



GHID DE INTERVENȚIE ÎN CAZURILE DE VIOLENȚĂ CIBERNETICĂ



2021

GHID DE INTERVENȚIE ÎN CAZURILE DE VIOLENȚĂ CIBERNETICĂ

adresat profesioniștilor din domeniul social care lucrează cu
persoanele afectate de violență sexuală și de gen

Material realizat în cadrul proiectului TECH-WISE, RISK-FREE,
implementat de Fundația Sensiblu

Finanțat prin programul Voices against Violence: The GBV
Initiative al Vital Voices Global Partnership USA

Colectivul de autori:

Cristina Horia, Asistent social principal, Președintă a Fundației Sensiblu

Claudia Bădica, Psihoterapeută

Ecaterina Avârvarei, Mediator social

Manuela Nicolae-Pîndaru, Asistent social principal

Mirela Bărbușoiu, Avocată

Despre Fundația Sensiblu

Înființată în anul 2002, Fundația Sensiblu este o organizație non-guvernamentală din România care promovează drepturile omului și egalitatea de gen. Se implică în susținerea cauzei persoanelor afectate de violență sexuală și de gen prin servicii directe de consiliere, campanii de awareness, lobby&advocacy pentru îmbunătățirea legislației. Contribuie la creșterea calității serviciilor sociale din România prin programe de formare în domeniul violenței sexuale și de gen pentru profesioniști care oferă servicii specializate.

Despre Vital Voices Global Partnership

Vital Voices Global Partnership a fost înființată în 1997, cu misiunea de a identifica, investi și aduce vizibilitate femeilor extraordinare din întreaga lume, dezlănțuind potențialul lor de leadership pentru a transforma viețile și a accelera pacea și prosperitatea în comunitățile lor. Organizația investește în femei lideri care rezolvă cele mai mari provocări ale lumii - de la violența de gen la criza climatică, inegalitățile economice și multe altele, identificându-i pe cei cu o viziune îndrăznească asupra schimbării și colaborând cu aceștia pentru a transforma această viziune în realitate. În ultimii 24 de ani, au construit o rețea de 18.000 de factori de schimbare în 182 de țări, fiecare îndrăznind să contribuie la crearea unei lumi mai echitabile pentru toți.

Opiniile exprimate în publicație sunt responsabilitatea exclusivă a autorilor. Ele nu reflectă neapărat punctele de vedere sau opiniile Vital Voices sau ale membrilor personalului acestuia.

Cuprins		7. MĂSURI DE CREȘTERE A SIGURANȚEI ÎN MEDIUL ONLINE	75
		Parolele	77
GHID DE INTERVENȚIE ÎN CAZURILE DE VIOLENȚĂ CIBERNETICĂ	1	Managerul de parole / password manager	78
Ghid de intervenție în cazurile de violență cibernetică	3	Autentificarea cu doi factori / în doi pași	79
1. INTRODUCERE	7	Geolocalizarea	79
2. VIOLENȚA SEXUALĂ ȘI DE GEN	13	Navigarea pe internet în siguranță	81
2.1. DEFINIȚIE	15	Siguranța în social media	83
2.2. FORME DE MANIFESTARE	16	Sexting, Tinder și viața reală	85
2.3. VIOLENȚA DOMESTICĂ	18	Sexting în siguranță	85
3. MEDIUL ONLINE, FACILITATOR AL VIOLENȚEI SEXUALE ȘI DE GEN.		Tinder și aplicațiile de online dating	85
VIOLENȚA CIBERNETICĂ	21	Din online în viața reală	86
3.1. MEDIUL ONLINE, FACILITATOR AL VIOLENȚEI SEXUALE ȘI DE GEN	23	8. DOCUMENTAREA ABUZULUI ÎN MEDIUL ONLINE	89
3.2. VIOLENȚA CIBERNETICĂ	27	9. PROCEDURI ORGANIZAȚIONALE PENTRU CREȘTEREA SIGURANȚEI	93
3.2.1. DEFINIȚIE	27	Securitatea spațiului în care se desfășoară activitatea	
3.2.2. FORME DE MANIFESTARE	29	de consiliere/găzduirea	95
3.2.3. VIOLENȚA CIBERNETICĂ ȘI DREPTURILE OMULUI	38	Securizarea echipamentelor	96
3.2.4. LEGISLAȚIA ÎN ROMÂNIA	40	Dosarele și datele beneficiarelor	97
4. COMPORTAMENTUL AGRESORULUI ÎN MEDIUL ONLINE.		Comunicarea în siguranță cu beneficiarele	97
SPECIFICITĂȚILE VIOLENȚEI CIBERNETICE ÎN CAZUL RELAȚIILOR INTIME	45	Comunicarea la telefon	98
4.1. AGRESORUL ȘI MOTIVELE LUI	47	Comunicarea prin mesaje	98
4.2. COMPORTAMENTUL AGRESORULUI	48	Comunicarea prin e-mail	98
4.3. SPECIFICITĂȚILE VIOLENȚEI CIBERNETICE		Comunicarea în social media	99
ÎN CAZUL RELAȚIILOR INTIME	50	Comunicarea video	99
5. IMPACTUL ASUPRA VICTIMELOR	53	Grupurile online	100
6. INTERVENȚIA PSIHO-SOCIALĂ ÎN CAZURILE DE VIOLENȚĂ CIBERNETICĂ	59	10. SECURITATEA ȘI STAREA DE BINE A PROFESIONIȘTILOR	
6.1. TRAUMA ȘI IMPACTUL ASUPRA SUPRAVIEȚUITOARELOR	61	CARE LUCREAZĂ CU CAZURI DE VIOLENȚĂ	103
6.2. ABORDAREA CENTRATĂ PE SUPRAVIEȚUITOR*	62	11. Bibliografie și resurse	109
6.3. EVALUAREA CAZURILOR DE VIOLENȚĂ	67	PLAN DE SIGURANȚĂ - MĂSURI DE CREȘTERE A SECURITĂȚII	
6.3.1. EVALUAREA RISCULUI	69	PERSOANELOR AFECTATE DE VIOLENȚĂ DOMESTICĂ	113
6.3.2. PLANUL DE SIGURANȚĂ	71		
Scopurile întocmirii planului de siguranță	71		
Pașii planului de siguranță	72		
Securitatea digitală, parte a planului de siguranță	73		

