transactions occur daily across 90 countries, with 850 million registered mobile banking and financial services accounts worldwide (Pazarbasioglu et al. 2020). Digital financial services, such as online banking, payment and identification platforms, are easily accessible via smartphones, tablets and computers (Nyman, Evertsson, and Henrikson 2023).

Finland provides a particularly relevant context for studying these services, given that online banking is nearly universal among its adult population and the country consistently ranks among the EU's leaders in digital service adoption. For example, in 2024, 97% of Finnish adults had used online banking services in the three months prior to a study (Eurostat 2025). Mobile payments are also common, as they were used by 60% of the Finnish population in 2024, primarily for payments between friends and family members or online shopping (Bank of Finland 2024). Finland's public sector is at the forefront of digitalization, supported by advanced ICT legislation, strong competition in communication services and comprehensive, high-quality online services (Ali-Yrkkö et al. 2023). As reported by the Finnish government (2024), key public services are already available in digital format, with the aim of further expanding digitalization and automation where appropriate. Citizens also have a high level of trust in digital government systems, as reflected in the exceptionally high level of digital adoption (Ali-Yrkkö et al. 2023). Consequently, Finnish people are broadly accustomed to managing a wide range of everyday needs through digital services (Mielismäki and Husso 2025). For example, the Social Insurance Institution of Finland (Kela) provides basic social security for people living in Finland, and its services are highly digitalized. Nearly all benefits can be applied electronically through OmaKela e-service, the primary customer service channel Kela provides. The benefits cover various life situations, including child benefits, parental allowances, sickness allowances, housing allowances, basic unemployment allowances and social assistance (Kansaneläkelaitos 2025, 2026a). In 2024, 83% of applications were submitted via the OmaKela e-service (Kansaneläkelaitos 2025). In addition to submitting applications, the e-service can be used, for example, to register and change the bank account number to which benefits are paid. Logging into OmaKela is conducted via electronic identification (Kansaneläkelaitos 2026b).

In Finland, electronic identification is a way to verify one's identity online (National Cyber Security Center 2026). Electronic identification is usually done using an identification application on one's mobile phone. The most common method is online banking identification (hereafter referred to as online banking ID), which refers to bank-issued credentials used for strong electronic identification across both banking and other online services. In recent years, 90% of identifications in Finland have been made using online banking IDs (Kemppainen et al. 2023). It requires entering into a contract with a bank and verifying one's identity in person. Another common method is a mobile certificate, which is based on two-factor authentication using the user's PIN code and the phone's SIM card.

Electronic identification is used for numerous public and private online services, including Kela (the Social Insurance Institution of Finland), the Finnish Tax Administration, MyKanta (a digital service used by the social welfare and healthcare sectors for health records and prescriptions), the Police e-service and municipal health services, such as Maisa, as well as online banking services and online stores requiring high-trust authentication. It is also used to digitally sign contracts, such as loans, rental agreements and official documents, and to grant powers of attorney.

Although strong electronic identification is considered a secure way to confirm a person's identity, it remains vulnerable in situations involving violence or coercion. When authentication takes place electronically via mobile phone, the perpetrator can access the victim's electronic identification method by stealing, demanding or coercing the victim into handing over their device (Husso et al. 2024; Nyman, Evertsson, and Henrikson 2023).

Methods

Data

In this study, we combined qualitative data from two research projects to analyse the different types of DFEA. Both studies explored TFDA in Finland. Although DFEA was not the main focus of the research, both datasets included detailed descriptions of how financial issues are linked to TFDA.

The first project, *Digital Violence and Its Intervention in Shelters of Domestic Violence*, was conducted by the Finnish Institute for Health and Welfare (THL). The second, titled DIGNITEAS – *The Challenges of Tackling Digital Violence Against Women in Police Work, Criminal Procedure, and Support Services*, was conducted by the University of Tampere and the Police University College.

The first study (Study 1) aimed to develop a screening tool to identify and address digital violence among victim-survivors in domestic violence shelters.[1] To achieve this objective, the project investigated the prevalence and different forms of digital violence among shelter clients. THL collected data by administering an online survey through Webropol in the summer of 2020, targeting employees from all 29 domestic violence shelters in Finland. The survey was distributed via email to the social workers at the domestic violence shelters and to all individuals working with victim-survivors at these shelters.

The study examined employees' perceptions of the digital violence experienced by their service users, their capacity to support affected victim-survivors and the shelters' operational methods for addressing the issue. The survey asked professionals in detail about the different forms of digital violence they encountered. Each statement was followed by an open-ended response section inviting the respondents to describe their experiences with that form of violence in greater detail. Examples of statements for which open-ended responses included descriptions of DFEA were as follows: 'The client reports that the perpetrator has broken into or otherwise accessed their user accounts (e.g. Gmail, Facebook, WhatsApp, Messenger, Tinder, Zalando and Verkkokauppa.com) or devices against their will'; 'The client reports that the perpetrator has used their online banking ID or other electronic identity verification methods without consent'; and 'Can you think of any other cases of digital violence targeting shelter clients that you would like to share?' The survey received responses from 28 shelters, with 107 shelter employees participating, 106 of whom belonged to the study's target group.

The second study (Study 2) focused on the characteristics and prevalence of digital violence against women and the progression of cases through the criminal justice process. The data were collected through four focus group interviews conducted between 2022 and 2023 with 15 representatives from eight support service facilities. These support centres are non-governmental organizations located in medium-sized to large cities, providing free and accessible services to people who have experienced violence and those close to them. Participants were selected on the basis of their specific knowledge and experience with digital violence, and each participating organization chose its own representatives to take part in the interviews.

