A Digital Communication Platform for Inter-Agency Collaboration to Manage High-Impact Domestic Abuse: Structure and Essentials

Catharina Vogt

German Police University, Criminology and Interdisciplinary Crime Prevention, Münster, Germany.
E-mail: c.vogt@respectresearchgroup.org

Abstract Interagency cooperation is a necessary response to domestic abuse to care best for victim-survivors. However, for many reasons especially pertaining data security, digital solutions to support such action remain scarce. This chapter explains what needs to be considered when installing such a tool into a network of front-line responders' activity by pointing to the advantages of digital communication platforms to manage high impact domestic abuse and summarising what IMPRODOVA researchers' expertise presented regarding the status quo of exchange of information in domestic abuse cases. Afterwards, criteria are defined that need to be fulfilled by an ICT tool set up for the management of domestic abuse by professional front-line responders. Moreover, criteria to be fulfilled by the users of the ICT tool set up for the management of domestic abuse by professional front-line responders are discussed. Finally, the stashcat® app is presented as a suitable tool meeting the before defined criteria to a great extent. This is also attested by the evaluation of the stashcat® app during its piloting by a Slovenian network of front-line responders. In sum, this chapter shows that digital solutions can assist professionals to communicate quick and effectively when supporting victim-survivors of domestic abuse.

Keywords: IMPRODOVA, domestic violence, digital support, ICT, police, social work, health sector, training

DOI https://doi.org/10.18690/978-961-286-543-6.16
ISBN 978-961-286-543-6

Introduction

Interagency cooperation is a necessary response to domestic abuse to promote victim-survivors' safety, satisfaction, and well-being. This insight is highlighted in many of the chapters of this book based on field studies with frontline responders and has also been echoed wider in scientific literature (e.g., Malos, 1997; Robinson, 2006; Vogt, 2020). While in some places in Europe such existing face-to-face cooperation networks are already considered as a best practice[1] to manage domestic abuse, digital solutions to support such action remain scarce. This is partly due to the required high level of security standards that such a tool must meet. This chapter explains the prerequisites that must be considered when installing such a tool in a network of frontline responders' activity. Especially during phases of lockdown or shutdown, such tools empower frontline responders to work in an agile and flexible mode, despite restrictions on contacts and thus to care for domestic abuse cases in a comprehensive way.

Cooperation networks aimed at managing domestic violence are understood as inter-institutional structures designed to provide a framework for working in partnership. These partnerships usually involve the police (often units specialised in domestic violence), victims' aid organisations, social services, courts and city administrations (Bradley et al., 2020) – in many cases, the police are the central figure as they deal with both victims and perpetrators, and because they have the legal mandate to intervene in matters of domestic violence and abuse. On one hand, partners of such networks bring their knowledge and expertise regarding domestic abuse cases and the respective interventions.

"This is to achieve a beneficial change for victims or a more appropriate treatment for perpetrators. The collaboration between agencies serves a greater purpose than any of the individual organisations can achieve by their specific tasks alone. Finding a common purpose, for instance, protecting and helping the victim, provides a shared mission and identity bonding various partners together" (Bradley et al., 2020, p. 6).

[1] Multi-agency risk assessment conferences (MARAC) and the Hanover Intervention Programme (HAIP), for example, are considered to be best practices (see the IMPRODOVA report by Bradley et al., 2020).

On the other hand, they also bring their organisational culture, which shapes their understanding of the domestic abuse phenomenon, the necessary action, their perception of other stakeholders involved in the management of domestic abuse, and their style of communication. In fact, whether cooperation networks can work depends on their communication. Members of such networks need to find a common ground in their communication, which includes respectful, trustful and open communication guided by strong leadership and accompanied by successful information management (Bradley et al., 2020). Thus, cooperation networks rely on complete and functional management systems including strong mechanisms for conflict prevention and resolution, as well as dedicated and competent network managers and boundary spanners. In order to facilitate inter-agency collaboration, improved rules and procedures must stimulate resource and information sharing among the participants.

