Heliyon 9 (2023) e17140

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

# A systematic review of ethical challenges and opportunities of addressing domestic violence with AI-technologies and online tools

Peter Novitzky [a,b,*], Janine Janssen [b,c,d], Ben Kokkeler [b,e]

[a] Department of Engineering – STEaPP, PETRAS National Centre of Excellence for IoT Systems Cybersecurity, University College London, United Kingdom
[b] Avans University of Applied Sciences, Breda, the Netherlands
[c] Open University of the Netherlands, Heerlen, the Netherlands
[d] Police Academy of the Netherlands, Apeldoorn, the Netherlands
[e] University of Twente, Department of Science, Technology and Policy Studies, the Netherlands

## ABSTRACT

Domestic violence remains a pressing complex social problem of people of any gender, age, socio-economic status, and ethno-cultural background, an issue that worsened worldwide during the COVID-19 pandemic. Digital, online, or artificial intelligence-based smart technological services, applications, and tools provide novel approaches in addressing domestic violence, including intimate partner violence. This systematic literature review analyses the ethical challenges and opportunities these (protective) digital and smart technologies provide to the stakeholders involved. Our results highlight that the public health and societal issue are the leading narratives of domestic violence, which is predominantly interpreted as gender-based violence. The review highlights an emerging trend of the role of machine learning- and artificial intelligence-based approaches in identifying and preventing domestic violence. However, we argue that little recommendation is available to professionals about how to use these approaches in a responsible way, and that the smartness of high-tech technologies is often challenged by basic-level technologies from perpetrators, creating an imbalance that also limits an impactful development of a comprehensive socio-technical regime that serves the safety and resilience of families in their communal setting.

## 1. Introduction

In Europe domestic violence (also known as domestic abuse, and includes intimate partner violence [IPV])—the pattern of physical or emotional abuse within households or ex-partners, either online and offline, to gain or maintain power and control [1]—is considered a pressing social problem. People of any gender, young or old, rich or poor, from different ethnic and cultural backgrounds can become victims of this particular form of violence [1,2]. Therefore, the Council of Europe on May 11, 2011 adopted the *Convention on Preventing and Combating Violence Against Women and Domestic Violence*, better known as the Istanbul Convention [3], a human rights treaty recognizing violence against women as a violation of human rights and a form of discrimination. The Istanbul Convention, which went into force on August 1, 2014, implements for signatory countries mechanisms to tackle domestic violence via prevention, protection, prosecution, integrated policy development, and monitoring mechanisms [3]. In addition, on Feb 9, 2021 the European Commission launched a public consultation with the aim of creating a legislative initiative that would be best at tackling gender-based

* Corresponding author. Department of Engineering – STEaPP, PETRAS National Centre of Excellence for IoT Systems Cybersecurity, University College London, Shropshire House (4th Floor), 11-20 Capper Street, London, WC1E 6JA, United Kingdom.

*E-mail address:* p.novitzky@ucl.ac.uk (P. Novitzky).

https://doi.org/10.1016/j.heliyon.2023.e17140
Received 14 March 2023; Received in revised form 1 June 2023; Accepted 8 June 2023
Available online 10 June 2023
2405-8440/© 2023 Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

and domestic violence in accordance with the EU's *Gender Equality Strategy* [4]. Domestic violence is not only a European issue, the United Nations 2030 Sustainable Development Goals (SDGs) considers global efforts to reduce violence as an essential way to create sustainable societies [5,6]. Furthermore, as with many societal issues, the challenge of domestic violence also worsened in the light of the global health crisis associated with tackling the COVID-19 pandemic (2020–2022). Hence, the enforced social isolation not only halted the monitoring of levels of domestic violence worldwide [2], it also aggravated the conditions under which domestic violence flourished [7].

Unfortunately, modern and emergent digital technologies are often utilized and abused by offenders of domestic violence [8]. While this raises interesting issues about the dual-use nature of modern and emergent digital technologies, this research paper would like to contribute to the overview of the opportunities these technologies may provide in protecting victims and which tools may contribute to the victims' safety. We give special consideration to Machine Learning/Artificial Intelligence-based (ML/AI) technologies as well, exploring their potential in the fight against domestic violence, and in particular its subcategory, IPV. We refer to ML/AI-based systems as digital technologies capable of performing tasks requiring intelligence by improving their task-specific performance over time through learning and experience [9].

Against this backdrop, the current systematic literature review answers the following question: what are the digital, online (web-based), or ML/AI-based technological services, applications, and tools associated with addressing domestic violence, and what ethical challenges and opportunities do these technologies pose to the stakeholders involved? In particular, we scrutinize the presence of any ethical governing principles, their application in practice, and the various methodological and design frameworks utilized during the application of online tools and digital technologies using artificial intelligence, along with a qualitative assessment of their practical implementations, practical lessons learnt, and their possible future challenges.

Such an overview is needed due to the dearth of systematic overviews of scholarly literature about addressing the challenges of domestic violence with emerging technologies, and their normative underpinnings. The complexity of the issue of domestic violence requires a systematic scrutiny of the theoretical frameworks, methods and approaches, and practical solutions that inform further development in this area.

## 2. Methodology

Our systematic literature review included four steps. First, we developed a set of keywords as search terms for interrogating the scientific databases. These comprised 3 domains: ethics-related, domestic violence-specific, as well as AI, digital, or online technologies-related syntaxes. The syntaxes were refined through multiple iterations and test-searches in the selected scientific databases to minimize the noise and optimize the relevance of the results. The overview of these domain-specific syntaxes is listed in Table 1.

Second, we queried the selected scientific databases with the combined syntax. Whenever it was necessary, the generic search syntax was adjusted to the database-specific syntax, while maintaining transparency. The searched databases excluded Google Scholar[1] for reasons of questionable reproducibility of the search results [10]. However, the search incorporated preprint sources available through the Dimensions.ai database[2] for mapping the most up-do-date research results possible. The overview of the databases queried is provided in Table 2.

The queries included full-text searches of the peer-reviewed publications. The search included results published during 2016–2021, and were limited to papers written in English.

The evaluation of the retrieved publications from the database search, following the syntax query containing the relevant search terms, was based on the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA 2020) methodology [11], applied for new systematic reviews (i.e., searches of databases and registers only).[3] The first round of relevance assessment was limited to the title and abstract of the retrieved publication. Publications that passed the first round underwent an additional second round of relevance assessment by reading the full-text of the publication.

A publication was deemed relevant if it referred to all 4 of the following criteria: a) questions or cases related to domestic violence broadly conceived; b) ethical or value-sensitive methodology, reflection, or evaluation of a technological system from the socio-ethical perspective; c) involved digital, online, or AI-based technological services and applications; d) were written in English.

The resulting list of publications from the database queries were exported into a reference manager, where they were analyzed for duplicity and any duplicates eliminated. Third, the titles and abstracts of the papers were assessed for relevance. Papers deemed irrelevant were excluded. Fourth, the resulting list of potentially relevant publications were then further qualitatively analyzed by reading the full-text of the articles (Fig. 1). The qualitative analysis of the results and their ethical relevance has been inspired by Mepham's methodology (a practical framework to guide ethical analysis and discussion) of ethical analysis [12], with the help of an ethical matrix adjusted to the needs of this literature review.

[1] Google Scholar: https://scholar.google.com.

[2] Research Square Partners with Dimensions to Provide Citation Data on Preprints: https://www.dimensions.ai/news/research-square-partners-with-dimensions-to-provide-citation-data-on-preprints/.

[3] PRISMA 2020 flow diagram for new systematic reviews which included searches of databases and registers only: https://www.prisma-statement.org//PRISMAStatement/FlowDiagram.

**Table 1**
The domain-specific search syntax.

| Domain | Syntax keywords |
|---|---|
| **Ethics** | (((ethical OR moral) AND (judgement? OR argument* OR reason* OR value?)) OR (ethics OR morality) OR utilitarian* OR deontolog* OR virtue OR virtuous OR libertarian* OR communitarian* OR just* OR rightful* OR norm OR decision OR (policy AND (guideline? OR guidance OR recommendation?)) OR principl* OR regulation OR intent* OR oversight OR accountab* OR liab* OR responsib* OR dignity OR (“human right”) OR (“vulnerable person”) OR autonomy) |
| **Domestic violence** | (((domestic OR household OR physical OR psychological OR “intimate partner” OR “intimate relationship” OR “spousal” OR digital) AND (violence OR terrorism OR abuse)) OR (“abusive relationship”) OR (“partner repercussion”) OR (coercive AND (control OR manipulation)) OR bossing OR gaslight* OR disparag* OR “sex trolling” OR (“silent household”) OR (“corrosive silence”) OR (“intimate partner” AND (rape OR assault OR stalk* OR molest* OR harassment)) OR (“sleep deprivation”) OR powerless* OR ((financial OR emotional) AND dependenc*) OR incest OR (cyber AND (bullying OR mobbing)) OR (“shielding relative”) OR (helpline OR “advice line” OR charities) OR (“violence against women and girls” OR “VAWG”) OR (“sexual exploitation”) OR (“sexual exploitation and abuse” OR “PSEA”)) |
| **AI and digital/online technologies** | ((“machine learning”) OR (“neural network”) OR (“pattern recognition”) OR ((reinforcement OR deep) AND learning) OR (“human-scale knowledge”) OR (“domain expert”) OR (“decision tree”) OR (“advice tracker”) OR ((smart* OR intelligen*) AND (instrument* OR home)) OR (“responsible use of technology”) OR (“tech abuse”) OR (“meaningful human control”) OR (“decision forming”) OR (“bot”) OR (“bots”) OR (“distress signal”) OR (“algorithmic fairness”) OR (“black box”) OR (“Pandora’s box”) OR AI OR (“artificial intelligence”) OR (“ambient intelligence”) OR empowerment OR (“victim support”) OR (violence AND (detection OR prevention OR warning OR signalling) AND app?) OR (“technology for good”) OR “AI4Good” OR creepware OR spyware OR spoofing OR (“partner surveillance”) OR (“social network”) OR (ICT OR technolog*) OR digitali?ation OR (“technology?facilitated” AND (sexual OR domestic) violence) OR “TFSV") |

## 3. Results

The database queries and output analyses resulted in 40 relevant publications. The overview of the results from the database queries and output analyses are listed in Table 3. The publication of Turobov et al. [13] was excluded following the inclusion criteria, as its main text is written in Russian, leaving 40 relevant publications in total for analysis.