All participants work directly with clients, although three also hold managerial responsibilities, and some serve organizations that are national in scope. Three of the four focus group interviews were conducted remotely, while one was held on-site at the support service facility. The duration of the interviews ranged from 59 to 82 minutes, and three researchers involved in the project served as interviewers. All interviewees had years of experience working with victim-survivors of violence in clinical or research settings.

The interviews were semi-structured. The themes of the interviews, provided to the interviewees in advance, were as follows:

(1) The concept of digital violence
(2) Training received on digital violence
(3) Working with cases of digital violence
(4) Recognizing digital violence in their own work
(5) How are criminal justice processes related to digital violence perceived from the perspective of support services and clients?
(6) What are the potential problems with criminal justice processes related to digital violence?
(7) What is needed to increase the capacity to address digital violence now and in the future?
(8) Training needs and capacity building for addressing digital violence

The interviews were recorded and transcribed. After transcription, all recordings were destroyed. The transcripts were not sent to the interviewees for further review.

Exploring information provided by clinical professionals offers an important perspective on the phenomenon of DFEA, as they encounter numerous victim-survivors with diverse experiences. This enables them not only to provide examples of specific situations involving DFEA but also to identify recurring patterns beyond individual cases.

Professionals in the shelters (Study 1) were required to hold a bachelor's degree in social work or healthcare, along with work experience and familiarity with crisis work related to domestic violence (Nipuli & Svetlof 2025). All adult clients using shelter services were systematically screened for the types of violence they had experienced, including economic and digital violence (Finnish Institute for Health and Welfare 2024). The employees who participated in the interview study (Study 2) were also experienced professionals in the field of violence, who were highly familiar with various forms of domestic violence and violence screening tools (Husso et al. 2024).

The Finnish language is gender neutral, which makes it difficult to conclusively determine the gender of the abuse victim-survivors described in the data. However, according to statistics, almost all shelter clients in Finland are women. In 2023, 90% of adult shelter service users were women, while 10% were men (Finnish Institute for Health and Welfare 2024). Most clients in non-targeted support services for violence are also women (see Tuominen et al. 2023). Furthermore, given that Study 2 specifically examined digital violence against women, the clients discussed by the interviewees can reasonably be assumed to have been predominantly women.

Methodologically, this study is situated within secondary qualitative analysis (SDA). SDA refers to research in which data originally collected for a previous study are reanalysed to address new research questions or to apply analytical strategies that were not part of the primary analysis (Ruggiano and Perry 2019; Szabo and Strang 1997). The use of an SDA approach is justified in this study because in both datasets, financial themes emerged prominently as an integral component of broader forms of technology-facilitated violence. Ethically, research participants should be aware of how their data will be used (Ruggiano and Perry 2019); this does not pose a concern in the present study, as both original projects focused on technology-facilitated violence. This study builds on that foundation by refining the analytical focus to examine more specifically how violence is enacted through monetary and financial means.

Analysis

The data were analysed using inductive thematic analysis, as described by Braun and Clarke (2006). This method was chosen for its flexibility and systematic approach to qualitative analysis, as well as its demonstrated suitability for studies aiming to conceptualize forms of violence (Kaittila, Hakovirta, and Kainulainen 2024). In inductive thematic analysis (Braun and Clarke 2006), preliminary themes are extracted from the data, and no pre-existing coding framework is used. The analysis follows six phases: data familiarization, initial coding, theme identification, theme review, theme definition and reporting.

In the initial stage of analysis, AK and ST read both the open-ended survey responses (Study 1) and the focus group interview data (Study 2). For the purposes of this analysis, DFEA is defined as abuse in which the perpetrator uses digital financial services or devices to limit the victim-survivor's access to money, monitor and control their use of money or economically exploit them (see Nyman, Evertsson, and Henrikson 2023). Using this definition, the researchers identified all descriptions – across both datasets – that contained information about DFEA in intimate relationships. All excerpts that met this definition were included. AK and ST independently reviewed the material, compared interpretations and reached consensus on which descriptions to include.

In Study 1, 102 text excerpts described DFEA and were thus included in the analysis. In Study 2, descriptions of DFEA were found across all four interviews. The textual excerpts from both datasets ranged from single sentences to detailed paragraphs that captured the experiences shared by the clients. Despite differences in format, the themes that emerged from the two datasets were largely similar. While the survey responses were more numerous but shorter and less contextualized, the focus group data offered richer, more detailed accounts of the processes underlying the abusive acts.

In the second stage, AK and ST conducted line-by-line coding of all text descriptions using an open-coding technique. The open-ended survey responses and interview data were qualitatively coded using the same analytical criteria. During this stage, the researchers explicitly considered how the research question – 'What forms of DFEA do professionals encounter in their work?' – guided the coding. The codes captured concrete abusive acts, and in relation to these acts, the data also included descriptions of their impacts on victim-survivors, the digital tools used and the processes through which the abusive actions were carried out.

In the third stage, the researchers deliberated over the codes and finalized their names. The codes were categorized into subthemes and grouped into main themes, forming an analytical framework. The decision to dichotomize DFEA into two overarching categories was made at this point. This structure emerged inductively from the data; the codes clustered clearly into (1) controlling/restrictive practices and (2) exploitative practices. This categorization has also been widely applied in studies concerning EA more broadly. Other possible groupings – such as categorizing DFEA based on the digital tools involved, as applied in Nyman, Evertsson, and Henrikson (2023)—were considered but ultimately rejected because they did not align as closely with how professionals described the abusive dynamics. In the fourth stage, the framework was discussed during two research group meetings that included the authors of this study. It was subsequently refined and approved by the research group.