Advantages of digital communication platforms to manage high-impact domestic abuse

While the need to ensure a solid information management system seems plausible in every form of collaboration, this is very important while handling domestic abuse cases (Bradley et al., 2020). In particular, the prevention of cases entailing a high risk of high-impact domestic abuse – i.e. the perpetrator's actions that that can be reasonably expected to lead to dangerous bodily injury, homicide or suicide for the victim – requires the close and fast collaboration of all frontline responders involved (Vogt, 2020). If all collaborators have carried out the necessary steps to work with one information and communication system or arranged for their own systems to properly communicate with this communication platform (e.g. feed the system with information), information on cases can be collected, shared and analysed by the collaborators. The combined exchange of information would enable collaborators to recognise victims and perpetrators faster and earlier and to monitor their trajectories more closely, for example. Sharing of information via a digital solution (taking professional confidentiality into account) would be easier and save resources for frontline responders collaborating in a network as this would give them the best way of knowing how to only share the information via the response platform instead of looking for telephone numbers, checking who is responsible etc.

Moreover, the likelihood of informed and good decisions in favour of victim-survivors thereby increases (Feld & Straus, 1989). When domestic violence cases, including background information, are quickly shared among network partners, the partners can also quickly take steps toward prevention, intervention or follow-up in line with their individual area of expertise. At best, this "avoids victims having to repeat their story several times to the succession of workers they meet: sharing a file containing what each partner needs to know – and has the right to know – about the situation being treated reduces this form of 'secondary victimization' due to being constantly re-interviewed" (Bradley et al., 2020, p. 10). Irrespective of times of pandemic or other situations where frontline responders are required to stay at home, such an information and communication technology (ICT) tool will enable the management of domestic abuse.

Besides, such a platform would also allow for the storing of content that defines the 'How' of the cooperation like policies, administrative rules, leadership, or training activities. Further, this platform could enable various groups of everyday management of first-responder personnel (e.g. police group leaders, 'silver' managers, school principals, senior physicians, departmental heads, heads of hospitals, head at other social agencies) to collaborate, and a first-responder frontline practice (e.g. patrol officers, general practitioners, paediatricians, gynaecologists, nurses, physicians at hospitals, emergency room staff, school and kindergarten teachers). If managed well, and within its regional boundaries, such a platform holds the potential to display a strong offensive against domestic abuse and strong protection for victim-survivors and their loved ones.

Exchange of information in domestic abuse cases: Status quo

According to the IMPRODOVA partners' collected insights, the status quo is that no such platform[2] is in use anywhere in their countries. Nonetheless, one can find websites[3] to obtain training tools, downloads of reports and other products.

[2] In Austria, it is planned that uniformed officers use an app integrated into the police issue smart phones that would guide through interventions in cases of domestic violence on site. This should include a short risk assessment and transfer the information directly into the case-documentation to save officers time during reporting.

[3]https://stop-violences-femmes.gouv.fr/outils-de-formation-violences-au;
http://gewaltfreileben.at/de/material/infopackage

The most elaborated system might be KANTA[4], an app used in Finland, where data recorded about all patients in healthcare services and pharmacies (and in social welfare services in the future) are saved. Information may only be shared among professionals with the consent of the (adult) patient. All data communicated between healthcare providers, pharmacies, contact points and the KANTA services are encrypted between authenticated users. Professionals use a personal smart card to sign into the information systems using strong authentication. User permissions required for different professional roles are defined by organisations. Log data are one way to monitor system usage. Besides, Finnish frontline responders use encrypted emails to share information. Only in cases of an emergency may information be shared by phone.

In other European countries, enthusiastic professionals share information with each other using services that are *not* developed for frontline responders, e.g. Google (Gmail for mailing, Drive for storage), Facebook Messenger (for communication), Dropbox (for storage), or WhatsApp. However, these tools are solely used for structuring the collaboration since no personal information regarding a case is allowed to be shared in this way. Some organisations have internal shared drives used to store and share resources (e.g. ROBOCOP); only in a few cases do they exist to enhance intra-agency cooperation.