Building on Mepham’s checklist of concerns [12], we used this matrix to provide categorizations of the reviewed articles that list domestic violence and/or IPV as a topic belonging one of the 6 main categories (Table 4; Fig. 2), the main gender-focus of affected stakeholders represented by the reviewed literature (Fig. 3), and the overview of research methodologies represented in the reviewed relevant publications (Fig. 4).

The overview of the distribution of these categories across the articles is demonstrated (Fig. 2). Most of the reviewed publications categorize domestic violence as a (global) public health (23%) or socio-cultural (23%) issue. The former categorization emerged in the 1980s [49]. A smaller proportion list domestic violence as a policing, criminal justice, and law enforcement challenge (11%), safety & security challenge affecting wellbeing of populations (8%), or as a human rights issue (7%). A consistent amount of publications approached IPV from the technology and ML/AI perspective (28%).

The majority of the reviewed publications investigated IPV from a women’s perspective (59%), while only a single study focused on men (3%). A large number of publications did not have any specific gender-focus (28%), while 10% of the studies used a gender-neutral inclusive approach (Fig. 3).

Most of the literature we reviewed on IPV and technology were literature reviews, ethnographic observation investigations, or research involving ML/AI with deep learning neural networks (20% each category). 9% of the reviewed publications reported on a prototype development of specific devices. These prototype-development often involved elements of participatory design approaches with relevant stakeholders’ involvement. Other studies used pure data-mining approaches, or conceptual analyses (7% each category) without direct stakeholder involvement. A single publication provided dedicated ethical analysis (2%; Fig. 4).

## 4. Findings

### 4.1. *The phenomenon of domestic and intimate partner violence*

#### 4.1.1. *Important concepts*

IPV is characterized by coercive control and is an inherently gendered crime, with women disproportionately affected (most commonly with men being the perpetrators and women the victims [2,14,49]). Thus, IPV is a subset of domestic violence, where the latter *per definitionem* includes also children or other individuals associated with a household [1]. Psychological violence, emotional violence, and emotional abuse are also used interchangeably in reports describing the correlated types of phenomena [2,53,54].

Mayhew and Jahankhani [26] list various types of coercive control, such as, isolation from friends and family members, deprivation of basic needs (e.g., food, sleep, meeting others, whereabouts, medical services); time and online communication monitoring (e.g., spyware, keyloggers); repeated humiliation and dehumanization (e.g., putting down, making one feel worthless) or intimidation; and financial control.

Abreu Maia et al. [49] categorize interpersonal violence into a) *family violence* (e.g., child maltreatment; IPV; elder abuse); and b) *community violence* (e.g., acquaintance and stranger violence; youth violence; assault by strangers, property crimes related violence; workplace violence). Some resources refer to domestic violence/IPV as to an ‘epidemic’ [14] that is endemic [54], whereas previous ethnological studies confirmed intimate partner and domestic violence in 90 societies, affecting 84.5% women, 6.7% men, and 74.4%

**Table 2**
Overview of queried databases and database-specific syntaxes.

| Database/URL | Database-specific syntax |
|---|---|
| **Web of Science/Web of Knowledge**/https://clarivate.com/webofsciencegroup/solutions/web-of-science/ | (TS=(((ethical OR moral) AND (judgement? OR argument* OR reason* OR value?)) OR (ethics OR morality) OR utilitarian* OR deontolog* OR virtue OR virtuous OR libertarian* OR communitarian* OR just* OR rightful* OR norm OR decision OR (policy AND (guideline? OR guidance OR recommendation?)) OR principl* OR regulation OR intent* OR oversight OR accountab* OR liab* OR responsib* OR dignity OR (“human right”) OR (“vulnerable person”) OR autonomy)) AND LANGUAGE: (English) AND (TS=((“machine learning”) OR (“neural network”) OR (“pattern recognition”) OR ((reinforcement OR deep) AND learning) OR (“human-scale knowledge”) OR (“domain expert”) OR (“decision tree”) OR (“advice tracker”) OR ((smart* OR intelligen*) AND (instrument* OR home)) OR (“responsible use of technology”) OR (“tech abuse”) OR (“meaningful human control”) OR (“decision forming”) OR (“bot”) OR (“bots”) OR (“distress signal”) OR (“algorithmic fairness”) OR (“black box”) OR (“Pandora’s box”) OR AI OR (“artificial intelligence”) OR (“ambient intelligence”) OR empowerment OR (“victim support”) OR (violence AND (detection OR prevention OR warning OR signalling) AND app?) OR (“technology for good”) OR “AI4Good” OR creepware OR spyware OR spoofing OR (“partner surveillance”) OR (“social network”) OR (ICT OR technolog*) OR digitali?ation OR (“technology?facilitated” AND (sexual OR domestic) violence) OR “TFSV”)) AND LANGUAGE: (English) AND (TS=(((domestic OR household OR physical OR psychological OR “intimate partner” OR “intimate relationship” OR spousal OR digital) AND (violence OR terrorism OR abuse)) OR (“abusive relationship”) OR (“partner repercussion”) OR (coercive AND (control OR manipulation)) OR bossing OR gaslight* OR disparag* OR “sex trolling” OR (“silent household”) OR (“corrosive silence”) OR (“intimate partner” AND (rape OR assault OR stalk* OR molest* OR harassment)) OR (“sleep deprivation”) OR powerless* OR ((financial OR emotional) AND dependenc*) OR incest OR (cyber AND (bullying OR mobbing)) OR (“shielding relative”) OR (helpline OR “advice line” OR charities) OR (“violence against women and girls” OR “VAWG”) OR (“sexual exploitation”) OR (“sexual exploitation and abuse” OR “PSEA”))) AND LANGUAGE: (English) |
| **Scopus Elsevier**/https://www.scopus.com/ | TITLE-ABS-KEY ((((domestic OR household OR physical OR psychological OR “intimate partner” OR “intimate relationship” OR spousal OR digital) AND (violence OR terrorism OR abuse)) OR (“abusive relationship”) OR (“partner repercussion”) OR (coercive AND (control OR manipulation)) OR bossing OR gaslight* OR disparag* OR “sex trolling” OR (“silent household”) OR (“corrosive silence”) OR (“intimate partner” AND (rape OR assault OR stalk* OR molest* OR harassment)) OR (“sleep deprivation”) OR powerless* OR ((financial OR emotional) AND dependenc*) OR incest OR (cyber AND (bullying OR mobbing)) OR (“shielding relative”) OR (helpline OR “advice line” OR charities) OR (“violence against women and girls” OR “VAWG”) OR (“sexual exploitation”) OR (“sexual exploitation and abuse” OR “PSEA”)) AND ((“machine learning”) OR (“neural network”) OR (“pattern recognition”) OR ((reinforcement OR deep) AND learning) OR (“human-scale knowledge”) OR (“domain expert”) OR (“decision tree”) OR (“advice tracker”) OR ((smart* OR intelligen*) AND (instrument* OR home)) OR (“responsible use of technology”) OR (“tech abuse”) OR (“meaningful human control”) OR (“decision forming”) OR (“bot”) OR (“bots”) OR (“distress signal”) OR (“algorithmic fairness”) OR (“black box”) OR (“Pandora’s box”) OR ai OR (“artificial intelligence”) OR (“ambient intelligence”) OR empowerment OR (“victim support”) OR (violence AND (detection OR prevention OR warning OR signalling) AND app?) OR (“technology for good”) OR “AI4Good” OR creepware OR spyware OR spoofing OR (“partner surveillance”) OR (“social network”) OR (ict OR technolog*) OR digitali?ation OR (“technology?facilitated” AND (sexual OR domestic) violence) OR “TFSV”) AND (((ethical OR moral) AND (judgement? OR argument* OR reason* OR value?)) OR (ethics OR morality) OR utilitarian* OR deontolog* OR virtue OR virtuous OR libertarian* OR communitarian* OR just* OR rightful* OR norm OR decision OR (policy AND (guideline? OR guidance OR recommendation?)) OR principl* OR regulation OR intent* OR oversight OR accountab* OR liab* OR responsib* OR dignity OR (“human right”) OR (“vulnerable person”) OR autonomy)) AND (LIMIT-TO (PUBYEAR, 2021) OR LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018) OR LIMIT-TO (PUBYEAR, 2017) OR LIMIT-TO (PUBYEAR, 2016)) |
| **Dimensions.ai**/https://app.dimensions.ai/ | ((((domestic OR household OR physical OR psychological OR “intimate partner” OR “intimate relationship” OR spousal OR digital) AND (violence OR terrorism OR abuse)) OR (“abusive relationship”) OR (“partner repercussion”) OR (coercive AND (control OR manipulation)) OR bossing OR gaslight* OR disparag* OR “sex trolling” OR (“silent household”) OR (“corrosive silence”) OR (“intimate partner” AND (rape OR assault OR stalk* OR molest* OR harassment)) OR (“sleep deprivation”) OR powerless* OR ((financial OR emotional) AND dependenc*) OR incest OR (cyber AND (bullying OR mobbing)) OR (“shielding relative”) OR (helpline OR “advice line” OR charities) OR (“violence against women and girls” OR “VAWG”) OR (“sexual exploitation”) OR (“sexual exploitation and abuse” OR “PSEA")) AND ((“machine learning”) OR (“neural network”) OR (“pattern recognition”) OR ((reinforcement OR deep) AND learning) OR (“human-scale knowledge”) OR (“domain expert”) OR (“decision tree”) OR (“advice tracker”) OR ((smart* OR intelligen*) AND (instrument* OR home)) OR (“responsible use of technology”) OR (“tech abuse”) OR (“meaningful human control”) OR (“decision forming”) OR (“bot”) OR (“bots”) OR (“distress signal”) OR (“algorithmic fairness”) OR (“black |

(*continued on next page*)

**Table 2** (*continued*)

| Database/URL | Database-specific syntax |
|---|---|
| | box") OR ("Pandora's box") OR AI OR ("artificial intelligence") OR ("ambient intelligence") OR empowerment OR ("victim support") OR (violence AND (detection OR prevention OR warning OR signalling) AND app?) OR ("technology for good") OR "AI4Good" OR creepware OR spyware OR spoofing OR ("partner surveillance") OR ("social network") OR (ICT OR technolog*) OR digitali?ation OR ("technology?facilitated" AND (sexual OR domestic) violence) OR "TFSV") AND (((ethical OR moral) AND (judgement? OR argument* OR reason* OR value?)) OR (ethics OR morality) OR utilitarian* OR deontolog* OR virtue OR virtuous OR libertarian* OR communitarian* OR just* OR rightful* OR norm OR decision OR (policy AND (guideline? OR guidance OR recommendation?)) OR principl* OR regulation OR intent* OR oversight OR accountab* OR liab* OR responsib* OR dignity OR ("human right") OR ("vulnerable person") OR autonomy)) |

children [55].