The participants from both studies were informed about the study's goals, their rights and the confidentiality and protection of their data. The ethicality of the research was secured by ensuring that none of the respondents' personal information or descriptions of their clients' situations were identifiable. Data excerpts were used to illustrate the analysis. Quotes from Study 1 were marked by study number and participant number (e.g. S1P2), while quotes from Study 2 were marked by study number, interview number and participant number (e.g. S2I1P3).

Ethics

The Ethics Committee of the Tampere Region granted ethical approval for Study 2 in June 2022. The necessary research permits were obtained from support service organizations. The participants in the focus group interviews were informed in advance of the study's implementation, the voluntary nature of their participation and the confidentiality of their information. They were asked to provide their written informed consent to participate in the interviews, to be recorded and to have the resultant materials used for research purposes and archived for further use. The informants were guaranteed full anonymity throughout the study. In addition, it was made clear to them that they could withdraw their consent during the study without any consequences.

The respondents in Study 1 (online survey) were informed about the survey, the voluntary nature of their participation and the confidentiality of their information via email. The responses were anonymous, and the online questionnaire required the respondents' consent to participate in the survey. As noted above, ethical approval was not required for Study 1, as its research design did not meet the criteria for ethical review under the Finnish National Board on Research Integrity.

Because the participants shared information about their clients' experiences of violence, special care was taken to prevent the indirect identification of both the professionals and the clients they described.

Results

The analysis revealed that clinical professionals encounter a range of distinct DFEA forms in their work with victim-survivors of intimate partner violence. The professionals' descriptions consistently illustrate how digital financial tools and identification methods are used to harm, restrict or exploit victim-survivors.

Based on the inductive analysis, these acts were clustered into two overarching categories (Table 1). The first category, *digitally facilitated economic exploitation*, encompasses acts in which the abuser gains financial benefits through digital means. The second, *digitally facilitated economic control*, refers to acts in which digital tools are used to limit, monitor or take over the victim-survivor's financial autonomy.

Digitally facilitated economic exploitation

The first theme, digitally facilitated economic exploitation, encompasses three distinct forms: The abuser (1) steals the victim-survivor's money, (2) uses the victim-survivor's identity to obtain financial benefits or (3) threatens to cause financial harm. The respondents described instances in which the abuser used the victim-survivor's online banking services to transfer money to their own account or to a third-party account. In some cases, the couple shared a joint account from which the abuser transferred money for personal use without mutual agreement. The respondents reported situations in which all accounts and devices were shared between the partners, allowing the abuser to use shared funds or their partner's funds for personal purposes:

> 'The abuser uses the client's bank account as if it were their own, transferring funds to their personal account' (S1P25).

A similar example was reported:

Table 1. Digitally facilitated economic exploitation and digitally facilitated economic control.

Digitally Facilitated Economic Exploitation	Digitally Facilitated Economic Control
• Digital theft • Identity misuse • Threatening to cause financial harm using digital technology	• Taking control of finances • Monitoring monetary matters

> There have been situations in which the abuser has gained access to the victims online banking ID, forcing the victim to close the account and open another. The abuser may also have transferred all the money from the victim's account. (S1P50)

In addition to online banking services, abusers reportedly exploited other platforms to access victim-survivors' money. For example, there were cases in which the abuser accessed the victim-survivor's mobile phone and used the MobilePay[2] app to transfer money from the victim-survivor's account to their own.

Identity misuse, in which an abuser uses a victim-survivor's personal information to obtain financial benefits, was another commonly reported form of exploitation. For instance, abusers may order products from online retailers using the individual's electronic identification or credit card information. In some cases, they placed orders in the victim-survivor's name and left the bills unpaid. Abusers also used victim-survivors' electronic identification information to apply for welfare benefits, such as childcare allowances, in the individuals' names and later transferred the funds from the victim-survivors' account to their own. Abusers may also designate their own bank account number on the application, resulting in welfare benefits granted to the victim-survivors being paid to the abusers. In Finland, financial benefits are primarily claimed and administered electronically, which facilitates this type of abuse:

> 'Occasionally, a violent spouse applies for benefits from, for example, the Social Insurance Institution of Finland on the client's behalf and keeps the money' (S1P104).

In cases of identity misuse, the consequences of the abuse may affect the victim-survivor years after the relationship has ended. The respondents revealed that financial exploitation can begin during the relationship or continue, and even escalate, after separation, with lasting consequences for the victim-survivor's financial situation. The participants noted instances in which the abuser had financially exploited the victim-survivor behind their back during the relationship, with the truth coming to light only after the relationship ended.

> Debts have been taken on and vehicles bought in the client's name without telling them. After the divorce, the victim has to deal with the debt and expenses from the Transport and Communications Agency until the situation is handled with the authorities. (S1P26)

> Yesterday, I met a client who said it had been three years since she reported the offence of stealing personal information – that her ex-partner had used their personal identity code to take out all kinds of loans and so forth – and that she had reported it. (S2I4P1)

The data also included descriptions of victim-survivors being subjected to coerced debt. The abuser had taken out payday loans[3] or applied for loans on the victim-survivor's behalf using the latter's electronic identification details. Typically, the individuals were unaware that the abuser had committed these acts. Alternatively, in some cases, the individual was pressured to apply for consumer credit, even though the money was intended to go to the abuser:

> 'The abuser has used the client's bank account entirely for their own purposes, taking out payday or instant loans using the client's online banking ID' (S1P68).

The respondents noted that, in addition to causing financial harm to the victim-survivor, abusers also used digital devices to threaten further financial damage. For example, one individual who had checked into a domestic violence shelter was harassed by the abuser through text messages, emails, phone calls and other means, while the abuser simultaneously destroyed the possessions the victim-survivor had left in their home.