Of course, the usual form of collaboration is the face-to-face gathering of professionals/frontline responders involved in the management of a particular case of domestic abuse. Examples of such meetings are MARACs and MATACs (e.g. Brooks-Hay et al., in this book[5]; Jaffré, 2019; Robinson, 2006). Depending on the way such a gathering is established, clients can also be present. In most of these meetings, all professionals present record the decisions and details of the meetings in their own respective databases, not a shared one. This is perceived as effective by most of the professionals because professional cultures are real hurdles, as one quote from a German interviewee shows:

> "We do not have something like an online platform for our network. It would be difficult, when it comes to the transmission of data. They

[4] https://www.kanta.fi/en/wellbeing-data
[5] The chapter on *Frontline response to high-impact domestic violence in Scotland*

> are only allowed to be sent encrypted. We have many 'online topics'. But HAIP is about regular meetings and exchange – I think that is the best. It would be nice to be connected online additionally. Nevertheless, that does not substitute one-on-one conversations that we have before or after HAIP meetings. [….] The shelter has to stay anonymous. It would be good to have something as an add-on."

Thus, it currently seems more efficient to share operational information in face-to-face meetings. However, innovation in information and communications technologies (ICT) has progressed so far that it is implausible to spare the management of domestic abuse from such arrangements (Rodríguez-Rodríguez et al., 2020). Naturally, the security architecture of the platform needs to be well considered, but this has already been ensured for other communication platforms that are designed for other purposes. Thus, the IMPRODOVA project[6] aimed to set up and pilot a national response platform.

Criteria to be met by an ICT tool intended to manage domestic abuse by professional frontline responders

Generally speaking, the envisioned ICT platform should be a digital solution that is well displayed on PCs, tablets and smartphones, and grants access to different stakeholder groups of frontline responders. On this platform, individual networks should have a closed space. The platform should allow for information to be shared in various ways like uploading, storing, changing, and downloading resources (e.g. external memory of the network, wiki, address book). At the same time, this platform should provide access to the training materials collected during the IMPRODOVA project[7]. Most importantly, the platform would need to have a solid security architecture. Legal issues would also have to be considered because such a platform would need a high level of moderation to comply with General Data

[6] All articles in this edited book are written in the context of the project *Improving Frontline Responses to High Impact Domestic Violence (IMPRODOVA)*. This EU-project is designed to provide solutions for an integrated response to high-impact domestic violence, based on comprehensive empirical research of how police and other frontline responders (e.g. medical and social work professionals) respond to domestic violence in European countries. Project website: www.improdova.eu.

[7] https://training.improdova.eu/en/. See also chapter on *Development of a training platform on domestic violence* by Bettina Pfleiderer and Paulina Juszczyk in this book.

Protection Regulations (GDPR)[8] and privacy rights as well as laws governing e.g. medical practices.

Given that usability and use-value depend on the platform's simplicity and its immediacy, with which it responds to practitioner needs, the guiding question for the set-up is: How should the communication or 'response' platform be constructed so that FLR are likely to actually use and benefit from it? To answer this question, the IMPRODOVA team conducted an internal workshop and an internal survey drawing from the rich background of the experienced practitioners and academic experts involved in the project (mostly law enforcement authorities). Six themes emerged: objective of usage, functions, usability, IT system, safety measures, and further demands to be met by the ICT tool for it to become usable by police.

Objective of usage

Altogether, there was considerable agreement on the demand to share information and documentation concerning domestic abuse cases. The platform should aim to support the communication in various communities of professionals. In Austria, with regard to victims' support groups in hospitals, the demand for a platform to communicate with other victim support groups was mentioned.

Functions

Multiple functions the platform should offer were named: The platform should allow the users to upload and share photos, documents, images. It should enable them to invite other professionals. It should offer modalities for open and hidden forums. It should be designed to avoid duplicated efforts to avoid the need to enter information in one system and then copy the same content into another[9]. Date and time, changes to documentation etc. would also need to be visible to everyone so that everybody is constantly up to date and can see who has made changes to a specific case.