A related term of cyber-violence is defined as a "broad range of repeated abuse (controlling and coercive behaviours) committed by one person (the perpetrator) against their current or former intimate partner (the victim) through the use of technology" regardless of geographical boundaries [14]. This is also called technology-facilitated abuse, which can occur at any stage of the relationship, however, such abuse may escalate over a long period of time, making an effort to leave the abusive relationship difficult [14]. It may involve a) abuse (unwanted calls, cyber-stalking); b) control (activities, locations, involvement with others; surveillance, monitoring, spyware apps, hacking into social media accounts); c) harassment (dissemination of intimate image, revenge porn, reputational damage); d) attempts to isolate the victim (tampering/destroying/hiding assistive technology devices); e) it may also involve existential threat (killing) [14,22].

#### 4.1.2. Social context

Although our analysis focused primarily on technology-facilitated IPV, children often are either affected by or themselves victims of domestic abuses. Emeuze [17] highlights that children and adolescents may also experience technology-based abuse in forms of online stalking, zoombombing, cyberbullying, doxing, sexualized trolling, non-consensual pornography, and other forms of coercive behaviours with adverse implications. Sasaki and Ishii-Kuntz [41] provide an overview of immediate, short-, and long-term effects of IPV on children and their families in the Japanese context.

Ucuz et al. [30] used ML techniques in psychiatric assessment process to support early post-abuse forensic evaluation and diagnostics of children. Wall, Jenney et al. [31] developed a novel technological application (CommuniCAT-CS) that facilitates data collection from children exposed to violence. Decker et al. [16] also report on the development of a myPlan Kenya app that provides a means for risk self-assessment that extends to children.

Our study also overlaps with the outbreak of the COVID-19 pandemic (2020–2022). The WHO [2] highlights that the overall impact of the pandemic on IPV prevalence rates is not well known, as it interrupted multiple survey studies. However, the WHO [2] emphasizes that the prevalence of IPV before the pandemic was already high globally (based on data collected during 2000–2018), and multiple reports from helplines, policy, health and other services suggest further increase of IPV during the pandemic. The 3-week average UK Domestic Abuse figures in cases of fatal violence on women by men roughly doubled at the beginning of the pandemic, compared with similar periods in previous years [26,56].

Emeuze [17] highlights that alongside the pandemic, domestic abuse is described as 'shadow pandemic' by a representative of UN Women, also confirming that domestic violence hotlines faced an unprecedented surge in calls in the first week of lockdowns. Digital interventions are valuable additions to socially and physically isolated people experiencing abuse [17].

#### 4.1.3. Causes

Among the main sources of domestic violence/IPV are commonly listed *a)* the current social norms and associated power relations, including attitudes supporting violence [22]; *b)* rapid urbanisation [49]; *c)* consumer aspirations [49]; *d)* unemployment [49]; *e)* lower level of acquired education [22,49,57]; *f)* poverty [22,49]; *g)* family dynamics and history [22]; *h)* drug and alcohol abuse [49]; and *i)* the ease of acquiring firearms [49].

Amusa et al. [22] define covariates that significantly influence the prediction of IPV. These include the fear of the partner as the most prominent one, followed by attitudes towards violence, then, history of abuse, and then, alcohol and drug use. Fear is the strongest predictor of IPV, while exhibiting reverse causality (endogeneity) [22].

The one of the explanatory phenomena corresponding with cyber-violence/technology-facilitated abuse is the anonymity provided by the technology. It may create *toxic disinhibition*, which refers to lowered or completely abandoned social restrictions in cyberspace, resulting in abusive behaviour that would otherwise not be expressed during an in-person interaction [14,58].

#### 4.1.4. Consequences

The effects of domestic violence/IPV, both in general terms as well as technology-facilitated violence, can be categorized as physical, mental/emotional, behavioural, societal, and sexual/reproductive aspects. As many of these extend to technology-facilitated violence, while the first (physical) and last (sexual/reproductive) concern the non-technical domain.

Among the common *physical* effects of domestic violence/IPV in the reviewed literature were listed maxillofacial injuries. In these

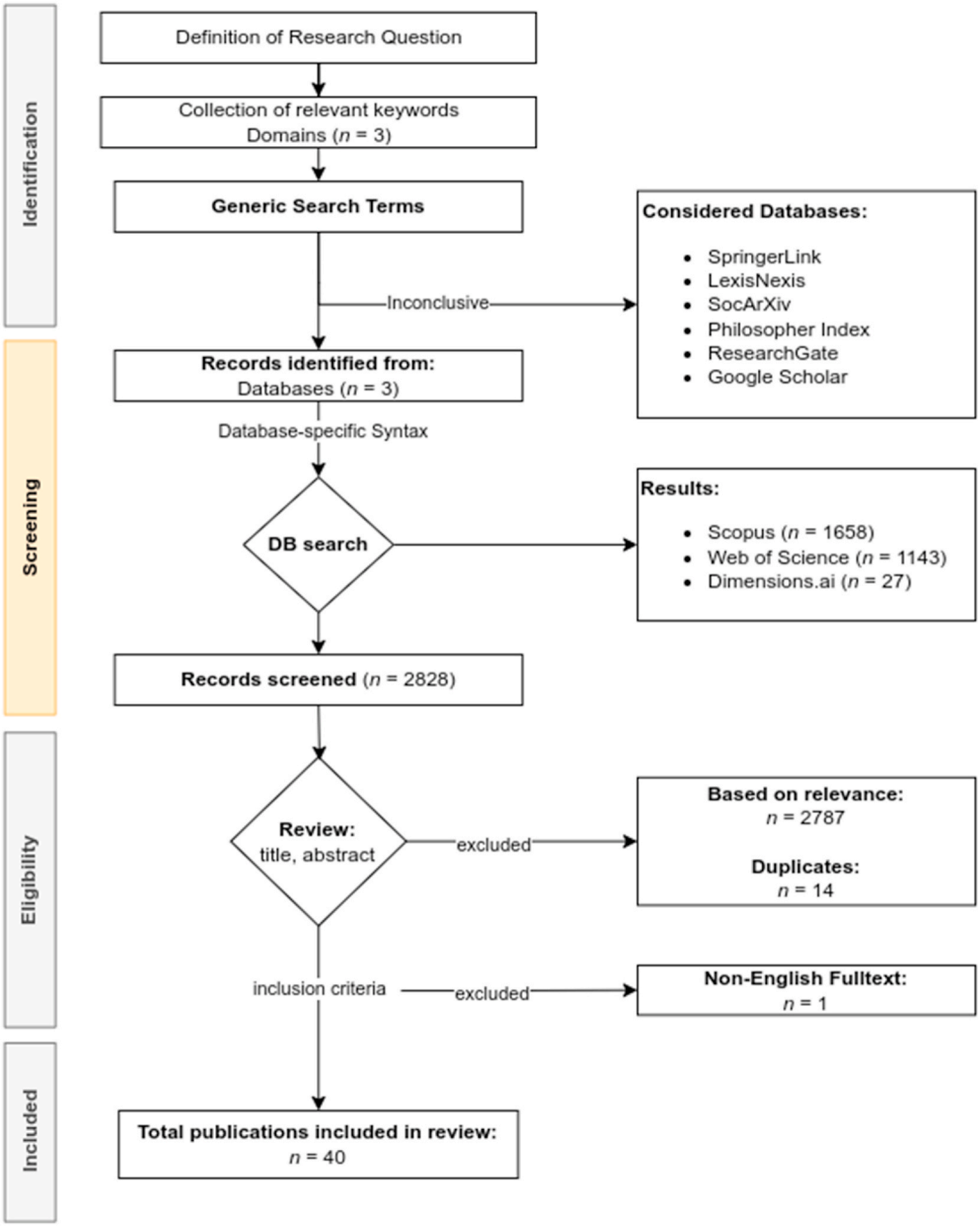

**Fig. 1.** PRISMA 2020 [11] flow chart.

**Table 3**
Overview of database results and number of relevant publications.

| Database | Total Number of Publications | Number of Relevant Titles/Abstracts | Duplicates from Total |
|---|---|---|---|
| **Web of Science/Web of Knowledge** | 1143 | 24 | N/A |
| **Scopus Elsevier** | 1665 | 12 | 14 |
| **Dimensions.ai** | 48 | 5 | 0 |

**Table 4**
Categorization of relevant publications based on source of domestic violence/IPV. The categories may overlap across a single publication.

| Category | Publications |
|---|---|
| Personal Safety & security, wellbeing | [14–20] |
| Technology, AI | [14–17,19–35] |
| Policing, Criminal Justice, Law enforcement | [14,23,26,36–41] |
| Societal, Cultural issue | [14,17,22,26,28,35,38–48] |
| Global or Public health issue | [2,14,15,17,22,25,27,29–32,42,45,49–52] |
| Human rights issue | [2,33,34,41,46] |

