Article

Not peer-reviewed version

A Smart App for the Prevention of Gender-Based Violence Using Artificial Intelligence

Agostino Giorgio *

Posted Date: 29 October 2025

doi: 10.20944/preprints202510.2228.v1

Keywords: personal safety; artificial intelligence; smartphone; smartwatch; app; gender-based violence

Article

A Smart App for the Prevention of Gender-Based Violence Using Artificial Intelligence

Agostino Giorgio

Politecnico di Bari, Bari, Italy; agostino.giorgio@poliba.it

Abstract

Gender-based violence is a widespread and persistent social scourge. The most effective strategy to reduce its impact is prevention, which has led to the adoption of a hand gesture conventionally recognized as a request for help. In addition, in cases of confirmed risk, a Judge may order the potential aggressor to wear an electronic bracelet to prevent them from approaching the victim. However, these measures have proven largely insufficient, as incidents of gender-based violence continue to recur. To address this limitation, the author developed an application, named "no pAIn app", based on artificial intelligence (AI), designed to create a virtual *shield* for potential victims. The app, which can run on both smartphones and smartwatches, automatically sends help requests with geolocation data when AI detects a real danger situation. The process is fully autonomous and does not require any user intervention, ensuring fast, discreet, and reliable assistance even when the victim cannot act directly.

Keywords: personal safety; artificial intelligence; smartphone; smartwatch; app; gender-based violence

---

1. Introduction

Gender-based violence (GBV) includes physical, psychological, or sexual aggression directed against individuals on the basis of gender, with women and girls representing the overwhelming majority of victims. Despite increasing social awareness and legal measures, GBV remains a pervasive violation of human rights and one of the most severe forms of gender inequality.

According to the European Union Agency for Fundamental Rights (FRA), one in three women in the EU has suffered physical or sexual violence at least once in her life, and one in twenty has been raped [1]. More recent data reveal that the phenomenon continues to represent a critical social emergency. In Italy, 116 women were murdered in 2020, 104 in 2021, 196 in 2022, and 120 in 2023, with approximately 70% of victims killed by their partner or former partner [2–11]. Globally, more than five women and girls are killed every hour, with more than half of the femicides committed by partners or relatives. The total number of women killed in 2022 exceeded 89,000, marking the highest level recorded in the past two decades [5].

In addition to the tragic human toll, GBV also has major socio-economic repercussions. The European Institute for Gender Equality (EIGE) estimates that gender-based violence costs the European Union around EUR 366 billion per year, with violence against women accounting for 79% of the total, or approximately EUR 289 billion [12]. These data highlight the urgent need for effective technological tools capable of supporting prevention and early intervention.

Among current strategies, one of the most recognized initiatives is the "Signal for Help", a universal hand gesture adopted worldwide to silently request assistance. However, this solution has intrinsic limitations: the signal may go unnoticed, the victim might be unable to perform it, or the act may occur in a private setting without witnesses.

There exists an electronic bracelet that potentially dangerous individuals are mandated to wear by a Judge to prevent them from approaching a potential victim but requires the victim to report a potential aggressor for a Judge to consider the case and potentially mandate the dangerous individual to wear it. However, this procedure is not always quick and effective, as victims of gender-based

 doi:10.20944/preprints202510.2228.v1

violence do not always report abusive partners. Suddenly, serious threats may also arise from individuals who are partially or completely unknown to the victim or are unsuspected, and thus unreported.

To address these challenges, the author previously proposed a hardware-based embedded system, named "no pAIn" (Never Oppressed, Protected by Artificial Intelligence Nonviolence system), which automatically detects dangerous situations through real-time AI-driven speech recognition and sends alert notifications with precise geolocation data [13]. This device operates as a "digital sentinel", a sort of electronic and fully automated digital signal-for-help signal transmitter, requiring no user interaction after activation and functioning as an invisible electronic safeguard. The "no pAIn" device is intended for use by potential victims rather than potential aggressors. The existing bracelet aims to keep the potential aggressor away from the person at risk of violence. Conversely, the new device, used by the person in danger, can be compared to a "shield" or a bodyguard, providing protection to prevent assaults.