[8] https://gdpr-info.eu/

[9] However, this is more a question of how the platform is integrated into the work of frontline responders' networks and (if the platform covers typical functions of messaging and data storage) less a question of the platform's functions.

Usability

Usability and use-value depend on the platform's simplicity and the immediacy with which it responds to practitioner needs. The platform should thus be intuitive, easy to use, visually clear, and logically organised. In addition, entering the data should be simple, straightforward and trustworthy (e.g. no need to enter the same data several times due to problems with Internet access).

IT system

The IT system behind the platform must ensure that all connected processes run smoothly; the platform should run fast on a computer or mobile device. It must be able to run in operating systems, be optimised for most ICT tools (especially smart phones), and be downloadable from the App Store and Google Play. Naturally, it should ensure real-time communication among users – who can then ask questions from other users in the case of an emergency or professional uncertainty. Thus, it must be accessible from everywhere and might also create a mirror of the site as an app. In this way, the contents could be accessed offline.

Safety measures

In terms of domestic abuse management and capacity-building, it is inevitable that all ICT solutions maintain the highest digital security simplicity in order to protect the victim-survivors whose data are being processed (Rodríguez-Rodríguez et al., 2020). Safety measures must ensure the data is protected from destruction or corruption due to an attack or other threats. Confidential data in particular must be protected from disclosure due to intrusion or phishing. With regard to the platform, one measure towards meeting this goal is that the platform must encrypt the data stored on it.

Equally, to protect the data stored on the platform, the server must be located in the European Union. Since the data generated or shared via this platform are European and subject to European law, and as the project using the platform is a European one, European security measures have to be applied.

The architecture with respect to who grants the right(s) of use or access to the platform to the different professionals is a primary concern: The platform must be secure in a general sense, such that it cannot be accessed in an unauthorised way. This means authentication is required. Users can run the platform only if it is password-protected. The uploading and sharing of information should also require registered user accounts. Namely, every frontline responder needs their own account to see who has made changes in the system (adding new information etc.). This will allow for better moderation and should require registered users to sign terms of use. The architecture should include a legal disclaimer providing clear guidance on which information to (not) share. At the same time, different safety measures might be related to different functions of the platform and thus the architecture should define who is moderating comments or who is allowed to post information. Related to this, access rights must be defined clearly, including a precise description of the different roles like moderator, user or guest. Still, it should be considered, if it is possible, to also anonymise certain users because anonymity might encourage shelters to become involved in inter-agency cooperation.

Further demands to be met by the ICT tool for it to be usable by the police

When it comes to including the police as frontline responders in the use of such an ICT tool, still more barriers must be overcome. From the view of European police organisations[10], such a platform must be organised to guarantee digital safety and security: One stakeholder has to host the data, ensure its safety etc. and must organise the way stakeholders can access folders and alter different files. The ICT tool must also be used outside of the secure police information system (e.g. access could be arranged through a secured Internet browser). If the system is security-audited by the Police ICT unit, then it is possible to use it inside the secure police information system.

Internal IT-security measures for law enforcement may prove to be significant barriers to accessing the mentioned ICT platform. Such an ICT platform would be far easier to access if it is accessible as a website rather than being a dedicated app. Even if access to this website may be restricted through police computers, officers may choose to use their personal smartphones.

[10] Information retrieved by the IMPRODOVA partners.

However, the content and information exchanged on such a platform is the most critical barrier to law enforcement practitioners becoming involved in such a networked ICT tool. It is hardly realistic to expect the police to share information on cases on a platform with other frontline responders. Instead, they could use it to obtain information, such as practical advice, protocols and usual case scenarios.

Criteria to be met by users of the ICT tool established for the management of domestic abuse by professional frontline responders

First of all, the ICT tool has to be used within a framework of professional frontline responders cooperating on the management of domestic abuse. It is preferable that most of them have already cooperated as a network and then shifted parts of their communication from face-to-face to virtual. On the strategical level, these already established boards or networks or platforms for managing professionals of different FLR fields should have together planned the mechanisms, care paths and resources before the digital cooperation commences. Participants of these boards should know each other from regular (e.g. quarterly) meetings. Still, sharing information on a platform or during a meeting is not the same and the processes are quite different. Thus, the question concerns need, confidence and trust in the way information is shared. Law, rules or a memorandum of understanding can support different types of processes. They are easier to determine and design for meetings.