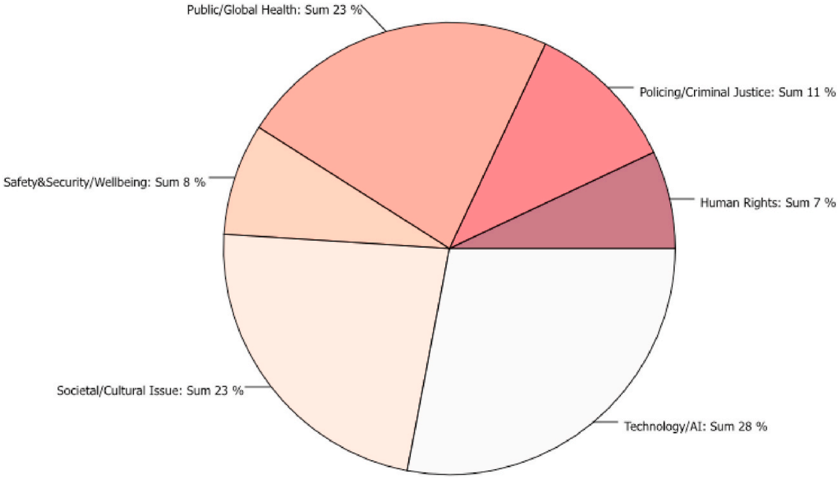

**Fig. 2.** Overview of topic-focus of relevant reviewed publications.

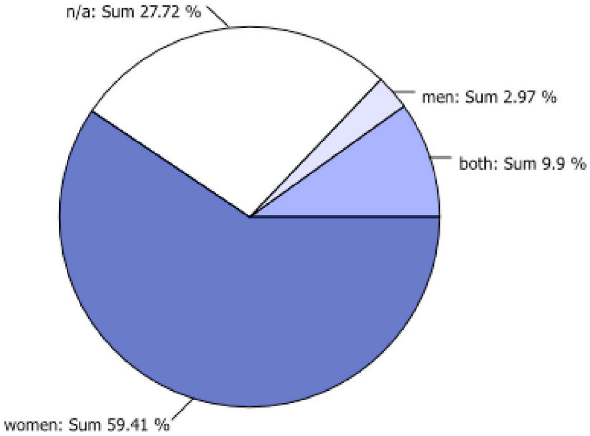

**Fig. 3.** Overview of gender-focus of relevant reviewed publications.

cases of violence it is usually the face that is a first point of contact in various human interactions [49]. Domestic violence/IPV can furthermore lead to additional physical disabilities and/or severe functional or permanent deformities [49].

Secondly, *behavioural* consequences of domestic violence/IPV may comprise attempts to isolate and control the victim. This can extend to technological means, e.g., limiting social interactions with relatives and friends, as well as surveillance as a part of parental contact [46]. Victims of technology-facilitated domestic violence/IPV are often reluctant to block the perpetrators on their devices out of fear of consequences (e.g., it is better to know what the perpetrator does than be agnostic and caught unguarded; [46]), which affects long-term behavioural patterns.

Thirdly, one of the major consequences of domestic violence/IPV involve *mental and emotional* wellbeing. Wellbeing is affected by cyberbullying [21] (which is a recognized phenomenon since 2003 [59]; temporary anxiety to suicide [21]; depression [22]; causing traumatic experiences and consequently the development of long-term PTSD [14,22]. Technology in this regard is has been utilized to

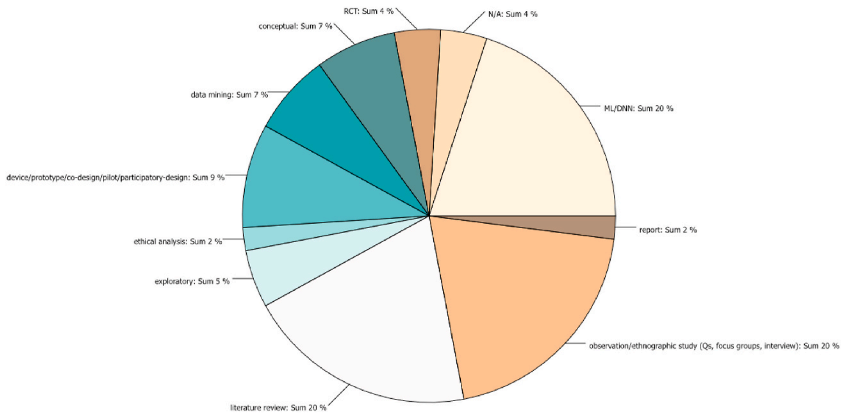

**Fig. 4.** Overview of research methodologies in the relevant reviewed publications.

spread terror (e.g., playing loud music remotely via smart speakers in the middle of the night; [60]); gaslighting [61]. Smart devices also enable the perpetrator to stalk via SNS and GPS location tracking [46]. Digital recordings were also used in cases of blackmailing (e.g., intimate records) [46].

Fourthly, *societal* effects of technology-facilitated domestic violence/IPV were linked with the unauthorized sharing of intimate records referred to as revenge porn [46]. Another such activity is fraping, which also involves unauthorized alteration of individual's profile information on social media accounts by a third party [18].

Finally, the effects of domestic violence/IPV on *sexual and reproductive* capacities are linked with sexually transmitted diseases, e.g., HIV/AIDS [22].

Henry et al. [38] identify the main challenges associated with domestic violence in its context, its significance, as well as impacts. They found a diverse variety of behaviours in IPV violent contexts, where technology is used to a) set up and b) commit the abusive act, which can then be conducted c) repeatedly. The sole focus on the technology may lead to misconceptions that digital technologies are somewhat independent of gender dynamics, and other contextual settings within a particular relationship may be thus overlooked. Thus, it is important to highlight that with this contextual information, the impacts of fear, and psychological distress play out differently on the parties involved [38].

#### 4.1.5. *Interventions and prevention*

The reviewed literature categorize the possible interventions of domestic violence/IPV prevention into primary, secondary, and tertiary programmes (including the use of technology). Primary prevention programmes aim to reduce the incidence of health threats before their occurrence, which include school- and community-based adolescent and family programmes precluding victimization and perpetration [50]. Primary prevention programmes may be disseminated as a part of mHealth over Internet and web-based educational activities, and usually focus on the underlying causes of IPV [42]. Secondary prevention programmes include IPV screening in healthcare settings, relocation into safe-haven shelters, counselling, medical and legal support preventing victimization [50]. Secondary prevention programmes focus on early detection post-exposure and subsequent treatment [42], while also incorporating diversion programmes, anger management, and de-escalation interventions organized for perpetrators [50]. Tertiary prevention programmes traditionally deal with mitigation efforts as well as the impacts of past experiences of IPV, PTSD counselling, recidivism reduction, or community reintegration [42,50].

### 4.2. *Overview of technologies and their impact*

#### 4.2.1. *Technological opportunities*

Al-Alosi [14] categorizes five key areas where technology can play a positive, empowering role in cases of IPV/domestic violence. These comprise: 1) provision of essential resources and services for victims; 2) reduction of loneliness, isolation, and facilitation of contact with (online) support groups; 3) provision of safety devices, assistance in safety plan development; 4) recording and collection of evidence for abuse; and 5) empowerment of victims.

First, essential (technological) resources and services predominantly focus on mobile phones, which represent a first point of contact, while providing access to a wide array of other services (e.g., housing, employment, safety) [14]. Informal self-help services and access to support groups can be also facilitated by phone, however, it has to be reminded that not every individual owns a phone as a personal device [47]. Access to technology further enables victims with necessary education enabling victims to help identify an abusive relationship and seek support; screening; follow-up care; legal services and advice, and mental health services, mostly in forms of technology dependent support (e.g., eGovernment) [14].

Providing these services online via anonymous access is useful, as face-to-face interactions often cause stigma, humiliation, and feelings of guilt and shame for the victims of abusive relationships [14,62].

Second, technological assistance may contribute to reducing the feelings of isolation and hopelessness in victims by providing access to online support groups, support buddies or other forms of peer support [29,45]. In Australia and United States phone companies offered free phone access to women experiencing IPV [14,63]. However, as suggested by the Duluth Power and Control wheel,[4] perpetrators may use tactics to isolate their partners by controlling what the victim does or has access to, and who she communicates with, further limiting interactions, which are often justified by jealousy for these actions [14].

Third, devices may provide heightened levels of safety and assist in safety plan development. A variety of disguisable tools and wearables can trigger alarms with the police (e.g., CCTV, watches, panic buttons) [14]. In the reviewed literature Campos Gaviño et al. [23] report on the development of Bindi, a non-intrusive wearable necklace pendant device accompanied by a watch (smart bracelet), which, alongside a smartphone app, measures physiological data (e.g., blood volume pulse, galvanic skin response, skin temperature) and records speech and environmental audio to associate emotions with physiological signals in order to detect increased stress levels and potential violence detection. Chitkara et al. [33] developed a cheap safety device in form of a glove, which delivers a non-lethal electric shock to an abuser during a violent activity.

Fourth, technologies can play an important role in recording and collecting evidence of abuse. The importance of such evidence lies in the practice of discrediting the victim in court proceedings, without which obtaining a court protection order can prove to be difficult [14]. Digital evidence may make the perpetrators accountable, and assist further in enforcing the intervention order by recording its breach [14,64]. However, the uncontrolled disclosure of such data can also lead to re-victimization [64].

Consequently, technological means may provide further empowerment to the victims of domestic abuse by providing continuous support in iterative actions and making progress toward the desired goal [14]. Technologies may also contribute to the development of an economic independence of victims of IPV to facilitate financial empowerment of IPV victims, however only a few studies explored the role of technology in this domain [14].

Rodriguez-Rodriguez et al. [19] provide a complete, holistic platform based on Internet of Things (IoT) devices to tackle IPV. The goal is to overcome the previous technological limitations of available solutions. The platform provides multi-layered deployment, commonly used in IoT environments, for IPV monitoring, detection, and reporting. The multi-layered approach involves: a) substrate, e.g., BAN where the real source of data is generated; b) sensorization layer, which may involve both, the previous victim as well as the offender, for monitoring with multiple IoT devices; c) communication layer, communicating wirelessly with a gateway; d) middleware layer, which usually include other domotic sensors that fuses and unites data from various sources; e) computing and management layer, which provides text, AV-recognition, and can employ also ML/AI techniques; f) display/interface layer, which facilitates meaningful visualization of a possible alarm; and g) output layer, which may continuously report on current status and may provide ML/AI-enhanced prediction, management of risky situations [19]. The proposed holistic platform provides continuous status monitoring of previous victims and offenders, emergency management, as well as the seamless exchange of necessary information between possible victims and law enforcement or other professional and trusted entities [19].