Building upon this previous work, the present paper introduces a software-based evolution of that concept—the "no pAIn App"—which replicates and enhances the same AI functionalities within a smartphone or smartwatch application. This new solution eliminates the need for dedicated hardware, thereby improving accessibility, scalability, and user adoption. The app operates autonomously in the background, leveraging on-device artificial intelligence for voice-based risk detection and secure cloud connectivity for automated emergency notifications.

The app offers numerous advantages. First, it eliminates the need for the victim of violence to exhibit any explicit gesture or other form of help request, which they may be unable to do. Additionally, it has the added benefit of notifying help requests with exact geolocation to individuals who may be physically far from the scene of violence and thus would not be able to see a hand gesture if made. Moreover, the opportunity to have an app, as an alternative to a physical device, avoids the need to purchase and wear an additional physical device simply using the smartphone (and/or smartwatch for those who use it), which is now commonly owned and utilized. The ability to install the App on smartwatches makes its use even more appealing.

The App operates in the background, is not visible to anyone, although the currently tested version includes various notifications on the display for debugging purposes. It can be automatically executed upon the startup of the smartphone or smartwatch (host device), provided that the individual who possesses it gives consent just once.

Recent research confirms a growing interest in AI- and IoT-based systems for personal safety and violence prevention. Patel et al. (2024) conducted a systematic review of AI-powered mobile applications for women's safety, highlighting their potential for real-time risk detection [14]. Mohammed et al. (2024) explored smart wearable systems for aggression detection using multimodal sensors [15], while Fernández et al. (2025) analyzed speech emotion recognition models applied to domestic violence detection [16]. Other studies focus on the use of edge AI for real-time human safety monitoring [17] and on smartphone-based solutions combining audio and contextual data to identify aggression [18].

Despite this progress, most available applications still require manual activation or depend on limited environmental cues. In contrast, the no pAIn App operates fully automatically, offering continuous, AI-driven monitoring capable of recognizing verbal aggression patterns and issuing immediate help requests even when the victim cannot act.

The remainder of this paper is organized as follows: Section 2 describes the methods and the core features of the app; Section 3 presents its design and implementation details; Section 4 demonstrates the app's operation and test results; and Section 5 provides conclusions and directions for future developments.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 October 2025 doi:10.20944/preprints202510.2228.v1

2. Method

The "no pAIn App" functions as an intelligent virtual sentinel designed to continuously monitor the acoustic environment and autonomously recognize high-risk situations. Its overall behavior and state transitions are summarized in the flowchart below

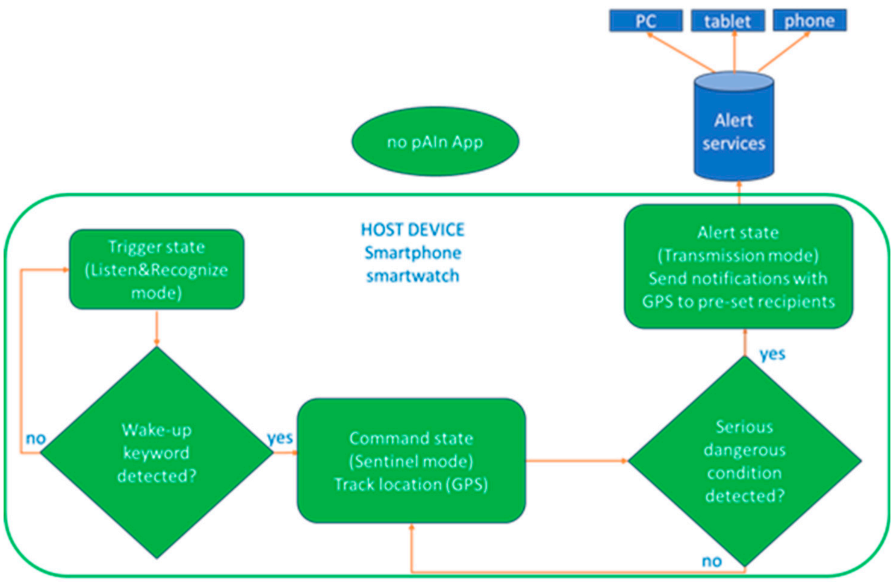

Figure 1. Flowchart of the "no pAIn App" operation.