Moreover, cooperation networks must possess a complete and functional management system that includes strong mechanisms for conflict prevention and resolution, as well as dedicated and competent network managers and boundary spanners. Hence, when it comes to the different roles users can have, the most essential one is that of the moderator. One might propose that the management level must include one person from every profession and the person who is guiding the process should be someone from a women's office etc. not involved in the everyday practice of handling a case of domestic abuse[11]. Since cooperation on the daily practical level needs a managerial level that is supported by an agreement and managerial functions (strategy setting, supervision, quality assurance, assessment), the requirement of dedicated and competent network managers of the response

[11] For example, this is the case of the Hannover Intervention Programme (HAIP) as described by Bradley and colleagues (2020).

platform may mean that its manager(s) should have training and experience in multi-agency cooperation, management, domestic violence as well as maintenance of a platform. Moderators of groups therefore must have the rights and opportunities and also the will to prevent and resolute, for example by setting up rules, giving access to the communication and addressing inappropriate user behaviour.

Likewise, conflict prevention and resolution should primarily be achieved by proper moderation and review of the contents provided on the ICT-enabled platform as well as the moderation of all forums and communication taking place on the platform. The central approach to achieve this should entail a combination of open access to viewing all information, combined with registration and moderation for all uploads or shared contents.

Second, cooperation networks in the realm of domestic abuse management need to involve the three areas of frontline response, i.e. the regulatory level, the everyday management of first responder personnel, and the frontline practitioners. This should also be reflected in the ICT platform. To represent the *regulatory level*, written directions and care paths can be made available on the platform. Parallel to this, the regulatory level (e.g. ministries) could be informed about the platform with a user's guide to the platform. Still, it must be considered that NGOs often *do not have regulatory levels* while the police and the medical profession are organised rather hierarchal and have to stick to their legal codes. Further, their everyday practice is structured by federal working instructions. Accordingly, the *everyday management of first responder personnel* might have a user account on the platform to be able to oversee the work of their staff using the platform. Nonetheless, it is the group of *frontline practitioners* who would and should be the end-users of such a platform in the sense described above. In order to serve their needs best, they should be involved in designing the platform. For example, all participating practitioners' contact information should be available on the platform along with resources like training materials or minutes of strategy meetings.

The third important point concerns the legal framework conditions: Within the context of domestic abuse, the platform clearly requires a high level of moderation to comply with privacy rights as well as laws governing medical practices. The platform therefore must cover data safety and GDPR issues to ensure the restricted sharing of protected (or confidential) data between professionals. Safety measures

could be defined by clarifying the role of each stakeholder group, for example by determining what each sector is able to actively share or passively retrieve from the system.

The stashcat® App

During the course of the IMPRODOVA research, the stashcat® app emerged as a useful tool to present the technical background of the digital communication platform for inter-agency collaboration to manage high-impact domestic abuse. stashcat® is a GDPR-compliant highly secure messenger with an integrated file storage, videoconferences, calendar and survey tool[12]. In order to test whether the stashcat® app would meet the requirements to serve as a communication platform for frontline responders active in the field of high-impact domestic abuse, the six themes of necessary requirements we defined above (objective of usage, functions, usability, IT system, safety measures, and further demands to be met by the ICT tool for it to be usable by the police) formed the standard against which the stashcat® app was compared. The following information was retrieved from the stashcat® flyer (stashcat® GmbH, n.d. b), the stashcat® handbook (stashcat® GmbH, n.d. a), the stashcat® website[13] and the stashcat® app.

Objective of usage

stashcat® is a messenger designed to serve organisations in their communication by combining typical functions of messengers (single chats and channels/groups) and personal file storage. File storage is also possible in channels and conversations.

Functions

Accordingly, the uploading and sharing of documents is possible in stashcat®. External links to documents can be shared with non-members as well. A synchronising function automatically synchronises local folders with the respective stashcat® folders.