Digitally facilitated economic control

The second theme encompasses two forms of digitally facilitated economic control: 1) taking control of the victim-survivor's finances and 2) monitoring them through digital platforms.

Unlike the earlier category, in which the motivation was financial gain, these actions were driven by a desire to dominate and restrict the victim-survivor's autonomy. The professionals described situations in which the abuser took control of the victim-survivor's finances by taking charge of the individual's bank account or seizing their credit or debit card. In some cases, the victim-survivor was unaware that the abuser had obtained their electronic identification details, while in other instances, the abuser explicitly demanded that the victim-survivor provide this information.

Demanding the victim-survivor's electronic identification details was the most frequently mentioned form of DFEA. In some cases, victim-survivors had access to their own bank accounts, although the abuser monitored the flow of money in and out. However, there were also situations in which the abuser took control of all the victim-survivor's financial affairs, leaving the individual without access to or information about their own funds. In the most extreme cases, victim-survivors – typically women from immigrant backgrounds – were unaware that electronic identification existed, leaving the abuser free to exploit it without their knowledge.

> Sometimes, there are situations in which the client has intentionally not been provided with training and guidance on how to use their online banking ID or any other digital services. So, there may be situations in which all digital activities have been in the wrong hands. (S1P13)

> Regardless of skills and IT skills and digital skills, the language barrier still has an impact. Take, for example, errands for the Social Insurance Institution—to fill out documents only in Finnish. Even if you speak English. I had those clients. They can't fill out information in Finnish because everything is in Finnish when you open the webpage. That's why abusers often manage these things on behalf of the client. (S2I3P1)

The respondents reported that electronic identification enables abusers not only to monitor and control the victim-survivor's financial status but also to access a range of personal accounts and sensitive information.

> The abuser has gained access to the victim's online banking ID and used it to access, for example, the client's Kanta health services.[4] And [the abuser] monitors what health services the client uses and what they discuss. (S1P106)

In this case, electronic identification enabled abusers to access private and sensitive information, which can lead to increased violence and endanger the safety of the victim-survivor.

The respondents also mentioned how digital platforms and devices allow abusers to track victim-survivors' whereabouts. For example, if an abuser has access to the individual's online banking services or loyalty card usage data, they can determine the victim-survivor's location by monitoring their transactions. Another significant challenge is the fraudulent use of victim-survivors' electronic identification details to assume power of attorney, enabling the abuser to act on the victim-survivor's behalf without their knowledge or consent. As the following example illustrates, digital environments enable an abuser to monitor the victim-survivor, even if one has sought help and attended a shelter.

> And then also just using digital services on behalf of the client – that, for example, in OmaKela, and other such [services]. Digitally, the health centres, Maisa[5] and others, they pose a somewhat large problem. Then, there's power of attorney to all of those, and the abuser can use it, for example, to gain information about the client while they're at a violence shelter – that, okay, now there's a scheduled appointment somewhere, and that they've seen a doctor to discuss the violence experienced. And that may show up in Maisa, and that's really so . . . a really abhorrent situation. (S1I3P2)

Discussion

This study presents qualitative findings on the types of DFEA that emerge within intimate relationships. These types were reported by clinical professionals who worked with victim-survivors of violence. According to these professionals, DFEA is a common form of violence characterized by various acts. Complementing earlier research on post-digital societies, this study demonstrates that digital technologies have become an integrated part of people's everyday lives (Cramer 2015). In the context of DFEA, these technologies provide platforms and practices that can be used to inflict harm. Financial technologies and electronic identification methods, in particular, create platforms for controlling and inflicting serious harm on victim-survivors (see also Bellini 2023; Nyman, Evertsson, and Henrikson 2023). These tools allow abusers to cultivate a sense of omnipotence and omnipresence, making victim-survivors feel that they can be monitored or harmed at any time and from any location (Woodlock 2017).

The findings of this study suggest that DFEA can be divided into two main categories: digitally facilitated economic exploitation and digitally facilitated economic control. According to recent studies, exploitation and restrictions on financial access are the most common forms of non-digital EA (see Adams et al. 2023). This suggests that the underlying dynamics of digital and non-digital EA are similar, even as the platforms and tools through which abuse is perpetrated differ. This study did not explicitly explore intimate partner violence as a manifestation of violence against women, and it did not specify the gender of the victim-survivors in the respondents' descriptions. However, the data and examples strongly suggest violence in which the victim-survivor is a woman. This is further evidenced by the fact that, at shelters in Finland – where most of the data were collected— 90% of adult clients are women (Finnish Institute for Health and Welfare 2024). Therefore, the results of this study support the observation that women are at particular risk for DFEA (see also Woodlock, Bentley, et al. 2020b).

The findings illustrate three distinct forms of digitally facilitated economic exploitation: stealing the victim-survivor's money, misusing their identity for financial gain and threatening to cause financial harm. The results portray instances in which the abuser exploits the victim-survivor's online banking services, such as mobile banking or money transfer applications, to access the individual's funds without their consent. Earlier studies of EA (see Cook et al. 2024; Kaittila, Hakovirta and Kainulainen 2024) indicate that there are instances in which the abuser may exploit societal services or benefit systems as part of their exploitative behaviour. The present study illustrates how the digitalization of services and benefits facilitates this type of abuse. Abusers can apply for welfare benefits, such as childcare allowances, in the victim-survivor's name online and misuse the funds for their own purposes, as these benefits are primarily administered electronically. Rectifying these situations can be particularly challenging for individuals, especially if they are not native Finnish speakers, since advisory services are predominantly conducted online, primarily in Finnish, and in-person guidance has significantly decreased (Pennanen et al. 2023). Identity misuse further extended to taking out loans or ordering goods in the victim-survivor's name, acts typically enabled by access to the victim-survivor's electronic identification details.