When launched, the App enters its initial monitoring phase, or Trigger state, during which it continuously analyzes incoming audio from the host device's microphone in Listen & Recognize mode. The AI processes speech data in real time without recording or storing it, ensuring full compliance with privacy principles. The implemented neural model distinguishes between normal conversation and speech patterns indicative of potential aggression or distress.

To personalize the system, the user may define specific keywords that act as wake-up triggers or markers of danger, in addition to a set of predefined general expressions. These keywords can be individually configured and adapted according to language and personal preference. The multilingual training datasets employed during model development encompass approximately 400 hours of recordings and about 7000 labeled samples, allowing for robust classification performance across diverse acoustic conditions.

Once the AI detects a wake-up or alert term, the App transitions from the Trigger to the Command state, activating the Sentinel mode. In this phase, the App collects precise GPS coordinates directly from the smartphone or smartwatch hosting it. Modern mobile devices are equipped with advanced location technologies that integrate data from GPS, cellular networks, Wi-Fi access points, and Bluetooth Low Energy (BLE), ensuring reliable indoor and outdoor geolocation [13].

If subsequent speech analysis indicates escalating danger, the App automatically shifts to the Alert state (Transmission mode). In this state, it autonomously generates and sends emergency notifications to predefined recipients — such as trusted contacts or assistance services — via multiple communication channels (email, Telegram, Discord, or in-app alerts). Each message contains a customizable text (e.g., "Request for Help") along with real-time geographic coordinates of the person in distress.

In line with privacy-by-design principles, the App transmits only minimal data: geolocation coordinates and alert metadata. No audio samples, transcripts, or personal information are ever recorded or shared. Data transmission occurs only after explicit consent is provided by the user

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 October 2025 doi:10.20944/preprints202510.2228.v1

during the one-time setup phase, which also allows configuration of recipient contacts and activation preferences.

After initial setup, the App operates entirely autonomously, running silently in the background. All subsequent activity — from keyword recognition to notification dispatch — occurs automatically, requiring no user intervention.

The subsequent paragraph describes the architecture of the "no pAIn App."

3. App Architecture and Design

Figure 2 presents a schematic overview of the software architecture. It comprises four functional blocks that operate sequentially and interact with the host device's hardware and cloud infrastructure.

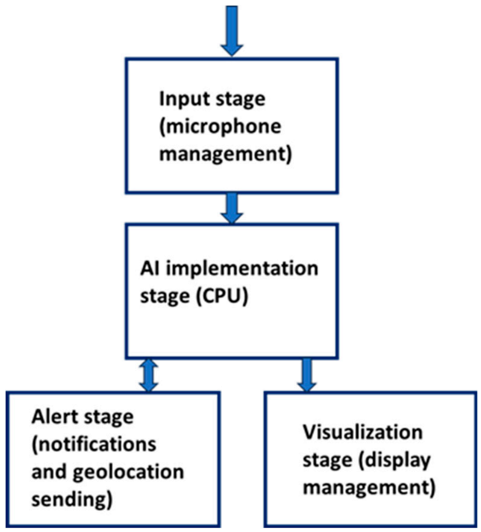

Figure 2. App architecture.

3.1. Input Stage

This module manages the acquisition of audio signals from the device's built-in microphone. It automatically configures sampling frequency and other audio parameters according to the specific terminal on which the App is installed. The input stream is continuously analyzed to extract acoustic features relevant to the AI classifier.

3.2. Artificial Intelligence Stage

The computational core of the App relies on the CPU of the host device, which executes an LSTM (Long Short-Term Memory) neural network trained for voice-based context recognition. The network can be retrained or fine-tuned to individual preferences, allowing it to identify the user's voice or custom "secret words" that trigger transitions between operational states (Trigger → Command → Alert). These personalized words, known only to the user, improve both reliability and resistance to false alarms. Even without customization, the model can still discriminate between neutral conversation and speech patterns associated with conflict or aggression.