[12] https://stashcat.com/en/
[13] Ibid.

Administrators are able to invite other external persons to stashcat®. Granting access to guest users is possible, too. Within stashcat®, users can invite each other to channels. Modalities for open and hidden forums exist in the form of public channels (accessible to every user), password-protected channels (for invited users or users who enter the correct password) and encrypted channels (hidden channels that cannot be found by search). The date and time of activities are always visible. Other functions include a contact book, calendar, survey function, voice and video calls as well as video conferencing.

Usability

Usability and use-value must be estimated by the frontline responders who use the platform (results are published by Juszczyk and Pfleiderer, 2021, and summarised below). From a general point of view, it can be stated that stashcat® is easy and intuitive to use. If questions arise, they can be answered by using the clearly structured stashcat® handbook (stashcat® GmbH, n.d. a).

IT system

The IT system and its processing in everyday practice need to be estimated by the frontline responders who use the platform (results are published by Juszczyk and Pfleiderer, 2021 and summarised below). stashcat® runs on Android and iOS, and can be downloaded on the App Store or Google Play.

Safety measures

The stashcat® app meets the highest standards of digital security in order to protect the data being processed (stashcat GmbH, n.d.[14]):

> The deployment of stashcat® takes place centrally on encrypted, redundant servers, which are operated by the MIVITEC GmbH in a high security centre in Munich, Germany. Frequent, automatic online backups avoid the loss of data through hardware failure, virus attacks or act of nature. [….] All relevant data is secured through the latest

[14] https://stashcat.com/en/technology

> SLL encryption methods in a second step. The protection takes place based on a 256-bit AES SSL/TLS encryption on the way to our servers and encrypts the data exchange between the server and terminal device. In a third step, an encryption on the user's terminal device takes place where the data is encrypted through a combination of AES and RSE algorithms. For the encryption with AES a key length of 256 bit is used while for the RSA encryption a key length of 4096 bit is employed. In this way we can ensure that neither unauthorized third parties nor the stashcat® team itself can decrypt or access any data. All relevant data is thus transmitted encrypted on the way to and from the server and stored there also encrypted. Encryption applies to all types of data, i.e. it includes all messages, comments and other text fields.

Further, chats can be masked before the user has left the application.

The app can only be accessed in an authorised way via invitation and authentication and the app can only be opened using a pin-code. Likewise, the uploading and sharing of information requires registered user accounts. User roles with individual authorisations are defined by the administrator of an organisation using stashcat® by creating individually defined permissions.

Further demands to be met by the ICT tool for it to be usable by the police

Among others, the stashcat® app was designed especially for government agencies[15]. Although stashcat® is hosted in Germany, it is also possible for organisations to host it on the premises of their own datacentre. Finally, the stashcat® environment is accessible as a website and also as a dedicated app and can thus be used outside of the secure police information system.

[15] https://stashcat.com/en/sectors/government-agencies, https://stashcat.com/en/references/nimes-police-department-lower-saxony

Evaluation of the stashcat® App

Regarding the technical point of view, overall the stashcat® app *in theory* satisfies all the criteria defined above as necessary to serve as a solid tool to manage domestic abuse by a network of professional frontline responders. With respect to the *practical application* of stashcat®, the tool was piloted by a Slovenian inter-agency network of professional frontline responders managing domestic abuse. The piloting team contained ten members of the local police, three members of the national-level police, six social workers and two additional coordinators from social work in the Murska Sobota area. The piloting team intended to use stashcat® to exchange critical information on actual cases and thus operated in a stashcat® environment separate from the IMPRODOVA researchers. For the evaluation, the piloting team completed an online survey provided by IMPRODOVA researchers (Juszczyk & Pfleiderer, 2021). The survey focussed on the usability and quality of stashcat® and led to a set of recommendations. Along with the stashcat® app, an accompanying webpage[16] providing training materials with regard to domestic abuse management in the Slovenian language was evaluated (for more details, see Jyszczyk & Pfleiderer, 2021).