INTRODUCERE



Violența sexuală și de gen este un fenomen cu impact negativ semnificativ asupra individului, comunității și societății în ansamblu, care subminează bunăstarea socială, economică, psihologică, spirituală și emoțională a victimei. Orice persoană, indiferent de vârstă, sex, gen, etnie, culoare, limbă, religie, orientare sexuală, stare de sănătate, dizabilitate, stare civilă, statut legal poate fi afectată de violența sexuală și de gen.

Anumite categorii de persoane sunt mai vulnerabile decât altele, cum ar fi fetele și femeile, persoanele cu dizabilități, persoanele aparținând anumitor grupuri minoritare, etnice, religioase și sexuale.

Pandemia de COVID-19 a reprezentat un nou factor de stres, care a condus la o intensificare a abuzurilor în viața reală, cu atât mai mult cu cât cuplurile, familiile, au petrecut mai mult timp împreună, fie în starea de urgență, fie în perioada de carantinare.

Conform Inspectoratului General al Poliției Române, în anul 2020 s-au înregistrat 26 809 loviri sau alte violențe, 80% dintre acestea fiind orientate împotriva femeilor și fetelor, la fel ca și 94% dintre violuri. Comparativ cu 2019, în 2020 a crescut cu 30% numărul de agresiuni sexuale și acte sexuale cu fete minore.

Odată cu creșterea timpului petrecut pe internet, social media și aplicații, utilizând dispozitivele tip smartphone, laptop, desktop, tabletă, pentru școală, timp liber sau serviciu, a crescut și vulnerabilitatea utilizatorilor în fața atacurilor cibernetice și a agresorilor și prădătorilor sexuali.

Accesarea fără permisiune a conturilor de e-mail și social media, citirea mesajelor, postarea și trimiterea de mesaje în numele victimei, instalarea unor aplicații de urmărire pe telefonul mobil, montarea unor dispozitive de urmărire pe mașină și a unor dispozitive de ascultare în locuință, sunt doar câteva dintre tehnicile identificate de supraviețuitoare ca fiind folosite de partenerii agresivi pentru menținerea controlului în relație, chiar și după încheierea acesteia. Diversitatea și complexitatea abuzului prin intermediul tehnologiei, lipsa informațiilor despre metodele de securizare, precum și dificultatea strângerii dovezilor pentru a cere sprijin, le descurajează pe supraviețuitoare să solicite ajutor și să se protejeze.

Siguranța, inclusiv online, este primordială în lucrul cu supraviețuitoarele violenței sexuale și de gen, iar sarcina specialiștilor care le oferă servicii este de a realiza o evaluare a riscurilor digitale și de a integra în intervenție utilizarea în mod responsabil și sigur a internetului, a social media și a tehnologiei. Este necesară o intervenție complexă și individualizată, realizată în funcție de obiectivele și nevoile persoanelor abuzate.

Prezentul ghid abordează violența cibernetică ca formă de violență sexuală

și de gen și vine în ajutorul profesioniștilor din domeniul social care oferă servicii specializate persoanelor aflate într-o situație de violență. Conține informații referitoare la violența sexuală și de gen în mediul online și offline, familiarizează specialistul cu mediul online și îi oferă cunoștințele și instrumentele care îl pot ajuta în munca lui cu persoanele afectate de violență sexuală și de gen. De asemenea, oferind modele de bună practică, ghidul vine în întâmpinarea organizațiilor care își propun abordarea în intervenție a acestei forme de violență și au nevoie de suport pentru dezvoltarea procedurilor și instrumentelor de lucru.