3.3. Visualization Stage

This component handles all visual outputs and interface notifications. It is active only in the debug version of the App, where visible indicators and logs assist in testing and validation. In the release version, however, the App is designed to operate invisibly in the background, without displaying any icons or messages, ensuring discretion and user safety.

 doi:10.20944/preprints202510.2228.v1

3.4. Alert and Notification Stage

This stage manages all emergency communications. The App employs a cloud-based notification strategy, illustrated schematically below in Figure 3

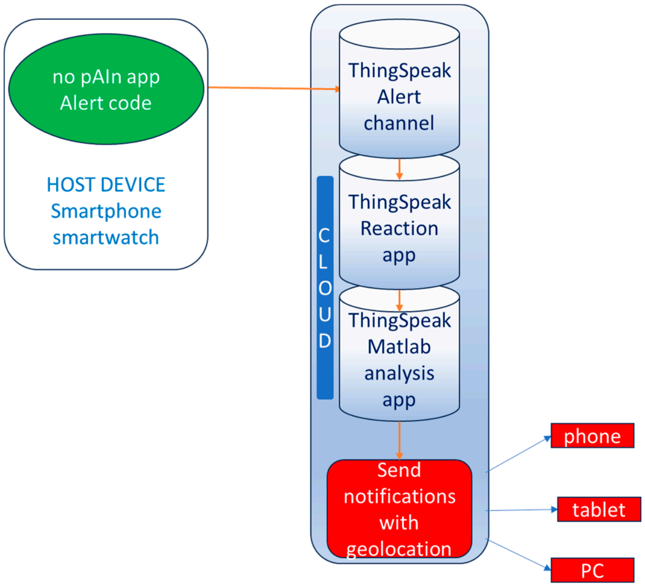

Figure 3. Diagram of the help request notification sending mode.

This block also includes the geolocation coordinate retrieval system. When the App switches from the Trigger to the Command state, it starts retrieving and updating GPS coordinates every second, storing them in a dedicated ThingSpeak cloud channel [14]. Data are transmitted via secure HTTPS connections. If the App subsequently detects an imminent threat and enters the Alert state, it sends a compact Alert Code to a designated Alert Channel on ThingSpeak using the MQTT protocol, which is particularly reliable for real-time IoT communication.

Upon receipt of the Alert Code, ThingSpeak triggers the reaction chain “Reaction – MATLAB Analysis”, as in Figure 3. The MATLAB Analysis routine retrieves the latest coordinates from the ThingSpeak geolocation channel and automatically dispatches alerts and geolocation information via HTTP(S) requests or third-party services such as IFTTT [15]. The geolocation coordinates are updated every second by the App always working in background.

This architecture provides several advantages. Delegating message delivery to the cloud minimizes the computational load and energy consumption of the smartphone or smartwatch, improves responsiveness, and ensures continuous protection. Once the Alert Code is transmitted, the App immediately reverts to Sentinel mode to continue monitoring.

If desired, additional direct-notification methods can be implemented locally within the host device processor, as previously demonstrated for the hardware-based prototype [13]. Such redundancy can further enhance reliability but should be balanced against higher energy usage and resource demand, especially in multitasking environments typical of mobile operating systems.

4. Results

The "no pAIn App" was developed in debug mode for Android and for iOS devices. and was installed and tested on both a smartphone and a smartwatch, as shown in Figure 4a and 4b, respectively.

In both cases, the App's performance was smooth and efficient. The tests conducted are highly encouraging as they reveal an extremely high accuracy in distinguishing real danger situations of

 doi:10.20944/preprints202510.2228.v1

aggression from "common" arguments or discussions that do not result in violence, as well as in sending the corresponding help requests.

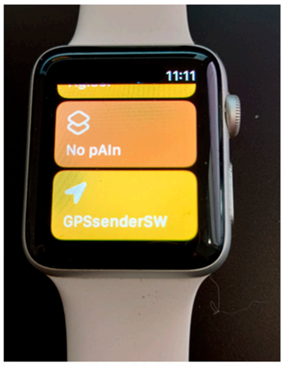

Figure 4a **Figure 4b**

Figure 4. "no pAIn App" interface 4a) on smartphone, 4b) on smartwatch.

During the testing phase, the screens of both the host smartphone and a smartphone receiving alert notifications were recorded simultaneously.

A realistic test scenario simulated a conversation gradually escalating in tone, allowing the App to demonstrate its ability to detect progressive risk signals. The app starts operating in background in "Listen&Recognize" mode, as shown in Figures 4a and 5a.