### 4.2.2. *The novelty of apps*

A specific sub-type of technologies are software-based applications, which usually run on mobile devices of users or can be reached through the world-wide-web. The reviewed literature lists multiple proof-of-concepts and tested solutions, focusing on the various levels of prevention and support.

The review conducted by Cardoso et al. [24] lists that 38% of mobile devices and 18% of apps provide some form of protection, while 58% of mobile devices and 14% of apps try to address perpetration. Shah et al. [20] refer to the works of Sandulescu et al. [65] and Saki et al. [66]: the former focusing on a general improvement of quality of life by mobile phone recorded stress-detection of sound features and analyzed by an ML-approach; the latter also using ML-based real-time sound classification by mobile phone.

Multiple papers referred to the myPlan safety app [15,17], the aim of which is to provide a complex support for the safety of people in low- and middle-income countries against IPV. This goal is achieved primarily as a computer-based decision aid, assisting survivors of IPV to make tailored informed decision about their wellbeing, utilizing Dutton's empowerment model [17]. A 12-months follow-up study proved the effectiveness of the myPlan app in terms of reduced total decisional conflict and increased subjective feeling of safety in decision-making in IPV [17,67].

Bellini et al. [45] report on the study in collaboration with a national charity (NGO) <Safe Start>, with whom they investigated the role of digital technologies in assisting perpetrators to reconsider and reform their abusive behaviour. Using ethnographic research methods the investigators highlight, for example, the role of modern messaging applications and social media to encourage partaking in regular meetings. However, the novelty of the types of technologies did not extend beyond the mobile phones, suggesting that often mundane and less sophisticated digital communication tools can prove to be efficient [45].

Tarzia et al. [68] and Jewkes et al. [51] report on the I-DECIDE project, which developed an online healthy relationship website application. The main benefits of such an approach are described as: its easy availability 24/7, as well as its seemingly anonymous nature (i.e., easier than telling someone) for asking questions and seeking support and reassurance for victims of IPV. In addition, a website can provide further information and raise overall awareness about the various forms, nuances, and the full spectrum of abusive relationships that would otherwise remain undetected [68]. Jewkes et al. [51] highlight the complex decision-making support of I-DECIDE for women experiencing IPV, and caveat that the needs these online tools try to provide may vary across the globe. Moreover, the acceptability of such technology needs to be established.

iSafe is also a web-based interactive and individualized Web-based decision aid for indigenous Māori women [17]. It involved a

[4] https://www.theduluthmodel.org/wheels/.

safety priority setting activity, a danger assessment tool, and an interactive matrix of resources to aid in the development of an individually tailored action plan [69].

Finally, Wall et al. [31] report on the development of tablet-based program, which assists in data collection while working with children exposed to IPV.

#### 4.2.3. A brand new field: AI/ML-based approaches

Studies reviewed by El Morr et al. [25] highlight the paucity of research addressing digital technologies in IPV prevention and interventions, especially in the domains of awareness, screening, prevention, and treatment. Despite the wide availability of digital technologies, ICT-based interventions are lacking in addressing IPV prevention and post-IPV challenges (e.g., mental illness, integration, coordination of healthcare and social services), which are currently missing from the literature [25].

There is an emerging amount of scholarly publications (Fig. 4) that approach IPV prevention from the ML/AI and data mining perspective. Although these algorithms often use historical data for retrospective studies [30], their learning capabilities through powerful statistical analysis (including deep neural networks), applied to large datasets (e.g., registries collected by institutions [22]; social media records [21]; audio records [20]) can predict risk levels of cyberbullying, IPV, etc. [19,27–29,32,34].

#### 4.2.4. Technological challenges

On the negative side, technologies themselves introduce challenges. Given the lack of any current categorization, we provide a preliminary grouping, based on the nature, extension, or level of challenges that are mentioned in the reviewed literature.

*Vulnerabilities from Operational Challenges*: Technologies can often break down, as highlighted by Al-Alosi [14]. Due to this fact, over-dependence on these technologies may expose the vulnerabilities of users (and victims of IPV) to a greater degree.

Mayhew et al. [26] specify attack vectors used in technology-facilitated domestic violence, e.g., stalking, violating secrecy of electronic correspondence (i.e., messaging, emails), using electronic device gifts (also to children) as surveillance technologies; smart heating, lighting and door control systems; voice personal assistants; audio systems.

Campos Gaviño et al. [23] furthermore highlight the challenges associated with solely technologically obtained evidence without real-time witnessing of the data generation process, as any digital data is intrinsically prone to manipulation. A related practice is called fraping, which refers to activities of unauthorized social media information alteration by third parties [18].

*Vulnerabilities from Empowerment of the Perpetrators*: Moreover, not all technological systems can be used by the victims. For example, electronic monitoring and body-worn cameras are predominantly used by law enforcement to document the response to IPV for the criminal justice system [14]. Furthermore, monitoring technological systems and similar may also empower the abusers as well (by providing surveillance and sousveillance capabilities).

Al-Alosi [14] mentions that a victim was denied the access to a Facebook account and therefore she visited her sister's account to regain a sense of belonging to her family. However, she also says that victims who maintain social media account risk being stalked (content-wise, and location-wise).

*Insufficient Awareness and Willingness to Use*: Another limitation of these technologies is that their potential is significantly undermined by the lack of willingness to engage with these technologies by the practitioners [14].

*Lack of Funding*: The limitations of technologies and their insufficient awareness is further exacerbated by the lack of necessary funding for technology allocation [14].

#### 4.2.5. Policy-related paradigm challenge emergence of statistical risk prediction and its effects on policing

Risk calculations emerged from the 18th century trade, commerce, and insurance industries that gradually expanded to social spheres; often coined as actuarial science, which refers to the calculation and management of risk and uncertainty [40]. It's growth is often associated with the emergence of neoliberal concepts of efficiency, supported by technocratic, data-driven, algorithmic and smart technologies and their governance [40].

Black et al. [36] refer to the book of *Policing the Risk Society* [70], which merges the ideas of 'risk society' (also called new penology thesis) developed by Beck [71]; with Michel Foucault's 'governmentality' perspective. The former refers to the increasing awareness of risk in societies of late modernity that favours management of offenders belonging to various risk groups instead of morally reforming them individually [71]. In this narrative the rehabilitative nature of punishment prevalent since the 19th century lost legitimacy in the 20th century, which led to increased penal severity, externalizing parts of the crime control beyond the state [72,73]. The latter develops a social constructionist account of risk 'in process' or 'ever becoming,' providing a less all-encompassing and more attainable risk management perspective [36]. Risk usually refers to the (statistical) likelihood of an individual not being the subject of a trial, or likelihood of not offending again [40]. Modern societies shift their focus from moral culpability of offenders to the assessment of riskiness of groups of societies in a statistical sense [74,75], while reconceptualizing risk management from a societal to a genuinely private issue [75].

Werth [40] distinguishes 4 generations of risk assessment approaches, used variously in correctional settings today: 1) clinical/professional/subjective evaluation conducted by professionals used on a case-by-case basis; 2) actuarial risk instruments implemented between 1930 and 1970 and beyond, which focused on the statistical prediction of reoffending using static risk factors (e.g., gender, criminal history, age at first arrest); 3) risk and needs assessment, which introduces next to static risk factors also dynamic/criminogenic needs, i.e., factors that can change and contribute to the individual correction (e.g., employment status, education level); 4) latest advancement in the risks and needs assessment focusing on linking better the assessment with correctional management and treatment.

In light of the latest developments, police work revolves around risk management, where the various continua of future risk predictions take precedence over actual danger, and society is often consumed by insecurity and fear [40,70]. Risk professionals thus generate forms of risk communication, in which technology provides the means for risk classification and knowledge, contributing to a 'perpetual quest for certainty' [70].

The concept of risk society gained increased prominence from the 1990s onwards, when terrorist attacks and economic uncertainties lead to the re-evaluation of existing risk management tools [36]. Actuarial criminal risk prediction instruments were developed since the 1920s, from the 1960s onwards parole agencies developed actuarial tools, and risk instruments becoming a necessity rather than a convenience from the early 1990s [40]. In this context the 'precautionary principle' paradigm prevailed over the discourses about manageable risk [36]. In this paradigm any level of risk is unacceptable, the effectiveness of risk assessment tools is limited, and consequently the only responsible action is the prevention of risk by any means, and the future cost of risk is immeasurable [70]. The governance based on the precautionary principle moves on the following continuum: zero risk–worst case scenario–shifting the burden of proof–serious and irreversible damage, where newly the worst case scenario dominates the discourse instead of evidence-based policy, assumed and developed knowledge about risks. Consequently, uncertainty becomes a justification for pre-emptive action before risks even become known [36].

Black et al. [36] employ Foucault's concept of *le dispositif* [76,77]. It refers to apparatus, i.e., an analysis of institutional constellations, administrative practices and beliefs that create conditions of exercising powers in society. This analysis uses the pretext that systems are historically situated, following certain inherent forces, resources, and norms [78]. The dispositif thus allows the analysis of, amongst others, unintended consequences, highlighting the way how everyday risks are governed instead of focusing on the calculable nature of the particular risks. The Foucauldian conceptualization sets the question of uncertainty into the organizational practice [79], which instead of focusing on the question of manageability of the unknown risks, analyses organizations as if management of the risk at hand is possible [36].

In addition, Werth [40] highlights the limitations of the latest risk instruments, and the prevailing hybrid responses of field level personnel. Actuarial risk management instruments are not short of additional rehabilitative and case-by-case approaches from practitioners, highlighting pertaining complexities of most of the cases and their goals (e.g., rehabilitation, retribution, risk containment). Field level personnel utilize the actuarial tools to protect themselves professionally to provide an institutional mechanism of justifying decisions, protection from professional oversight, or potential job loss (referred to 'institutional insulation' [40]). However, they often also defer these risk techniques by altering, minimizing, subverting, or resisting them in a variety of circumstances. Reasons behind these practices vary from the lack of trust in these techniques compared with their own clinical, professional evaluations; using them only in specific occasions for supporting a decision on risk but rarely on needs; or adjusting the scores to match pre-existing opinions as well as compensate based on information that is not part of the risk techniques [40].