Ghidul a fost elaborat în cadrul proiectului TECH-WISE, RISK-FREE, implementat de Fundația Sensibilu în programul Voices against Violence: the GBV Global Initiative al organizației Vital Voices Global Partnership.

Proiectul TECH-WISE, RISK-FREE a fost implementat în perioada noiembrie 2020 - octombrie 2021 și s-a adresat profesioniștilor care oferă servicii specializate persoanelor afectate de violență sexuală și de gen, în mediul public sau privat. Proiectul a venit într-un context pandemic în care comunicarea directă, față-în-față, a pierdut teren în fața celei mijlocite de echipamente tip smartphone, laptop, tabletă, a internetului și a aplicațiilor, iar vulnerabilitatea utilizatorilor în fața atacurilor în mediul online a crescut proporțional cu timpul petrecut în spațiul virtual și interacțiunile avute, numărul aplicațiilor și al dispozitivelor utilizate.

În cadrul proiectului a fost realizată o cercetare pe tema violenței cibernetice - *Cercetare privind nivelul de conștientizare a riscurilor digitale*, atât în rândul profesioniștilor, cât și al persoanelor afectate, la care au răspuns 103 specialiști și 70 de supraviețuitoare ale violenței sexuale și de gen, având ca scop:

- *identificarea provocărilor cu care specialiștii s-au confruntat în intervenția în aceste cazuri, impactul pe care utilizarea tehnologiei îl are asupra profesiei lor, a organizației/instituției în care lucrează și asupra beneficiarelor cărora le furnizează serviciile*
- *identificarea eventualelor situații de abuz online și prin intermediul tehnologiei pe care supraviețuitoarele le-au experimentat în relația lor, a provocărilor cu care s-au confruntat în utilizarea tehnologiei, a internetului și a platformelor social media, precum și a ceea ce le-ar fi fost de ajutor dacă s-ar fi aflat într-o astfel de situație*

Răspunsurile au fost aprofundate în cadrul a 3 focus-grupuri, atât cu supraviețuitoare, cât și cu profesioniști. Rezultatele cercetării și al focus-grupurilor, disponibile și pe site-ul www.fundatiasensibilu.ro, au arătat că atât supraviețuitoarele, cât și profesioniștii, nu țin pasul cu evoluția tehnologiei, tot timpul apare ceva nou, fie că sunt aplicații utile, fie că sunt viruși și amenințări. Respondentele au menționat că agresiunile din spațiul virtual le-au erodat încrederea în ceilalți, dar retragerea din online nu este o

soluție, ci e nevoie de educație digitală personală.

Cu această evoluție rapidă a tehnologiei și aplicațiilor, fără ca educația digitală să poată ține pasul, spațiul virtual devine un teren de joacă pentru agresori. În același timp, serviciile sociale și suportul pe care îl acordă persoanelor trebuie să fie adaptate noii realități. Este un proces adaptativ, inclusiv la nivelul furnizării de servicii sociale, care ar trebui să ia în considerare noile tehnologii și tacticile pe care agresorii le-ar putea adopta pentru a-și menține controlul asupra victimelor lor.

Cercetarea privind nivelul de conștientizare a riscurilor digitale a reprezentat punctul de pornire pentru 10 sesiuni de training la care au participat 150 de profesioniști din domeniul social, din servicii publice și private, în care au fost abordate aspecte legate de mediul online, formele de violență sexuală și de gen în online și offline, victime și agresori, impactul asupra supraviețuitoarelor, trauma și intervenția în cazurile de violență cibernetică, modalități de creștere a siguranței în mediul online, atât la nivel personal, cât și organizațional.

Cinci furnizori de servicii pentru supraviețuitoarele violenței sexuale și de gen ai căror angajați au participat la training au fost incluși ulterior într-un program de coaching și mentorat pentru dezvoltarea politicilor și procedurilor de lucru interne, care să cuprindă și violența cibernetică și principii de lucru cu supraviețuitoarele. Serviciile cu care s-a lucrat în programul de coaching au fost: Direcția de Asistență Socială Bistrița, Locuința protejată Venus Pitești, Direcția de Asistență Socială și Protecția Copilului Ialomița, Direcția de Asistență Socială și Protecția Copilului Sector 2 București, Direcția Generală de Asistență Socială a Municipiului București.

În ghid vom folosi termenii de victimă, supraviețuitoare a violenței sau persoană afectată de violență, în funcție de context și mesajul pe care vrem să-l transmitem. Atunci când vorbim despre plângeri, acțiuni în instanță folosim termenul de victimă pentru a evidenția că o persoană a suferit abuzuri, iar termenii de supraviețuitoare și persoană afectată de violență când punem accent pe capacitatea de reziliență a acestora și în relație cu serviciile sociale.