As the conversation progressed, the discussion became more heated and suspicious, prompting the woman to utter words indicating fear and anxiety (the set "wake-up" keyword was detected), thus switching the "no pAIn App" to "Sentinel" mode. In this mode, the App immediately acquires the geolocation coordinates and stores them in the cloud, updating them every second, while preparing for the potential transmission of alert notifications. The transition of the App to "Sentinel" mode (protection activated) is indicated on the display in Figure 5b. Comparing Figures 5a and 5b, it is evident that the GPS coordinates change from a value of 0.0, indicating not detected, to the actual value, signifying that the App has successfully retrieved the geolocation values in "Sentinel" state.

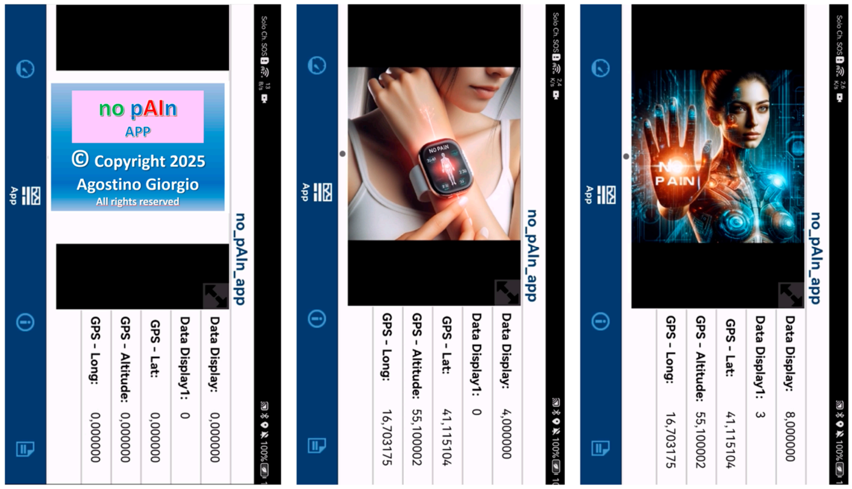

Figure 5a **Figure 5b** **Figure 5c**

Figure 5. Sequence of screenshots of the "no pAIn App" in action: 5a) in "Listen&Recognize" mode, 5b) in "Sentinel" mode, 5c) in "Help Request Transmission" mode.

Subsequently, the speech escalates to a tone that indicates severe danger according to the AI. The App switches from "Sentinel" mode to "Transmission" mode, initiating the transmission of help requests to predefined recipients, including the geolocation data.

Figure 6 displays the sequence of alerts received on a smartphone: a Telegram message via IFTTT, an email from Gmail via IFTTT, and a Discord message

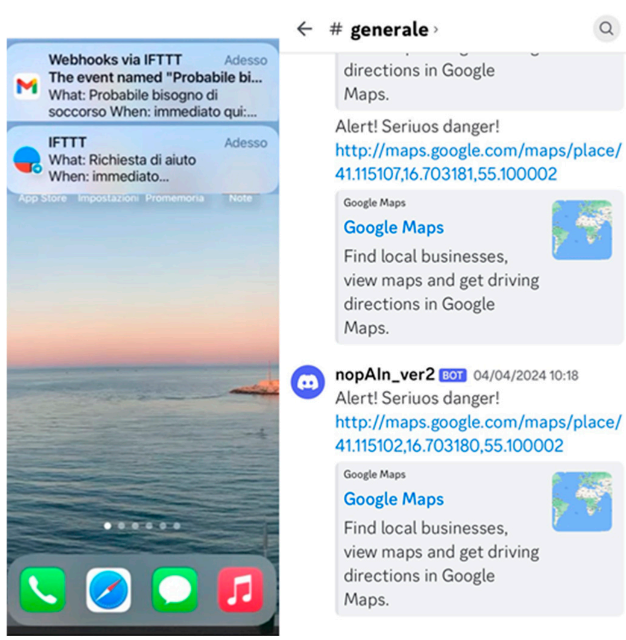

Figure 6. Sequence of receiving emergency request notifications with geolocation coordinates.