The research by Powell et al. [39] provide insights into the practices of police forces while dealing with cases of IPV, and highlight that there is a dearth of existing literature on adult experiences of technology-facilitated (sexual) violence. They also highlight that electronic forms of IPV in certain cases represent a Catch-22: sometimes they provide sufficient evidence of victims' experience, in other occasions they are do not acknowledge acts of abuse as serious harms [39].

In the policy domain the Smart Home Anti Domestic Abuse framework (SHADA), proposed by Mayhew et al. [26], suggests further legislative amendments to the UK Domestic Abuse bill based on the SHADA framework; requests more precise functional standard definition for technology developers of smart environments affecting domestic abuse; and argue for increased awareness of the general public about digital coercion and IPV in line with the SHADA framework [26].

## 5. Discussion

This literature review of the current use of technology in the area of domestic abuse highlighted that questions of IPV are at the heart of family privacy; there is a novel group of ML/AI-based techniques aiming at forecasting and prevention of IPV; the IPV debate is one-sidedly gender-based omitting all other forms of cohabitation; and fast pace of technological innovation. Below we will elaborate each of these topics individually.

### 5.1. Domestic violence and family privacy

Families are referred to as the nuclei of societies, and for the required level of intimacy, privacy is necessary [80]. This privacy is justifiably questionable at the evidence of domestic violence and IPV, and the safety, wellbeing, or best interest of the involved parties (be it any of the intimate partners, or children). In such cases the involvement of law enforcement, community assistance, and healthcare professionals is rightful in order to avoid further escalation of harm, for protection and respect of human dignity.

The challenge lies with the first and unreported cases of domestic violence, which often remains ignored, unnoticed, or dismissed by close communities, relatives, etc., associated with the affected families, and often lead to (re-)victimization with negative spill-overs to children [14,81,82]. Ubiquitous smart home appliances, ambient voice assistants, wearables, or even mobile phones may have the capabilities to constantly monitor the increasing prevalence of such incidents. However, such scenario would not only be seriously intrusive to family privacy, but they would also intrude into the privacy of homes (and anybody who even temporarily shares the same environment).

Rather, aligned with the rediscovery of the (moderate) communitarian perspectives applicable to emerging technologies [83], the distincion of Bell [84] of the various types of communities sound plausible for the issue of domestic violence and the role of technology in it. Bell [84] emphasizes communities of a) place, b) memory, and c) psychological communities; all relevant for valued (communal) life. Communities of place refer to locality in physical and geographical sense, associated mostly with home or birthplace.

Communities of memory refer to groups sharing morally significant history, while psychological communities represent interactive bonds based on trust, cooperation, and altruism [84]. For domestic violence—traditionally described as a complex issue—all three forms of communities can be instrumental in a richer conceptualization of prevention, detection, and recovery. Such a conceptualization is then capable to overcome any reductionist interpretation of technologies as quick-fixes.

### 5.2. Emergent ML/AI-based techniques

The literature review highlighted a novel emergent trend in employing ML/AI-based techniques in forecasting, predicting, and thus preventing possible IPV incidents. While still in their infancy, the extrapolation of these results based on probability scores should always require a human-in-the-loop and a close collaboration with affected communities. It remains unclear what the appropriate (and legally justifiable) course of action should be if an ML/AI-based technique predicts the possibility of IPV as e.g., 40% or 70%. Arguably, with ML/AI-based techniques, alongside secondary (early-detection) and tertiary (impact mitigation), technologies also increasingly facilitate the possibility of primary (preventative) interventions [50].

The presence of ML/AI-based techniques should be always supervised and qualified for the right interpretation in a decision-making setting, either for the user or professionals. Furthermore, the legal framework for law enforcement and other professional services associated with IPV prevention need to be specified. There is a dearth of literature on the legal and professional role of law enforcement and other professional supportive and protective services in relation to emergent technologies, regarding how they should be used responsibly in reporting, evidence collection, and further prevention of IPV. The reviewed literature also suggests that the legal framework worldwide needs further development to incorporate the ubiquitous presence of smart environments.

### 5.3. IPV as gender-based violence

The results of our literature review suggest that the majority of the IPV-related scholarly debate investigates it through the gender-based lens. This result is in line with the review of El Morr et al. [25], who also identified 32 studies associated with women, and only 1 involved both men and women. Also in our review, only a single paper [43] investigated the IPV from the perspective of men, and none incorporated other non-binary relationships. A noticeable amount of literature mentioned by Werth [40] and Sasaki et al. [41] refer to female-to-male domestic violence. While the problem of IPV can be interpreted as a gender-based violence, it is imperative to extend the research on the role and effects of technologies in personal relationships also to non-binary and other alternative arrangements.

There is a danger of bias in the collected datasets that is being analyzed and threat-models developed for ML/AI-based techniques. For example, a large amount of variables to train artificial neural networks in order to determine domestic violence predictors used by Silva et al. [28] presume that the attacker is the husband who harmed his wife. While Werth [40] mentions the efforts of creating gender-responsive risk assessment tools, he also refers to studies that highlight underutilized research on empirical data of female crime patterns. We, however, argue that without more inclusive datasets further harm can be caused to any human being involved in domestic violence, by either not being able to detect in due time the dangers of such harm, or by ignoring the specific nuances presented by the irresponsible and harmful use of technology, before the gender-based view can be applied.

### 5.4. Fast pace of technological innovation

The fast technological development endorses quick commercialization and marketability of devices and services. For example, Mayhew et al. [26] highlight that although digital abuse may be considered advanced, increasingly their performance over the years became technologically uncomplicated, given the proliferation of networks, pervasiveness of commonplace technologies, and freely available tools. Bellini et al. [45] refer to this as *mundane technologies* (citing Dourish et al. [85]). Similarly, AirTags created by Apple since its release faces repeated criticism that it enables and empowers stalkers and other malicious actors to monitor their victims [86, 87]. Researchers from the Technical University of Darmstadt developed an smartphone app AirGuard with the purpose of reporting the presence of stalkerware devices that a user comes within reach the maintain one's privacy [88]. At the time of writing this article, the class action trial *Hughes et al v. Apple Inc.* has been filed in California against the unwarranted use of stalkerware [89].

Mayhew et al. [26] also highlight the challenges associated with the ubiquitous presence of technologies. However, the coercive control is not facilitated exclusively by (consumer) devices but the digital infrastructure. Fast network access, 5G, electric vehicles, smart home power networks, the whole inter-connected infrastructure empowers abusers, and the authors warn against the emergence of abuse-for-hire services in the future [26]. It can be argued that the fast pace of innovation somehow still circumvent the necessary ethical requirements for engineering design [90]. For example, property renting is a highly regulated business worldwide, providing sufficient protection for all tenants of a household worldwide. However, Internet access, with the provided ISP routers, are agnostic of the legal protection for Internet access for (adult) members of a household. Such a lack of legal recognition creates an imbalance between the tech-savvy household network maintainer, without any possible protection of the less technologically skilled parties. Currently, no meaningful solution exists to set up dual- or multiple admin accounts to household gateways to the Internet (i.e., home routers). The responsible design of essential home devices, along with legal assurances similar to rental contracts, would certainly empower the vulnerable partner, once elements of IPV or other forms of abusive incidents emerge.

### 5.5. Bigger picture

The purpose of this article was to provide a systematic literature review analysing the ethical challenges and opportunities of digital and smart technologies provide to the stakeholders involved in tackling domestic abuse. As delineated, domestic violence remains a grave and complex social problem affecting people of any gender, age, social status, ethnic or cultural backgrounds. The issue of domestic violence and IPV worsened during the worldwide lockdowns during the COVID-19 pandemic. Digital, online, or artificial intelligence-based smart technological services, applications, and tools provide some novel approaches in addressing domestic violence, as well as they support the various stages of support for victims. However, our results not only highlight the prevailing public health and societal issues as the leading narratives of domestic violence. They also confirm its predominant gender-based violence interpretation. Our review highlights an emerging trend for the role of ML/AI-based approaches in identifying and preventing domestic violence. However, we argue that research on the socio-technical applications for domestic violence prevention, detection, and recovery is still in early stages, resulting in little amount of recommendations available to professionals. There is a dearth of knowledge for professionals on how to use these approaches in a responsible way, and on how to respond to the phenomenon that the smartness and high-tech nature of technologies is often challenged by quicker uptake of basic-level technologies from perpetrators, creating an imbalance for professionals to tackle this issue. Overall, this knowledge gap limits an impactful development of a comprehensive socio-technical regime that serves the safety and resilience of families in their communal setting.

## Funding information

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1.

## Author contribution statement

Peter Novitzky: Conceived and designed the research; Performed the research; Analysed and interpreted the data; Contributed to the analysis; Wrote the paper.

Janine Jansen: Conceived and designed the research; Performed the research; Analysed and interpreted the data; Contributed to the analysis; Wrote the paper.

Ben Kokkeler: Conceived and designed the research; Performed the research; Analysed and interpreted the data; Contributed to the analysis; Wrote the paper.

## Data availability statement

Data included in article/supp. material/referenced in article.

## Additional information

Supplementary content related to this article has been published online at [URL].

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.heliyon.2023.e17140.

## References

[1] UN, What is domestic abuse?, (n.d.), https://www.un.org/en/coronavirus/what-is-domestic-abuse.

[2] WHO, Violence against women prevalence estimates, in: 2018: Global, Regional and National Prevalence Estimates for Intimate Partner Violence against Women and Global and Regional Prevalence Estimates for Non-partner Sexual Violence against Women, World Health Organization, 2021. https://www.who.int/publications/i/item/violence-against-women-prevalence-estimates.

[3] CoE, Convention on Preventing and Combating Violence against Women and Domestic Violence, 2011. https://www.coe.int/en/web/gender-matters/council-of-europe-convention-on-preventing-and-combating-violence-against-women-and-domestic-violence.