O atenție specială va fi acordată violenței care se manifestă în relațiile intime (violența domestică), atât în mediul online, cât și offline, având în vedere natura relației emoționale dintre parteneri, conviețuirii și accesului fizic al agresorului atât la victimă, cât și la dispozitivele și conturile de e-mail sau aplicațiile pe care le folosește.

Fără a minimiza impactul pe care violența sexuală și de gen îl are asupra altor persoane (băieți/ bărbați, membrii LGBTQIA), accentul va fi pus pe femei și fete ca victime ale violenței, statistic acestea reprezentând categoria cea mai afectată.

VIOLENȚA SEXUALĂ , ȘI DE GEN



2

2.1. DEFINIȚIE

Violența sexuală și de gen (VSG) reprezintă un termen umbrelă pentru orice act comis împotriva voinței unei persoane, bazat pe normele de gen (diferențele atribuite social între femei și bărbați) și relații inegale de putere. Reprezintă o încălcare a drepturilor omului și afectează capacitatea unei persoane de a se bucura de drepturile sale.

Sexul se referă la caracteristici fizice și fiziologice, inclusiv cromozomi, expresia genelor, nivelurile și funcția hormonilor și anatomia reproductivă / sexuală. Sexul este de obicei clasificat ca femeie sau bărbat, dar există variații în atributele biologice care cuprind sexul și modul în care sunt exprimate aceste atribute. (Canadian Institutes of Health Research, “What is gender? What is sex?”, 28 April 2020, <https://cihr-irsc.gc.ca/e/48642.html>)

Genul se referă la rolurile, comportamentele și atributele construite social și cultural, asociate cu masculinitatea și feminitatea într-un anumit moment și loc. Normele de gen sunt schimbabile în timp; influențează identitățile individuale, relațiile sociale și distribuția resurselor și puterii în societate. Deși genul este adesea înțeles social ca exprimând așteptări cu privire la un comportament adecvat pentru bărbați și femei, genul este non-binar și divers. Se referă la persoane de toate identitățile și expresiile de gen. (UN Women, “Concepts and definitions”, <https://www.un.org/womenwatch/osagi/conceptsanddefinitions.html>)

Violența sexuală și de gen afectează persoanele din întreaga lume, în perioade de pace sau de conflict, în spațiul privat sau public, cu consecințe care depășesc sfera individuală, care se extind asupra familiilor și comunităților. Violența sexuală și de gen poate afecta orice persoană, indiferent de vârstă, sex, gen, orientare sexuală, dizabilitate, rasă, etnie, religie, statut social, statut legal, nivel de educație etc.

Anumite categorii sunt mai vulnerabile în fața acestui fenomen, cum ar fi fetele și femeile, femeile refugiate, persoanele cu dizabilități, membrii comunității LGBTQIA, persoanele aparținând anumitor grupuri minoritare și religioase. Statisticile și convențiile internaționale afirmă că fetele adolescente, femeile tinere, femeile aparținând minorităților etnice și ale altor minorități, persoanele trans și femeile cu dizabilități se confruntă cu un risc mai mare de a fi expuse la diferite forme de violență, pentru simplul fapt că sunt femei.

Cercetarea din 2014 a Institutului European pentru Egalitatea de Șanse între Femei și Bărbați (EIGE) arată că, în țările din Uniunea Europeană,

- 1 din 3 femei a experimentat violență fizică sau sexuală, de la vârsta de 15 ani
- 1 din 2 femei a fost hărțuită sexual

- 1 din 20 femei a fost violată
- 1 din 5 femei a fost urmărită
- 95% dintre persoanele traficate pentru scopuri sexuale sunt femei

Conform Convenției Consiliului Europei privind prevenirea și combaterea violenței împotriva femeilor și a violenței domestice, cunoscută sub numele de Convenția de la Istanbul, "violența împotriva femeilor" este înțeleasă drept o încălcare a drepturilor omului și o formă de discriminare împotriva femeilor și va însemna toate acțiunile de violență de gen care rezultă în, sau care sunt probabile a rezulta în, vătămarea sau suferința fizică, sexuală, psihologică sau economică cauzată femeilor, inclusiv amenințările cu asemenea acțiuni, coerciția sau deprivarea arbitrară de libertate, indiferent dacă survine în public sau în viața privată.

În cazurile de violență sexuală și de gen, **agresorul** poate fi orice persoană, grup, instituție care folosește abuzul de putere, autoritate sau control, incluzând soțul, partenerul intim, persoana care îngrijește, un membru al familiei, părinte, cadru didactic, lucrători umanitari, soldați/forțe de ordine/polițiști/militari, angajatori, instituții, rețele de traficanți etc.