The Discord message is sent with automatic reading enabled on the receiving device. This option is very convenient to avoid the risk that the recipient of the help request might miss the notifications.

 doi:10.20944/preprints202510.2228.v1

The voice-recognition module operated with real-time responsiveness, showing no perceptible delay between speech input and system reaction. Notifications are promptly sent to the smartphone in real time as soon as the "no pAIn App" switches from "Sentinel" mode to "Transmission" mode.

Within a fraction of a second after the help request, the victim's location is identified, and potential rescuers can be immediately alerted. As a result, the "no pAIn App" demonstrates remarkable efficiency in preventing gender-based violence.

During repeated tests under different background noise levels, the AI-based classification achieved an estimated accuracy of approximately 98% in correctly identifying risk-related speech patterns, with average latency below one second from keyword detection to alert transmission

Anyway, for greater security and reliability, the app has been designed so that it can switch directly from the trigger state to the alert (transmission) mode not only following voice recognition but also through a tap on the app icon (which thus works as a "no pAIn button") or through three taps on the back of the smartphone, thereby also implementing a form of gesture-based control and rescue activation.

5. Conclusions

This article describes an app based on the use of artificial intelligence to prevent gender-based violence. The app currently stands out as original for its operational characteristics, leveraging cutting-edge technologies for the development and implementation of artificial intelligence, internet technologies, and geolocation.

The app features an exceptionally high degree of automation as it does not require any user intervention to perform its protective and preventive functions against assaults. The use of AI facilitates the early identification of risks related to domestic and gender-based violence, thus allowing for the prevention of such tragic events with a high degree of probability.

The app has been developed in debug mode, and the tests conducted show very promising results regarding the reliability of voice classification and the timely transmission of alert notifications. The most immediate design development involves optimizing the project to transition from the debug version to a release that makes the app marketable.

Although both the "no pAIn" father device and the "no pAIn App" share the same conceptual foundation—namely, the prevention of gender-based violence through artificial intelligence-based recognition of aggression and the automatic dispatch of help requests—they differ substantially in their implementation and technical architecture. The device version, described as an embedded system based on the Arduino Nano RP2040 Connect microcontroller, integrates hardware components such as an omnidirectional microphone, Wi-Fi module, optional GPS unit, and microcontroller firmware optimized for TinyML speech recognition. This design allows fully autonomous operation even without user intervention or reliance on external smart devices, making it ideal for concealed, standalone use. Conversely, the no pAIn App translates the same behavioral logic into a software environment, operating directly on the smartphone or smartwatch. It leverages the host device's built-in microphone, GPS, and communication interfaces, and executes the same finite-state control structure (Trigger–Command–Alert) entirely through software. From a technical standpoint, the app eliminates the need for dedicated hardware, external power sources, and microcontroller-level programming, while ensuring easier deployment, cost-free scalability, and continuous connectivity through mobile networks. Moreover, the app benefits from the high processing power and advanced geolocation algorithms of modern smartphones, as well as from the possibility of seamless updates and integration with existing communication apps (e.g., Telegram, Gmail, Discord). However, the embedded device offers advantages in discretion and independence from the smartphone, which may be disabled or confiscated during an assault. Overall, the app implementation represents a significant advancement in terms of accessibility, affordability, and user convenience, providing a software-based evolution of the same AI protection concept previously embodied in the physical device.

 doi:10.20944/preprints202510.2228.v1

An important area of project for future development concerns certain third-party services used by the hardware device, which could be specifically developed. The commercial prospects are also significant and could involve not only the commercialization of the app but also some services. This includes the internet services that underpin its operation (which could be specifically developed and provided by a provider) and the alert and rescue organization service. A dedicated company, for example, could handle receiving and managing help requests 24/7 and subsequently coordinate assistance requests (such as contacting the police).

It is also conceivable to have a sort of "insurance" against assaults based on the use of the “no pAIn App” and related services.