Digitally facilitated economic control refers to situations in which the abuser monitors and controls the victim-survivor's finances through digital platforms. Controlling another's finances is a traditional form of abuse. In the past, victim-survivors of violence were forced to collect receipts for all transactions; now, digital technologies enable abusers to monitor their partners in real time by using stolen electronic identification details or by coercing their partners into granting access to their online banking accounts or loyalty card data. As Nyman, Evertsson, and Henrikson (2023) argued, digital financial services limit opportunities for victim-survivors to hide or destroy financial information they want to keep private. The results of the present study indicate that, in addition to financial information, electronic identification details may grant access to information that extends well beyond financial matters, including access to individuals' health information. Therefore, electronic identification poses a significant threat to the safety and privacy of victim-survivors.

This study responds to the documented need to conceptualize and further develop a theoretical understanding of EA within intimate relationships (Postmus et al. 2020). To theorize DFEA as a phenomenon, our findings indicate that it is necessary to integrate two strands of scholarship—(1) economic abuse theory (see Postmus et al. 2020) and measurement (Adams et al. 2020), which conceptualize the economic domain of intimate partner violence IPV through control and exploitation – and (2) technology-facilitated coercive control (Dragiewicz et al. 2018; Woodlock 2017), which explains how networked technologies amplify omnipresence and omnipotence, enabling perpetrators to be *everywhere*, to surveil and to project power beyond physical proximity. In our data, electronic identification systems, online banking and connected devices extend routine financial control and economic exploitation into spaceless yet persistent patterns of domination. Thus, DFEA is best understood not as a new logic of abuse but as an intensification and institutionalization of economic control and exploitation through digital systems.

In summary, while classifying EA by the acts themselves remains analytically valuable, our results underscore that forms of violence overlap and interlock, and their interpretation requires shared conceptual frameworks that connect economic control and exploitation to coercive control and its technology-facilitated affordances. This integrated perspective helps explain DFEA's entanglement with other IPV modalities and its embeddedness in financial and institutional systems, thereby advancing theoretical understanding of how economic domination is maintained and magnified in post-digital societies.

In recent years, the phenomenon of DFEA has garnered academic attention (Bellini et al. 2023; Nyman, Evertsson, and Henrikson 2023). Studies conducted in various countries have identified common patterns, indicating that perpetrators of DFEA exploit, monitor, restrict and sabotage their victim-survivors' financial well-being using digital tools. However, each study has revealed new dimensions of the phenomenon. These studies clearly demonstrate how societal practices and platforms facilitate such abuse, underscoring the ongoing need to explore the observed forms of DFEA and their consequences across different societal contexts.

This study has some acknowledged limitations. First, the data were not specifically centred on DFEA; they emerged as a secondary theme described by the participating professionals in their responses to the questionnaire and during the interviews. Therefore, a dedicated study designed specifically around DFEA is needed to develop a more comprehensive understanding of this form of abuse. Another issue with the data is the limited sample. Clinical professionals who work with victim-survivors of violence provided their perspectives on DFEA. By exploring the experiences of other professionals, such as police officers or financial counsellors, a different understanding of the types of DFEA can be reached. Exploring this phenomenon from a multiprofessional perspective would provide new insights for understanding this type of violence (Notko et al. 2022).

Implications

The results of this study contribute to the recognition and understanding of various types of DFEA. They also provide insights into how current digital systems and practices may inadvertently facilitate DFEA. This study strongly supports an observation made by Nyman, Evertsson, and Henrikson (2023) that digital financial services are predicated on the implicit assumption that threats to financial security originate from outside the family. Consequently, a critical re-examination of digital practices and platforms is necessary to address the structural vulnerabilities that enable DFEA.

This study highlights the significance of promoting awareness of the various forms of DFEA. In turn, this could encourage discussions of the experiences of victim-survivors and the reduction of the stigma associated with these experiences. Communication efforts should be directed at two distinct groups: the general public and professionals who may encounter victim-survivors of DFEA. Awareness is the first step towards obtaining help or developing effective support practices. In addition, tools and processes should be developed for services through which social, health and legislative professionals encounter victim-survivors, as well as for financial and technological institutions.

In addition to identification and intervention, the prevention of DFEA should be a key focus. This requires promoting cooperation between different actors in society, such as policymakers; social and health service providers; law enforcement personnel, such as police and prosecutors; and financial and technological institutions. Identifying the factors that enable DFEA at the national level is essential for determining the actions needed to eliminate such behaviour.

High-quality material on this objective is already available – for instance, from the Safety Net Project (National Network to End Domestic Violence n.d.), which supports the fight against DFEA in various sectors. Similar material should be developed in other countries, tailored to their respective national contexts, legislation and relevant stakeholders. Practical applications could include developing screening tools for social and healthcare professionals and bank employees to help them recognize DFEA, as well as developing training modules that explain what DFEA is, how to screen for it and how to support and advise clients experiencing DFEA within the boundaries of the professional's own role.

Notes

1. THL is responsible for the guidance, assessment, development, and national coordination of domestic violence shelters in Finland. These services are regulated by the Shelters Act (30.12.2014/1354), which defines a shelter as a 24/7 crisis work unit that providing secure housing, psychosocial support, counselling, and guidance to anyone who has experienced or is threatened by domestic violence, regardless of age or gender.
2. MobilePay is a mobile payment application used in Finland. The service allows payments by means of a smartphone application.
3. A payday loan is a short-term unsecured loan, often characterized by high interest rates.
4. The Kanta Services are a set of digital services that store citizens' social welfare and health care data.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The work was supported by the Ministry of Social Affairs and Health (Finland).