Violența sexuală și de gen

- Reprezintă o încălcare a drepturilor omului
- Afectează integritatea fizică și psihologică/emoțională a unei persoane
- Reprezintă o discriminare a anumitor categorii de persoane care nu se încadrează în normele sociale
- Este un obstacol în calea egalității de gen
- Este un fenomen sub-raportat, iar agresorii sunt frecvent iertați
- Afectează toți indivizii și societatea în ansamblu
- Produce un cost foarte mare pentru societate din cauza resurselor utilizate pentru remedierea impactului asupra supraviețuitoarelor (Consiliul Europei)

2.2. FORME DE MANIFESTARE

Convenția de la Istanbul menționează în cuprinsul ei următoarele forme de violență sexuală și de gen: violența psihologică, urmărirea, violența fizică, violența sexuală, inclusiv violul, căsătoria forțată, mutilarea genitală a femeilor, avortul forțat și sterilizarea forțată, hărțuirea sexuală, infracțiunile în numele "onoarei".

Consiliul Europei a restrâns formele de mai sus în 5 categorii interdependente: violența fizică, violența verbală (inclusiv discursul instigator la ură), violența emoțională/psihologică, violența sexuală și violența socio-economică.

Violența fizică este un act prin care se dorește provocarea de durere și/sau rănire fizică. Include: bătăi, arsuri, lovituri cu picioarele, pumnii, mușcăturile, mutilarea, atacurile cu acid, uciderea cu sau fără folosirea obiectelor sau a armelor, combinată cu alte forme de violență sexuală sau de gen, trafic de persoane și sclavie (vânzarea și traficul de ființe umane în scopul practicării forțate a sexului și a muncii sau a unor servicii, sclavie sau practici similare sclaviei, înlăturarea unor organe), sechestrarea. Această formă de VSG reprezintă cel mai mare pericol pentru viața unei persoane, consecințele putând duce până la deces.

Violența verbală se referă la atacurile verbale cu scopul de a minimiza pe cineva, în public sau în privat, de a produce o suferință emoțională, ridiculizarea, folosirea unor cuvinte injurioase, care sunt deranjante pentru celălalt, amenințările la adresa persoanei sau celor dragi. În unele situații, atacurile verbale pot să vizeze intenționat anumite particularități ale persoanei respective, cum ar fi genul, religia, orientarea sexuală, etnia etc. Atunci când femeile sunt vizate, cel mai frecvent atacurile verbale au conotații sexuale - glume despre disponibilitatea sexuală a unei femei, viol etc. Include folosirea în adresare în mod peiorativ a cuvintelor legate de identitatea de gen a unei persoane, rasa, etnia, orientarea sexuală, deficiențele fizice sau psihice etc. Violența verbală este clasificată ca discurs instigator la ură când "se bazează pe presupunerea nejustificată că o persoană sau un grup de persoane sunt superioare celorlalți și incită la acte de violență sau discriminare, subminând astfel respectul față de grupurile minoritare și afectând coeziunea socială." (Comisia Europeană împotriva Rasismului și Intoleranței (ECRI))

Violența emoțională/psihologică este forma de violență care însoțește toate celelalte, însă se poate manifesta și singură. Impactul emoțional poate determina acte sau tendințe/gânduri suicidare în rândul supraviețuitoarelor. Include acele comportamente, atitudini, manifestări, cuvinte folosite cu scopul de a răni integritatea și demnitatea altei persoane, cum ar fi: izolarea, ignorarea, limitarea sau negarea accesului la informații și servicii, excluderea din anumite activități, dezinformarea, comportamentul amenințător, intimidarea, neglijarea, defăimarea, șantajul, minimizarea etc.

Violența sexuală este forma cea mai dificil de abordat din cauza tabuurilor și stereotipurilor care împiedică și dezvăluirile legate de identitate, orientare și practici sexuale. Similar celorlalte forme de VSG, violența sexuală este despre abuzul de putere; include: violul și tentativa de viol, angajarea într-o penetrație vaginală, anală sau orală de natură sexuală neconsimțită a corpului unei alte persoane cu orice parte corporală sau obiect, abuzul sexual asupra copiilor, forțarea cuiva să întrețină relații sexuale cu o altă persoană, forțarea cuiva să privească un act sexual sau imagini cu conținut sexual, exploatarea sexuală, hărțuirea sexuală, violul ca armă de război, sterilizarea forțată, nașterea forțată etc.

Violența socio-economică are ca scop izolarea și ținerea supraviețuitoarei într-o stare de dependență față de agresor. Se manifestă prin: discriminarea sau negarea accesului la servicii, oportunități și resurse (financiare și de alt tip); marginalizarea și excluderea socială, ostracizare, bazate pe orientare sexuală; practici juridice obstructive; negarea accesului la exercitarea drepturilor sociale, civile, economice, în special femeilor. La nivel social, presupune refuzul accesului la educație sau la muncă egal remunerată în principal femeilor, refuzul accesului la servicii, excluderea din anumite locuri de muncă, refuzul de a se bucura de drepturile civile, culturale, sociale și politice. În unele societăți, persoanele LGBTQIA pot fi chiar judecate penal pentru identitatea lor sexuală.