[4] EC, Equality: Commission Opens Public Consultation on Tackling Violence against Women and Domestic Violence, 2021. https://ec.europa.eu/info/news/equality-commission-opens-public-consultation-tackling-violence-against-women-and-domestic-violence-2021-feb-09.

[5] M. Eisner, A. Nivette, A.L. Murray, M. Krisch, Achieving population-level violence declines: implications of the international crime drop for prevention programming, J. Publ. Health Pol. 37 (2016) 66–80, https://doi.org/10.1057/s41271-016-0004-5.

[6] UN, SDG16: Peace, Justice and Strong Institutions: Promote Peaceful and Inclusive Societies for Sustainable Development, Provide Access to Justice for All and Build Effective, Accountable and Inclusive Institutions at All Levels, 2015. https://sdgs.un.org/goals/goal16.

[7] UNFICYP, Domestic Violence and COVID-19, 2020. https://unficyp.unmissions.org/domestic-violence-and-covid-19.

[8] K. Kam, The New Domestic Violence: Technology Abuse, WebMD Health News, 2020. https://www.webmd.com/mental-health/news/20201130/the-new-domestic-violence-technolog-abuse.

[9] M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, A. Dafoe, P. Scharre, T. Zeitzoff, B. Filar, H. Anderson, H. Roff, G.C. Allen, J. Steinhardt, C. Flynn, S.Ó. hÉigeartaigh, S. Beard, H. Belfield, S. Farquhar, C. Lyle, R. Crootof, O. Evans, M. Page, J. Bryson, R. Yampolskiy, D. Amodei, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, 2018, https://doi.org/10.48550/ARXIV.1802.07228.

[10] M. Gusenbauer, N.R. Haddaway, Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources, Res. Synth. Methods 11 (2020) 181–217, https://doi.org/10.1002/jrsm.1378.

[11] M.J. Page, J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, C.D. Mulrow, L. Shamseer, J.M. Tetzlaff, E.A. Akl, S.E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M.M. Lalu, T. Li, E.W. Loder, E. Mayo-Wilson, S. McDonald, L.A. McGuinness, L.A. Stewart, J. Thomas, A.C. Tricco, V.A. Welch, P. Whiting, D. Moher, The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, BMJ (2021) n71, https://doi.org/10.1136/bmj.n71.

[12] T.B. Mepham, Bioethics: an Introduction for the Biosciences, second ed., Oxford University Press, 2008. https://global.oup.com/academic/product/bioethics-9780199214303.

[13] A. Turobov, M. Chumakova, A. Vecherin, World best practices in applying mathematical and statistical crime prediction algorithms, Mezhdunarodnye Protsessy 17 (2019) 153–177.

[14] H. Al-Alosi, Fighting fire with fire: exploring the potential of technology to help victims combat intimate partner violence, Aggress. Violent Behav. 52 (2020), 101376.

[15] M.R. Decker, S. Wood, S.R. Kennedy, Z. Hameeduddin, C. Tallam, I. Akumu, I. Wanjiru, B. Asira, B. Omondi, J. Case, A. Clough, R. Otieno, M. Mwiti, N. Perrin, N. Glass, Adapting the myPlan safety app to respond to intimate partner violence for women in low and middle income country settings: app tailoring and randomized controlled trial protocol, BMC Publ. Health 20 (2020).

[16] M.R. Decker, S.N. Wood, Z. Hameeduddin, S.R. Kennedy, N. Perrin, C. Tallam, I. Akumu, I. Wanjiru, B. Asira, A. Frankel, B. Omondi, J. Case, A. Clough, R. Otieno, M. Mwiti, N. Glass, Safety decision-making and planning mobile app for intimate partner violence prevention and response: randomised controlled trial in Kenya, BMJ Glob. Health 5 (2020), e002091.

[17] C. Emezue, Digital or digitally delivered responses to domestic and intimate partner violence during COVID-19, JMIR Pub. Health Surveill. 6 (2020) 294–302.

[18] A. Grimani, A. Gavine, W. Moncur, An evidence synthesis of covert online strategies regarding intimate partner violence, Trauma Viol. Abuse (2020), 1524838020957985.

[19] I. Rodriguez-Rodriguez, J.-V. Rodriguez, A. Elizondo-Moreno, P. Heras-Gonzalez, M. Gentili, Towards a holistic ICT platform for protecting intimate partner violence survivors based on the IoT paradigm, Symmetry-Basel. 12 (2020) 37.

[20] S.K. Shah, Z. Tariq, Y. Lee, Audio IoT analytics for home automation safety, in: N. Abe, H. Liu, C. Pu, X. Hu, N. Ahmed, M. Qiao, Y. Song, D. Kossmann, B. Liu, K. Lee, J. Tang, J. He, J. Saltz (Eds.), 2018 IEEE International Conference on Big Data (Big Data), IEEE, New York, 2018, pp. 5181–5186, https://doi.org/10.1109/BigData.2018.8622587.

[21] S. Agrawal, A. Awekar, Deep learning for detecting cyberbullying across multiple social media platforms, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, pp. 141–153, 10772 LNCS.

[22] L.B. Amusa, A.V. Bengesai, H.T.A. Khan, Predicting the vulnerability of women to intimate partner violence in South Africa: evidence from tree-based machine learning techniques, J. Interpers Violence (2020), 0886260520960110.

[23] M.Á. Campos Gaviño, D. Larrabeiti López, Toward court-admissible sensor systems to fight domestic violence, in: Communications in Computer and Information Science, 2020, pp. 278–291, 1284 CCIS.

[24] L.F. Cardoso, S.B. Sorenson, O. Webb, S. Landers, Recent and emerging technologies: implications for women's safety, Technol. Soc. 58 (2019), 101108.

[25] C. El Morr, M. Layal, Effectiveness of ICT-based intimate partner violence interventions: a systematic review, BMC Publ. Health 20 (2020) 1372.

[26] J. Mayhew, H. Jahankhani, Current challenges of modern-day domestic abuse, in: Advanced Sciences and Technologies for Security Applications, 2020, pp. 267–282.

[27] E. Rituerto-González, J.A. Miranda, M.F. Canabal, J.M. Lanza-Gutiérrez, C. Peláez-Moreno, C. López-Ongil, A hybrid data fusion architecture for bindi: a wearable solution to combat gender-based violence, in: Communications in Computer and Information Science, 2020, pp. 223–237, 1284 CCIS.

[28] J. Silva, E.G. Aleman, G.C. Acuña, O.R. Bilbao, H. Hernandez-P, B.L. Castro, P.A. Meléndez, D. Neira, Use of artificial neural networks in determining domestic violence predictors, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019, pp. 132–141, 11656 LNCS.

[29] S. Subramani, S. Michalska, H. Wang, J. Du, Y. Zhang, H. Shakeel, Deep learning for multi-class identification from domestic violence online posts, IEEE Access 7 (2019) 46210–46224.

[30] I. Ucuz, A. Ari, O.O. Ozcan, O. Topaktas, M. Sarraf, O. Dogan, Estimation of the development of depression and PTSD in children exposed to sexual abuse and development of decision support systems by using artificial intelligence, J. Child Sex. Abuse (2022).

[31] M.A. Wall, A. Jenney, M. Walsh, Conducting evaluation research with children exposed to violence: how technological innovations in methodologies and data collection may enhance the process, Child Abuse Negl. 85 (2018) 202–208.

[32] K.Z. Wang, A. Bani-Fatemi, C. Adanty, R. Harripaul, J. Griffiths, N. Kolla, P. Gerretsen, A. Graff, V. De Luca, Prediction of physical violence in schizophrenia with machine learning algorithms, Psychiatr. Res. 289 (2020), 112960.

[33] D. Chitkara, N. Sachdeva, Y.D. Vashisht, Design of a women safety device, in: 2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), IEEE, New York, 2016, https://doi.org/10.1109/R10-HTC.2016.7906858.

[34] R. Gokhale, M. Fasli, Matrix Factorization for Co-training Algorithm to Classify Human Rights Abuses, 2019, pp. 2170–2179.

[35] E. Zeng, F. Roesner, Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study, in: 28th USENIX Security Symposium (USENIX Security 19), USENIX Association, 2019, pp. 159–176.

[36] A. Black, K. Lumsden, Precautionary policing and dispositives of risk in a police force control room in domestic abuse incidents: an ethnography of call handlers, dispatchers and response officers, Polic. Soc. 30 (2020) 65–80.

[37] N. Henry, A. Powell, Sexual violence in the digital age: the scope and limits of criminal law, Soc. Leg. Stud. 25 (2016) 397–418.

[38] N. Henry, A. Flynn, A. Powell, Technology-facilitated domestic and sexual violence: a review, Violence Against Women 26 (2020) 1828–1854.

[39] A. Powell, N. Henry, Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives, Polic. Soc. 28 (2016) 1–17.

[40] R. Werth, Risk and punishment: the recent history and uncertain future of actuarial, algorithmic, and "evidence-based" penal techniques, Soc. Compass 13 (2019), e12659.

[41] T. Sasaki, M. Ishii-Kuntz, Intimate partner violence: domestic violence from Japanese perspectives, in: Family Violence in Japan, 2016, pp. 79–101, https://doi.org/10.1007/978-981-10-0057-7_3.

[42] E.J. Anderson, K.C. Krause, C.M. Krause, A. Welter, D.J. McClelland, D.O. Garcia, K. Ernst, E.C. Lopez, M.P. Koss, Web-based and mHealth interventions for intimate partner violence victimization prevention: a systematic review, Trauma Violence Abuse (2019), 1524838019888889.

[43] A. Machado, D. Hines, M. Matos, Help-seeking and needs of male victims of intimate partner violence in Portugal, Psychol. Men Masc. 17 (2016) 255–264.

[44] A. Weitzman, S. Cowan, K. Walsh, Bystander interventions on behalf of sexual assault and intimate partner violence victims, J. Interpers Violence 35 (2020) 1694–1718.

[45] R. Bellini, S. Forrest, N. Westmarland, J.D. Smeddinck, Mechanisms of Moral Responsibility: Rethinking Technologies for Domestic Violence Prevention Work, 2020.

[46] R. Leitão, Digital technologies and their role in intimate partner violence, in: Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, 2018, p. src11.