ORCID

Anniina Kaittila http://orcid.org/0000-0001-8322-3688
Sonja Tihveräinen http://orcid.org/0000-0002-2796-9562
Johanna Hietamäki http://orcid.org/0000-0002-0387-223X
Jarno Tuominen http://orcid.org/0000-0002-3892-3199
Marita Husso http://orcid.org/0000-0002-3714-8477

References

Adams, A. E., M. L. Beeble, A. Biswas, R. L. Flynn, and L. Vollinger. 2023. "An Exploratory Study of Financial Health as an Antecedent of Economic Abuse Among Women Seeking Help for Intimate Partner Violence." *Violence Against Women* 30 (15–16): 3825–3853. https://doi.org/10.1177/10778012231170867

Adams, A. E., M. L. Beeble, and K. A. Gregory. 2015. "Evidence of the Construct Validity of the Scale of Economic Abuse." *Violence & Victims* 30 (3): 363–376. https://doi.org/10.1891/0886-6708.VV-D-13-00133

Adams, A. E., M. R. Greeson, A. K. Littwin, and M. Javorka. 2020. "The Revised Scale of Economic Abuse (SEA2): Development and Initial Psychometric Testing of an Updated Measure of Economic Abuse in Intimate Relationships." *Psychology of Violence* 10 (3): 268–278. https://doi.org/10.1037/vio0000244

Adams, A. E., C. M. Sullivan, D. Bybee, and M. R. Greeson. 2008. "Development of the Scale of Economic Abuse." *Violence Against Women* 14 (5): 563–588. https://doi.org/10.1177/1077801208315529

Afrouz, R. 2023. "The Nature, Patterns and Consequences of Technology-Facilitated Domestic Abuse: A Scoping Review." *Trauma, Violence & Abuse* 24 (2): 913–927. https://doi.org/10.1177/15248380211046752

Ali-Yrkkö, J., O. Kässi, M. Pajarinen, and P. Rouvinen. 2023. *Digibarometer 2023: Data, AI, and Economic Growth. Digibarometri 2023*. Helsinki: Taloustieto Oy.

Bank of Finland. 2024. *Consumer Survey on Payment Methods and Cash*. Helsinki: Bank of Finland. https://www.suomenpankki.fi/en/statistics/dashboards-and-open-data/cash-statistics/kuluttajakysely/?epslanguage=en.

Bellini, R. 2023. "Paying the Price: When Intimate Partners Use Technology for Financial Harm." Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23). Association for Computing Machinery, Hamburg, Vol. 872, 1–17. https://doi.org/10.1145/3544548.3581101

Bellini, R., K. Lee, M. A. Brown, J. Shaffer, R. Bhalerao, and T. Ristenpart. 2023. *The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence. USENIX Security Symposium*, 87–104. Anaheim, CA: USENIX Association. https://www.usenix.org/conference/usenixsecurity23/presentation/bellini. (USENIX Security 23.

Braun, V., and V. Clarke. 2006. "Using Thematic Analysis in Psychology." *Qualitative Research in Psychology* 3 (2): 77–101. https://doi.org/10.1191/1478088706qp063oa

Bruno, L., S. Strid, and H. Ekbrand. 2024. "Men's Economic Abuse Toward Women in Sweden: Findings from a National Survey." *Violence Against Women* 31 (9): 2194–2218. https://doi.org/10.1177/10778012241257248

Cook, K., A. Byrt, T. Edwards, and R. Burgin. 2024. "Postseparation Financial Abuse Perpetrated Through Government Systems: A Survey of Australian Mothers' Experiences of Child Support." *Violence Against Women* 31 (12–13): 3355–3379. https://doi.org/10.1177/10778012241280057

Corrie, T., and M. McGuire. 2013. Economic Abuse: Searching for Solutions. Good Shepherd Youth & Family Services and Kildonan UnitingCare. https://goodshep.org.au/wp-content/uploads/2020/12/economic-abuse_final-report.pdf.

Cramer, F. 2015. "What Is 'Post-digital'?" In *Postdigital Aesthetics*, edited by D. M. Berry and M. Dieter, 12–26. London: Palgrave Macmillan. https://doi.org/10.1057/9781137437204_2

Dragiewicz, M., J. Burgess, A. Matamoros-Fernandez, M. Salter, N. P. Suzor, D. Woodlock, and B. Harris. 2018. "Technology-Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms." *Feminist Media Studies* 18 (4): 609–625. https://doi.org/10.1080/14680777.2018.1447341

Dutton, M. A., and L. A. Goodman. 2005. "Coercion in Intimate Partner Violence: Toward a New Conceptualization." *Sex Roles* 52 (11–12): 743–756. https://doi.org/10.1007/s11199-005-4196-6

Eige, F. R. A., and Eurostat. 2024. *EU Gender-Based Violence Survey – Key Results. Experiences of Women in the EU-27*. Luxembourg: Publications Office of the European Union. https://ec.europa.eu/eurostat/documents/7870049/20464303/KS-01-24-013-EN-N.pdf/052adbe2-40bd-9472-87c0-ed14c7106bfa?version=1.0&t=1732193841491.

Eurostat. 2025. "Digitalisation in Europe – 2025 Edition." https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025.

Feenberg, A. 2019. "Postdigital or Predigital?" *Postdigital Science & Education* 1 (1): 8–9. https://doi.org/10.1007/s42438-018-0027-2

Finnish Government. 2024. "Finland's National Roadmap: EU Digital Decade Policy Programme 2030 (Publication of the Finnish Government 2024:7). https://urn.fi/URN:ISBN:978-952-383-743-0.