Practicile tradiționale dăunătoare sunt o formă de VSG care poate fi întâlnită în anumite societăți sau comunități, însă nu pot fi considerate ca norme și nici invocate ca scuze pentru agresiunile asupra persoanelor. "...cultura, obiceiul, religia, tradiția sau așa numita „onoare” nu vor fi considerate ca o justificare a acestor acte. Aici sunt cuprinse, în special, afirmațiile că victima a încălcat normele sau obiceiurile culturale, religioase, sociale sau tradiționale ale comportamentului adecvat” (*Convenția de la Istanbul*). Includ: mutilarea genitală feminină, mariaje forțate, mariaje între minori, crime de onoare și mutilarea, infanticid și/sau neglijare, negarea dreptului femeii la educație.

2.3. VIOLENȚA DOMESTICĂ

Violența domestică este o formă specifică de violență sexuală și de gen, care se poate manifesta în mediul online și offline, între foști sau actuali parteneri, care conviețuiesc sau nu.

Conform Legii 217/2003, *violența domestică înseamnă orice inacțiune sau acțiune intenționată de violență fizică, sexuală, psihologică, economică, socială, spirituală sau cibernetică, care se produce în mediul familial sau domestic ori între soți sau foști soți, precum și între actuali sau foști parteneri, indiferent dacă agresorul locuiește sau a locuit împreună cu victima.*

Presupune o relație intimă între agresor și victimă, care implică o legătură emoțională, existența unor copii, bunuri comune, un spațiu comun și un timp petrecut împreună. Este un fenomen cu un grad mare de recidivă, ce implică violențe repetate asupra aceleiași persoane, se produce de cele mai multe ori în preajma copiilor și în spatele ușilor închise. Considerarea violenței domestice ca „o problemă privată”, invizibilă, s-a aflat la baza inacțiunii statelor în a-și proteja cetățenii de violențe sau abuzuri, caracterizată de lipsa adoptării unor mecanisme eficiente de intervenție și suport pentru supraviețuitoare.

La fel ca în celelalte forme de violență sexuală și de gen, numărul majoritar al persoanelor afectate este reprezentat de femei. La nivel global, 27% din femeile și fetele cu vârste între 15 și 49 de ani au fost abuzate fizic și/sau sexual cel puțin o dată de fostul sau actualul partener. 38% din crimele cu victime femei sunt comise de partenerii acestora. (*Organizația Mondială a Sănătății, 2018*)

În primele 6 luni ale anului 2021, 10.643 de femei și tinere din România au raportat infracțiuni de loviri și alte violențe, în 65% din cazuri făptuitorul a fost partenerul sau fostul partener. 84% din incidente au avut loc la domiciliu. Poliția a intervenit în 28.486 de cazuri de violență domestică, dintre care 7.659 erau cu risc ridicat. 22 de femei au fost ucise. (*Institutul General al Poliției Române, 2021*)

MEDIUL ONLINE,
FACILITATOR AL VIOLENȚEI
SEXUALE ȘI DE GEN.
VIOLENȚA CIBERNETICĂ



3.1. MEDIUL ONLINE, FACILITATOR AL VIOLENȚEI SEXUALE ȘI DE GEN

Accesul la internet nu mai este considerat un lux, ci a devenit, pentru mulți dintre noi, o necesitate. Mai mult decât atât, în 2016 a fost recunoscut ca drept al omului de către Organizația Națiunilor Unite.

În România, în ianuarie 2021, 15,49 milioane de români aveau acces la internet, în creștere cu 133 mii față de 2020. Dintre aceștia, 12 milioane sunt utilizatori de social media, reprezentând 62,6% din populația României. În ianuarie 2021, erau 26 milioane de conexiuni mobile la internet, însemnând 135,6% din populația totală (unii utilizatori au mai mult de o conexiune mobilă). Penetrarea internetului în țara noastră este de 80,7%. (*Raportul Digital 2021, We are social*, <https://wearesocial.com/digital-2021>).

Internetul și tehnologia au schimbat cele mai simple activități umane, de exemplu: plata facturilor, achiziționarea de bunuri de larg consum și de strictă necesitate, lectura, accesul la informație, servicii, cursuri și școală etc.

Pentru 74% dintre supraviețuitoarele violenței sexuale și de gen implicate în "Cercetarea privind nivelul de conștientizare a riscurilor digitale", realizată de Fundația Sensibilu în cadrul proiectului TECH-WISE, RISK-FREE, accesul la internet și tehnologie le-a permis căutarea de informații despre violență și serviciile disponibile.

Inclusiv relațiile romantice și sexuale au cunoscut transformări, prin folosirea site-urilor și aplicațiilor de dating, webcams, videochat, messaging și social media, care le permite oamenilor să construiască relațiile intime într-un mod cu totul nou. Utilizarea tehnologiei și a mediului online în acest fel poate părea foarte interesantă și provocatoare, dar pot fi folosite și cu intenția de a face rău.