Future work will focus on the implementation of advanced multimodal recognition algorithms combining audio, motion, and physiological signals to further improve early detection and reduce false alarms.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. European Union Agency for Fundamental Rights (FRA). *Violence against Women: An EU-Wide Survey—Main Results Report*; FRA: Vienna, Austria, 2014. Available online: https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report (accessed on 24 October 2025).
2. Istituto Nazionale di Statistica (ISTAT). *Violenza sulle Donne—Il Fenomeno: Omicidi di Donne*. Available online: https://www.istat.it/it/violenza-sulle-donne/il-fenomeno/omicidi-di-donne (accessed on 24 October 2025).
3. RaiNews. *Istat: Violenza sulle Donne, Femicidi in Famiglia*. Available online: https://www.rainews.it/articoli/2022/11/istat-violenza-donne-femminicidi-famiglia-42c5e092-8d4e-44a7-85a2-b0f52801ff98.html (accessed on 24 October 2025).
4. Internazionale. *Dati e Grafici sulla Violenza di Genere*. Available online: https://www.internazionale.it/bloc-notes/giulia-testa/2019/11/25/dati-grafici-violenza-genere (accessed on 24 October 2025).
5. ANSA. *Record di Femminicidi nel Mondo nel 2022: Quasi 89.000 Donne Uccise*. Available online: https://www.ansa.it/sito/notizie/mondo/europa/2023/11/25/record-femminicidi-nel-mondo-nel-2022-quasi-89.000-donne-uccise_b3349caf-4aed-40d8-9438-01ae34fe53a0.html (accessed on 24 October 2025).
6. Sky TG24. *Femminicidi in Italia: Tutti i Dati*. Available online: https://tg24.sky.it/stories/cronaca/femminicidi-italia/index.html (accessed on 24 October 2025).
7. Elle Italia. *Dati Ufficiali sui Femminicidi 2023*. Available online: https://www.elle.com/it/magazine/women-in-society/a46517044/dati-femminicidi-2023-ufficiali/ (accessed on 24 October 2025).
8. ONU Italia. *Violenza di Genere: Dati 2023*. Available online: https://www.onuitalia.com/2023/11/24/donne-14/ (accessed on 24 October 2025).
9. Tag24. *Femminicidi in Italia: Dati ISTAT 2023*. Available online: https://www.tag24.it/946219-femminicidi-dati-istat-2023-120-donne-uccise-meta-dai-partner/ (accessed on 24 October 2025).
10. Today.it. *Femminicidi: Quanti in Italia nel 2023*. Available online: https://www.today.it/attualita/femminicidi-dati-italia-quanti-2023.html (accessed on 24 October 2025).
11. Money.it. *Quanti Femminicidi in Italia nel 2023: Numeri, Europa e Mondo*. Available online: https://www.money.it/quanti-femminicidi-italia-2023-numeri-europa-mondo (accessed on 24 October 2025).
12. *La Violenza di Genere Costa all’Europa 366 Miliardi di Euro all’Anno*; Il Sole 24 Ore, Milano, Italia, 2023.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 29 October 2025 doi:10.20944/preprints202510.2228.v1

13. Giorgio, A. *No Pain Device: Empowering Personal Safety with an Artificial Intelligence-Based Nonviolence Embedded System. Electronics* **2024**, *13*, 1766. https://doi.org/10.3390/electronics13091766.
14. Patel, S.; Khan, R.; Sharma, D. *AI-Powered Mobile Applications for Women Safety: A Systematic Review. Sensors* **2024**, *24*, 1789.
15. Mohammed, A.S.; Li, X.; Rahman, M.A. *Smart IoT Wearables for Violence Detection Using Multimodal Sensors. IEEE Access* **2024**, *12*, 112345–112360.
16. Fernández, L.; Ortega, M.; Sánchez, A. *Speech Emotion Recognition Models for Domestic Violence Detection. Comput. Methods Programs Biomed.* **2025**, *254*, 108921.
17. Rossi, T.; Bianchi, F.; Greco, D. *Edge AI for Human Safety Monitoring. Inf. Sci.* **2025**, *665*, 120437.
18. Chatterjee, K.; Singh, P.; Das, R. *Smartphone-Based Detection of Aggression Using Audio and Contextual Cues. IEEE Internet Things J.* **2024**, *11*, 13487–13499.
19. ThingSpeak Cloud Platform. Available online: https://www.thingspeak.com (accessed on 24 October 2025).
20. IFTTT Cloud Automation Platform. Available online: https://www.ifttt.com (accessed on 24 October 2025).