In general, stashcat® received a positive rating from the respondents. Respondents reported that stashcat® was on average straightforward to use, information was easy to locate and that its functions were working as expected and easy to understand. In this respect, however, police officers rated the survey items more positively than social workers. It seemed that stashcat® was running less smoothly on the social workers' devices or at least that they had other reasons for their difficulties in using it. Nonetheless, both groups of professionals on average provided positive feedback on the usability of stashcat® for domestic violence risk assessment, support delivery, victim protection and collaboration. Police officers and social workers stated that they perceived stashcat® as secure, innovative and appealing to work with. Their communication as a piloting team was also perceived as trusting, respectful and constructive.

[16] https://www.fvv.um.si/improdova/

Recommendations pertaining the use of stashcat® were that all institutions involved should (beforehand) meet at joint events to agree on objectives and exchanged content. Jusczcyk and Pfleiderer (2021, p. 12f) note that "… a focus should be put on the points where individual services connect in order to help victims of domestic violence. Especially frontline responders from the social sector would benefit from such a preparatory meeting. In addition, it should be checked whether it is technically possible to have more options to adapt the app to the frontline responders' personal needs and requirements".

To sum up, the technical criteria of stashcat® support its use as a tool for inter-agency collaboration in cases of domestic abuse. Still, its implementation must always consider the human factors and especially users' needs, and integrate them accordingly.

Conclusion

Digital solutions feature among the top achievements of the twenty-first century, as do apps and technology designed to support victim-survivors of domestic abuse (e.g. Finn & Atkinson, 2009; Hassija & Gray, 2011). Software and apps to support the coordinated action of frontline responders have, however, been missing. The stashcat® app is a first step towards rectifying this gap and comprehensively working to support victim-survivors' safety and well-being.

References

Bradley, L., Brooks-Hay, O., Burman, M., …, & Vogt, C. (2020). *Identifying gaps and bridges of intra- and inter-agency cooperation.* https://improdova.eu/pdf/IMPRODOVA_D2.4_Gaps_and_Bridges_of_Intra-_and_Interagency_Cooperation.pdf?m=1585673383&

Feld, S. L. & Straus, M. A. (1989) Escalation and desistance of wife assault in marriage. *Criminology.* 27 (1), 141-162. DOI: 10.1111/j.1745-9125.1989.tb00866.x.

Finn, J., & Atkinson, T. (2009). Promoting the safe and strategic use of technology for victims of intimate partner violence: Evaluation of the technology safety project. *Journal of Family Violence, 24*(1), 53-59.

Hassija, C., & Gray, M. J. (2011). The effectiveness and feasibility of videoconferencing technology to provide evidence-based treatment to rural domestic violence and sexual assault populations. *Telemedicine and e-Health, 17*(4), 309-315.

Juszczyk, P., & Pfleiderer, B. (2021). *Assessment of the National Response Platform Pilot.* https://improdova.eu/results/reports/index.php

Malos, G. H. E. (1997). Inter-agency initiatives as a response to domestic violence. *The Police Journal*, *70*(1), 37-45.

Robinson, A. L. (2006). Reducing repeat victimization among high-risk victims of domestic violence: The benefits of a coordinated community response in Cardiff, Wales. *Violence Against Women*, *12*(8), 761-788.

Rodríguez-Rodríguez, I., Rodríguez, J. V., Elizondo-Moreno, A., Heras-González, P., & Gentili, M. (2020). Towards a holistic ICT platform for protecting intimate partner violence survivors based on the IoT paradigm. *Symmetry, 12*(1), 37. https://doi.org/10.3390/sym12010037

stashcat® GmbH (n.d. a). *Manual for using stashcat®®. Version 3.27*. https://stashcat®.com/fileadmin/user_upload/emailassets/stashcat®-Handbuch_EN.pdf

stashcat® GmbH (n.d. b). *The secure messenger with file storage for mission critical authorities*. Information flyer.

Vogt, C. (2020). Interagency Cooperation. *European Law Enforcement Research Bulletin*, 19, 153-163. https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/412