În ciuda beneficiilor imense pe care conectarea digitală le-a adus omenirii, este din ce în ce mai evident faptul că a deschis noi uși pentru opresiuni și violență. Există un consens tot mai mare că aceleași forme de discriminare de gen în plan social, economic, cultural și structurile politice care duc la violență de gen sunt reproduse și uneori amplificate în mediul online.

În ultimii ani, este tot mai intensă preocuparea față de modul în care internetul a devenit un spațiu în care se manifestă diverse forme de agresiune, în mod special asupra femeilor și fetelor, precum: hărțuirea și urmărirea online, expunerea informațiilor personale, distribuirea fără consimțământ a imaginilor sau filmelor cu conținut intim, comentariile referitoare la aspect, umilirea publică, manipularea imaginilor, amenințări legate de religie sau

identitate sexuală, spargerea conturilor de e-mail sau social media, furtul de identitate, exploatarea imaginii copiilor și pornografia infantilă, șantajul sexual etc.

De asemenea, este îngrijorător rolul pe care tehnologia și mediul online îl au în exploatarea femeilor și fetelor în scopuri de trafic, turism sexual și pornografie infantilă.

În cercetarea "Violența împotriva femeilor: o anchetă la nivelul UE - Principalele rezultate" realizată de Agenția pentru Drepturile Omului a Uniunii Europene în anul 2014, se estimează că o femeie din 10 a suferit deja o formă de violență cibernetică după vârsta de 15 ani, iar un studiu al Comisiei ONU de internet în bandă largă pentru dezvoltare digitală (2015) arată că 73% dintre femei și fete au fost expuse sau au experimentat violențe online. Fetele și femeile între 18 și 24 de ani sunt cele mai vulnerabile în fața urmărilor și hărțuirii sexuale în mediul online. (<https://en.unesco.org/sites/default/files/highlightdocumentenglish.pdf>).

În Raportul anual 2017 A/HRC/35/9 al Înalțului Comisar ONU pentru Drepturile Omului se afirmă că "violența online împotriva femeilor trebuie tratată în contextul mai larg al discriminării de gen și al violenței offline, iar statele ar trebui să adopte măsuri legislative adecvate și să asigure răspunsuri adecvate pentru a aborda fenomenul violenței împotriva femeilor online, inclusiv prin investigarea și sancționarea făptașilor, despăgubirea victimelor și instruire cu privire la aplicarea normelor și standardelor internaționale privind drepturile omului a celor din sistemul judiciar".

În era digitală, normalizarea comportamentelor violente și cultura care tolerează violența împotriva femeilor, promovată și facilitată de social media, consolidează atitudinile sexiste și violente și contribuie la norme și practici care fac spațiile online și offline ostile față de femei și grupurile cu risc cel mai mare de a fi discriminate. La nivel global, femeile sunt de 27 de ori mai susceptibile de a fi hărțuite online. (Agenția pentru Drepturi Fundamentale a Uniunii Europene (2014). *Violence against women: an EU-wide survey - Main results* (Violența împotriva femeilor: o anchetă la nivelul UE - Principalele rezultate), Luxemburg).

Raportul A / HRC / 38/47 Raportului special privind violența împotriva femeilor, cauzele și consecințele violenței online împotriva femeilor și fetelor din perspectiva drepturilor omului afirmă că "Statele ar trebui să recunoască violența împotriva femeilor online și facilitată de tehnologia informațiilor și internet ca o încălcare a drepturilor omului și o formă de discriminare și violență bazată pe gen împotriva femeilor și să aplice în mod corespunzător instrumentele internaționale de bază ale drepturilor omului."

Spațiul virtual devine nesigur pentru femei, cu un impact direct asupra

dreptului la liberă exprimare, la viață intimă, la siguranță, la libertate de mișcare, la sănătate și de a participa la viața publică. Violența bazată pe gen în mediul online dezavantajează femeile prin limitarea capacității lor de a beneficia de aceleași oportunități online de care beneficiază frecvent bărbații (de exemplu, ocuparea forței de muncă, autopromovare și/sau auto-exprimare). 28% dintre femeile care s-au confruntat cu violențe online și-au restrâns activitatea în mediul virtual (*Raportul Raportului Special privind violența împotriva femeilor, cauzele și consecințele acesteia asupra violenței online împotriva femeilor și fetelor din perspectiva drepturilor omului A/HRC/38/47*).