Finnish Institute for Health and Welfare. 2024. Shelters for Victims of Domestic Violence 2023. Statistical Report 33. https://urn.fi/URN:NBN:fi-fe2024060343438.

Fonseca, J. R. S. 2014. "e-Banking Culture: A Comparison of EU 27 Countries and Portuguese Case in the EU 27 Retail Banking Context." *Journal of Retailing & Consumer Services* 21 (5): 708–716. https://doi.org/10.1016/j.jretconser.2014.05.006

George, A., and B. Harris. 2014. *Landscapes of Violence: Women Surviving Family Violence in Regional and Rural Victoria*. Geelong, VIC: Deakin University. https://eprints.qut.edu.au/104420/.

Harris, B. A., and D. Woodlock. 2019. "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies." *The British Journal of Criminology* 59 (3): 530–550. https://doi.org/10.1093/bjc/azy052

Harris, B., and D. Woodlock. 2022a. "Spaceless Violence: Women's Experiences of Technology-Facilitated Domestic Violence in Regional, Rural and Remote Areas." *Trends & Issues in Crime and Criminal Justice*: 644. https://doi.org/10.52922/ti78405

Harris, B., and D. Woodlock. 2022b. "'You Can't Actually Escape It': Policing the Use of Technology in Domestic Violence in Rural Australia." *International Journal for Crime, Justice and Social Democracy* 11 (1): 135–148. https://doi.org/10.5204/ijcjsd.2190

Husso, M., S. Piippo, J. Houtsonen, M. Mela, S. Tihveräinen, J. Haapanen, L. Hakkarainen, and A. Knihtilä. 2024. "Naisiin kohdistuvaan digitaaliseen väkivaltaan puuttumisen haasteet poliisin työssä, rikosprosessissa ja tukipalveluissa. [Challenges of Tackling Digital Violence Against Women in Police Work, Criminal Procedure, and Support Services]." In Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja [Publication Series of the Government's Analysis, Assessment and Research Activities]. Helsinki: Valtioneuvoston kanslia [Prime Minister's Office]. 65. https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/c0f6513f-68f2-469d-8b55-97b021810784/content.

Johnson, L., Y. Chen, A. Stylianou, and A. Arnold. 2022. "Examining the Impact of Economic Abuse on Survivors of Intimate Partner Violence: A Scoping Review." *BMC Public Health* 22 (1): 1014. https://doi.org/10.1186/s12889-022-13297-4

Kaittila, A., M. Hakovirta, and H. Kainulainen. 2024. “Types of Economic Abuse in Postseparation Lives of Women Experiencing IPV: A Qualitative Study from Finland.” *Violence Against Women* 30 (2): 426–444.
Kansaneläkelaitos. 2025. *Toimintakertomus Ja Tilinpäätös: Vuosi 2024 [Operating Report and Financial Statements: Year 2024]*. Social Insurance Institution of Finland (Kela). https://www.kela.fi/documents/d/guest/kela-toimintakertomus-2024.
Kansaneläkelaitos. 2026a. “Benefits Available from Kela.” https://www.kela.fi/benefits-available-from-kela .
Kansaneläkelaitos. 2026b. “Omakela E-Service.” https://www.kela.fi/e-services.
Kemppainen, L., T. Kemppainen, A. Kouvonen, Y.-K. Shin, E. Lilja, T. Vehko, and H. Kuusio. 2023. “Electronic Identification (E-ID) as a Socio-Technical System Moderating Migrants’ Access to Essential Public Services – the Case of Finland.” *Government Information Quarterly* 40 (4), Article 101839. 101839. https://doi.org/10.1016/j.giq.2023.101839
Killean, R., A.-M. McAlinden, and E. Dowds. 2022. “Sexual Violence in the Digital Age: Replicating and Augmenting Harm, Victimhood and Blame.” *Social & Legal Studies* 31 (6): 871–892. https://doi.org/10.1177/09646639221086592
Leitão, R. 2021. “Technology-Facilitated Intimate Partner Abuse: A Qualitative Analysis of Data from Online Domestic Abuse Forums.” *Human–Computer Interaction* 36 (3): 203–242. https://doi.org/10.1080/07370024.2019.1685883
Marganski, A., and L. Melander. 2018. “Intimate Partner Violence Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experiences and Its Association with In-Person Dating Violence.” *Journal of Interpersonal Violence* 33 (7): 1071–1095. https://doi.org/10.1177/0886260515614283
Mielismäki, H., and M. Husso. 2025. *Ethical Implications of AI-Driven Chatbots in Domestic Violence Support*. Vol. 13. Social Inclusion, Cogitatio Press. https://doi.org/10.17645/si.9998
National Cyber Security Center. 2026. “Electronic Identification.” https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification.
National Network to End Domestic Violence. n.d.. “Safety Net Project.” https://www.techsafety.org/financial-abuse-and-technology.
Notko, M., M. Husso, S. Piippo, M. Fagerlund, and J. Houtsonen. 2022. “Intervening in Domestic Violence: Interprofessional Collaboration Among Social and Health Care Professionals and the Police.” *Journal of Interprofessional Care* 36 (1): 15–23. https://doi.org/10.1080/13561820.2021.1876645.
Nyman, C., L. Evertsson, and A.-S. Henrikson. 2023. “Digitally Facilitated Economic Abuse in the Age of Digital Financial Services – New Risks for Economic Abuse in Intimate Partner Violence.” *Journal of Gender-Based Violence* 7 (3): 368–382. https://doi.org/10.1332/239868023X16909576356057
Pazarbasioglu, C., A. Garcia Mora, M. Uttamchandani, H. Natarajan, E. Feyen, and M. Saal. 2020. “Digital Financial Services (White Paper).” World Bank Group. https://thedocs.worldbank.org/en/doc/305a39cbb6f35567db78bda6709c5cd8-0430012025/original/World-Bank-DFS-Whitepaper-DigitalFinancialServices.pdf.
Pennanen, P., M. Jansson, P. Torkki, M. Harjumaa, I. Pajari, E. Laukka, S. Lakoma, et al. 2023. *Digitaalisten Palvelujen Vaikutukset Sosiaali- Ja Terveydenhuollossa* [Impacts of Digital Services in Social and Health Care]. (Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2023:52). Valtioneuvoston kanslia. https://urn.fi/URN:ISBN:978-952-383-059-2.
Piippo, S., M. Mela, J. Houtsonen, S. Tihverainen, and M. Husso. 2026. “Technology-Facilitated Violence and Gender-Based Harm: Investigative Challenges from the Perspective of the Police, Prosecutors, and Support Services in Finland.” In *New Perspectives on Global Gender-Based Violence. Critical Criminological Perspectives*, edited by A. Wilcock and H. Williams. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-032-13210-9_3.
Postmus, J. L., G. L. Hoge, J. Breckenridge, N. Sharp-Jeffs, and D. Chung. 2020. “Economic Abuse as an Invisible Form of Domestic Violence: A Multicountry Review.” *Trauma, Violence & Abuse* 21 (2): 261–283. https://doi.org/10.1177/1524838018764160
Postmus, J. L., S. B. Plummer, S. McMahon, N. S. Murshid, and M. S. Kim. 2012. “Understanding Economic Abuse in the Lives of Survivors.” *Journal of Interpersonal Violence* 27 (3): 411–430. https://doi.org/10.1177/0886260511421669
Ruggiano, N., and T. E. Perry. 2019. “Conducting Secondary Analysis of Qualitative Data: Should We, Can We, and How?” *Qualitative Social Work* 18 (1): 81–97. https://doi.org/10.1177/1473325017700701
Sharp-Jeffs, N. 2016. *Supporting Survivors of Financial Abuse: Learning for the UK*. London: London Metropolitan University. https://survivingeconomicabuse.org/wp-content/uploads/2021/04/Sharp-Supporting-Survivors-of-EA-2017.pdf.
Shelters Act. 1354/2014. (Fin.).
Stark, E. 2007. *Coercive Control: The Entrapment of Women in Personal Life*. New York: Oxford University Press.
Statistics Finland. 2023. Sukupuolistunut Väkivalta Ja Lähisuhdeväkivalta Suomessa [Gendered and domestic violence in Finland]. Tilastokeskus. https://urn.fi/URN:ISBN:978-952-244-717-3.
Stylianou, A. M. 2018. “Economic Abuse within Intimate Partner Violence: A Review of the Literature.” *Violence & Victims* 33 (1): 3–22. https://doi.org/10.1891/0886-6708.33.1.3