[47] N. Sambasivan, G. Checkley, A. Batool, N. Ahmed, D. Nemer, L. Sanely Gaytan-Lugo, T. Matthews, S. Consolvo, E. Churchill, "Privacy is not for me, it's for those rich women": performative privacy practices on mobile phones by women in south asia, in: Fourteenth Symposium on Useable Privacy and Security (SOUPS 2018), USENIX Association, Berkeley, 2018, pp. 127–142.

[48] K. Susuki, A Newly Emerging Ethical Problem in PGIS Ubiquitous Atoque Absconditus and Casual Offenders for Pleasure, 2018, pp. 22–27.

[49] L.V. Abreu Maia, I.M. Bernardino, E.F. Ferreira, S. d'Avila, R.C. Martins, Exposure to violence, victimization differences and maxillofacial injuries in a brazilian state capital: a data mining approach, J. Public Health-Heidelberg 26 (2018) 345–353.

[50] E.J. Anderson, J. McClelland, C. Meyer Krause, K.C. Krause, D.O. Garcia, M.P. Koss, Web-based and mHealth interventions for intimate partner violence prevention: a systematic review protocol, BMJ Open 9 (2019).

[51] R. Jewkes, E. Dartnall, More research is needed on digital technologies in violence against women, Lancet Pub. Health 4 (2019) e270–e271.

[52] L. Tarzia, D. Iyer, E. Thrower, K. Hegarty, "Technology doesn't judge you": young Australian women's views on using the internet and smartphones to address intimate partner violence, J. Technol. Hum. Serv. 35 (2017) 199–218.

[53] UNSD, Guidelines for Producing Statistics on Violence against Women, United Nations, Department of Economic; Social Affairs — Statistics Division, 2014. https://unstats.un.org/unsd/gender/docs/Guidelines_Statistics_VAW.pdf.

[54] UN, The Sustainable Development Goals Report 2022, United Nations, 2022. https://unstats.un.org/sdgs/report/2022/The-Sustainable-Development-Goals-Report-2022.pdf.

[55] D. Levinson, Family violence in cross-cultural perspective, in: Handbook of Family Violence, Springer US, 1988, pp. 435–455, https://doi.org/10.1007/978-1-4757-5360-8_18.

[56] K.I. Smith, Coronavirus Doesn't Cause Men's Violence against Women, 2020. https://kareningalasmith.com/2020/04/15/coronavirus-doesnt-cause-mens-violence-against-women/.

[57] J. Martins, E. Helena, F. Keim, Epidemiological characteristics of trauma patients maxillofacial surgery at the hospital Geral de Blumenau SC from 2004 to 2009, Arq. Int. Otorrinolaringol. 14 (2014) 192–198, https://doi.org/10.7162/s1809-48722010000200008.

[58] J. Suler, The online disinhibition effect, Cyberpsychol. Behav. 7 (2004) 321–326, https://doi.org/10.1089/1094931041291295.

[59] R.L. Servance, Cyberbullying, cyber-harassment, and the conflict between schools and the first amendment, Wisoncin Law Rev. 6 (2003) 1213–1244. https://heinonline.org/HOL/P?h=hein.journals/wlr2003&i=1227.

[60] M. Cismaru, G. Jensen, A.M. Lavack, If the noise coming from next door were loud music, youd do something about it, J. Advert. 39 (2010) 69–82, https://doi.org/10.2753/joa0091-3367390405.

[61] B. Guerin, M. de Oliveira Ortolan, Analyzing domestic violence behaviors in their contexts: violence as a continuation of social strategies by other means, Behav. Soc. Issues 26 (2017) 5–26, https://doi.org/10.5210/bsi.v26i0.6804.

[62] E. Rempel, L. Donelle, J. Hall, S. Rodger, Intimate partner violence: a review of online interventions, Inf. Health Soc. Care 44 (2018) 204–219, https://doi.org/10.1080/17538157.2018.1433675.

[63] C.L. Mason, S. Magnet, Surveillance studies and violence against women, Surveill. Soc. 10 (2012) 105–118, https://doi.org/10.24908/ss.v10i2.4094.

[64] C. Fraser, E. Olsen, K. Lee, C. Southworth, S. Tucker, The new age of stalking: technological implications for stalking, Juv. Fam. Court J. 61 (2010) 39–55, https://doi.org/10.1111/j.1755-6988.2010.01051.x.

[65] V. Sandulescu, S. Andrews, D. Ellis, N. Bellotto, O.M. Mozos, Stress detection using wearable physiological sensors, in: Artificial Computation in Biology and Medicine, Springer International Publishing, 2015, pp. 526–532, https://doi.org/10.1007/978-3-319-18914-7_55.

[66] F. Saki, A. Sehgal, I. Panahi, N. Kehtarnavaz, Smartphone-based real-time classification of noise signals using subband features and random forest classifier, in: 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2016, https://doi.org/10.1109/icassp.2016.7472068.

[67] N.E. Glass, N.A. Perrin, G.C. Hanson, T.L. Bloom, J.T. Messing, A.S. Clough, J.C. Campbell, A.C. Gielen, J. Case, K.B. Eden, The longitudinal impact of an internet safety decision aid for abused women, Am. J. Prev. Med. 52 (2017) 606–615, https://doi.org/10.1016/j.amepre.2016.12.014.

[68] L. Tarzia, C. May, K. Hegarty, Assessing the feasibility of a web-based domestic violence intervention using chronic disease frameworks: reducing the burden of 'treatment' and promoting capacity for action in women abused by a partner, BMC Wom. Health 16 (2016).

[69] J. Koziol-McLain, A.C. Vandal, D. Wilson, S. Nada-Raja, T. Dobbs, C. McLean, R. Sisk, K.B. Eden, N.E. Glass, Efficacy of a web-based safety decision aid for women experiencing intimate partner violence: randomized controlled trial, J. Med. Internet Res. 19 (2018) e426, https://doi.org/10.2196/jmir.8617.

[70] R.V. Ericson, K.D. Haggerty, Policing the Risk Society, University of Toronto Press, 1997, https://doi.org/10.3138/9781442678590.

[71] U. Beck, Risk Society, Sage Publications UK, 1992. https://www.ebook.de/de/product/3241981/ulrich_beck_risk_society.html.

[72] D. Garland, The Culture of ControlCrime and Social Order in Contemporary Society, Oxford University Press, 2002, https://doi.org/10.1093/acprof:oso/9780199258024.001.0001.

[73] D. Garland, The rise of risk, in: A. Doyle, R.V. Ericson (Eds.), Risk and Morality, University of Toronto Press, 2003, pp. 48–86. https://www.ebook.de/de/product/3880460/risk_and_morality.html.

[74] M.M. Feeley, J. Simon, The new penology: notes on the emerging strategy of corrections and its implications, Criminology 30 (1992) 449–474, https://doi.org/10.1111/j.1745-9125.1992.tb01112.x.

[75] G. Mythen, S. Walklate, Criminology and terrorism, Br. J. Criminol. 46 (2005) 379–398, https://doi.org/10.1093/bjc/azi074.

[76] M. Foucault, The Birth of Biopolitics: Lectures at the Collège de France, 1978-79, Palgrave Macmillan, 2008.

[77] M. Foucault, Security, Territory, Population Lectures at the Collège de France, 1977-78: Lectures at the Collège de France, 1977-78, Palgrave Macmillan, 2009.

[78] M.B. Salter, Imagining numbers: risk, quantification, and aviation security, Secur. Dialog. 39 (2008) 243–266, https://doi.org/10.1177/0967010608088777.

[79] M. Power, Riskwork: Essays on the Organizational Life of Risk Management, Oxford University Press, 2016. https://www.ebook.de/de/product/28782544/riskwork_essays_on_the_organizational_life_of_risk_management.html.

[80] J.C. Inness, Privacy, Intimacy, and Isolation, Oxford University Press, 1996. https://global.oup.com/academic/product/privacy-intimacy-and-isolation-9780195104608.

[81] E. Gracia, Unreported cases of domestic violence against women: towards an epidemiology of social silence, tolerance, and inhibition, J. Epidemiol. Community Health 58 (2004) 536–537, https://doi.org/10.1136/jech.2003.019604.

[82] S.E. Carrell, M. Hoekstra, Family business or social problem? The cost of unreported domestic violence, J. Pol. Anal. Manag. 31 (2012) 861–875, https://doi.org/10.1002/pam.21650.

[83] E. Ruttkamp-Bloem, Epistemic just and dynamic AI ethics in africa, in: Social and Cultural Studies of Robots and AI, Springer International Publishing, 2023, pp. 13–34, https://doi.org/10.1007/978-3-031-08215-3_2.

[84] D. Bell, Communitarianism, in: E.N. Zalta, U. Nodelman (Eds.), The Stanford Encyclopedia of Philosophy, Fall 2022, Metaphysics Research Lab, Stanford University, 2022. https://plato.stanford.edu/archives/fall2022/entries/communitarianism/.

[85] P. Dourish, C. Graham, D. Randall, M. Rouncefield, Theme issue on social interaction and mundane technologies, Personal Ubiquitous Comput. 14 (2010) 171–180, https://doi.org/10.1007/s00779-010-0281-0.

[86] J. Stempel, Apple Is Sued by Women Who Say AirTag Lets Stalkers Track Victims, Reuters, 2022. https://www.reuters.com/legal/apple-is-sued-by-women-who-say-airtag-lets-stalkers-track-victims-2022-12-06/.

[87] S. Cole, Police Records Show Women Are Being Stalked with Apple AirTags across the Country, Motherboard, 2022. https://www.vice.com/en/article/y3vj3y/apple-airtags-police-reports-stalking-harassment.

[88] A. Heinrich, N. Bittner, M. Hollick, AirGuard – protecting android users from stalking attacks by apple find my devices, arXiv.org, https://doi.org/10.48550/ARXIV.2202.11813, 2022.

[89] L. Hughes, J. Doe, Hughes et al v. Apple inc. https://www.classaction.org/media/hughes-et-al-v-apple-inc.pdf, 2022.

[90] I. van de Poel, Investigating ethical issues in engineering design, Sci. Eng. Ethics 7 (2001) 429–446, https://doi.org/10.1007/s11948-001-0064-0.