Stylianou, A. M., J. L. Postmus, and S. McMahon. 2013. “Measuring Abusive Behaviors: Is Economic Abuse a Unique Form of Abuse?” *Journal of Interpersonal Violence* 28 (16): 3186–3204. https://doi.org/10.1177/0886260513496904

Szabo, V., and V. R. Strang. 1997. “Secondary Analysis of Qualitative Data.” *Advances in Nursing Science* 20 (20(2): 66–74. https://doi.org/10.1097/00012272-199712000-00008

Temple, J. R., H. J. Choi, M. Brem, C. Wolford-Clevenger, G. L. Stuart, M. Fleschler Peskin, and J. Elmquist. 2016. “The Temporal Association Between Traditional and Cyber Dating Abuse Among Adolescents.” *Journal of Youth & Adolescence* 45 (2): 340–349. https://doi.org/10.1007/s10964-015-0380-3

Tuominen, J., A. Kaittila, V. Halme, J. Hietamäki, M. Hakovirta, and H. Olkoniemi. 2023. “Changes in Frequency and Form of Domestic Violence in Calls to Violence Helpline During COVID-19 in Finland.” *Psychology of Violence* 13 (6): 447–455. https://doi.org/10.1037/vio0000474.

Wilson, B., S. Zawitkowski, S. Weiss, L. Docherty, and P. C. Barata. 2024. “How the Invisible Becomes Visible: The Lived Experience of Economic Abuse in Heterosexual Relationships.” *Violence Against Women* 30 (15–16): 3799–3824. https://doi.org/10.1177/10778012231185540

Woodlock, D. 2017. “The Abuse of Technology in Domestic Violence and Stalking.” *Violence Against Women* 23 (5): 584–602. https://doi.org/10.1177/1077801216646277

Woodlock, D., K. Bentley, D. Schulze, N. Mahoney, D. Chung, and A. Pracilio. 2020b. Second National Survey of Technology Abuse and Domestic Violence in Australia. WESNET. https://wesnet.org.au/wp-content/uploads/sites/3/2020/11/Wesnet-2020-2nd-National-Survey-Report-72pp-A4-FINAL.pdf.

Woodlock, D., M. McKenzie, D. Western, and B. Harris. 2020a. “Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control.” *Australian Social Work* 73 (3): 368–380. https://doi.org/10.1080/0312407X.2019.1607510

Ybarra, M., M. Price-Feeney, A. Lenhart, and K. Zickuhr. 2017. Intimate Partner Digital Abuse. Report 01.18.17. Data & Society Research Institute. CiPHR Center for Innovative Public Health Research. https://datasociety.net/pubs/oh/Intimate_Partner_Digital_Abuse_2017.pdf.