- **52%** dintre femeile și fetele tinere au suferit agresiuni online, inclusiv amenințări mesaje, hărțuire sexuală și partajarea de imagini private fără consimțământ
- **64%** dintre toți respondenții cunosc pe cineva care a suferit hărțuire, agresiuni sau violență
- **87%** dintre fete consideră că problema se înrăutățește
- **30%** au spus că principala lor grijă este schimbul de imagini, videoclipuri sau mesaje private fără acordul lor
- Alții sunt îngrijorați de
 - Mesaje răutăcioase și umilitoare (21%)
 - Limbaj abuziv și amenințător (15%)
 - Hărțuire sexuală (20%)
 - Partajarea conținutului fals (14%)
- **51%** dintre cei care au suferit agresiuni online spun că au fost afectați emoțional și/sau le-a fost afectată bunăstare fizică.
- **68%** din agresiunile online experimentate au avut loc pe platformele de socializare (sursa [The online crisis facing women and girls threatens global progress on gender equality - World Wide Web Foundation](#))

Accesibilitatea tehnologiei, a internetului, aplicațiilor și platformelor social media, precum și necesitatea unor cunoștințe tehnice minime, le facilitează agresorilor accesul la victimele lor și creează noi oportunități pentru săvârșirea agresiunilor în mediul online, doar cu un click, din confortul casei lor, fără a fi în proximitatea victimei.

Unul dintre elementele care oferă protecție agresorilor în mediul online este anonimitatea, pe care o folosesc pentru a scăpa de consecințele faptelor lor în viața reală. Anonimitatea are avantaje și dezavantaje. Îndeplinește o funcție importantă pentru activiști, femei și alte persoane cu risc de discriminare, permițându-le să caute informații, să găsească solidaritate și sprijin, să scape de cenzură și să împărtășească opinii fără teama de a fi „descoperite”. În special, persoanele care se confruntă cu discriminare și persecuție pe baza orientării lor sexuale și a identității de gen și/sau

cele care se confruntă cu violență de gen, găsesc în anonimitate o soluție pentru a eluda restricțiile și a-și exercita dreptul de liberă exprimare. Anonimitatea asigură protejarea intimității și exprimarea liberă a gândurilor și sentimentelor.

Pe de altă parte, anonimitatea poate conduce la o senzație de libertate absolută care poate degenera în comportamente antisociale: lipsa sentimentului de responsabilitate, lipsa sentimentului de vinovăție și agresivitate crescută. Oferă o "mantie" invizibilă prădătorilor și hărțuitorilor, care se ascund în spatele unor conturi/profiluri false, fără teama că vor fi prinși sau sancționați.

Anonimitatea intensifică frica și amplifică impactul asupra victimelor, pentru că nu știu cine se ascunde în spatele unui cont, dacă e o persoană necunoscută sau una din cercurile apropiate, care ar putea avea acces la ele în viața reală, având astfel ocazia de a-și pune în practică amenințările din mediul virtual. Anonimitatea nu trebuie confundată cu "autorul necunoscut". Cele mai multe dintre femei sunt hărțuite de cineva cunoscut, care se folosește de anonimitate pentru a abuza.

Dintre supraviețuitoarele violenței care au răspuns la "Cercetarea privind nivelul de conștientizare a riscurilor digitale", doar 7% se simt în siguranță când folosesc tehnologia și internetul și numai 11% știu ce să facă dacă se confruntă cu hărțuiri în mediul online.

Odată cu interconectarea platformelor, limitele sociale au dispărut. Penetrarea rețelei sociale a victimelor, accesul la prietenii și cunoștințele acestora le permit agresorilor menținerea și extinderea controlului, chiar și atunci când nu mai sunt conectați direct cu persoana vizată.

Practic, agresorii devin omniprezenți, "sunt cu tine chiar și când nu sunt lângă tine", așa cum s-a exprimat una dintre supraviețuitoare într-un focus grup. Purtând cu sine permanent un smartphone sau un laptop, presiunea și conștientizarea abuzului sunt permanente pentru persoanele afectate de violență.

Persistența, replicabilitatea, disponibilitatea (posibilitatea de a fi căutată) și vizibilitatea informației în mediul online amplifică anxietatea și trauma supraviețuitoarelor. Astfel, abuzurile sunt extinse dincolo de limitele temporale, durează și după ce faptele în sine s-au consumat, prin însăși existența informației în mediul virtual.

Mai mult decât atât, mediul online schimbă martorii la violență. De exemplu, dacă în cazul unui act de violență domestică offline, martorii sunt cei din jurul partenerilor - vecini, familie extinsă, copii etc., în cazul violenței sexuale și de gen în mediul online, audiența este anonimă, invizibilă, și extinsă dincolo de rețeaua socială a agresorului și supraviețuitoarei. Prin aprecierea, vizualizarea și distribuirea informațiilor, fotografiilor, filmelor despre o persoană, audiența se transformă într-un agresor secundar, crescând riscul de revictimizare.

Elementele care ne vulnerabilizează în mediul online

- Simplitatea faptului că suntem online
- Rasa, etnia, genul, dizabilitatea
- Obiceiurile, comportamentele noastre în online
- Dispozitivele pe care le folosim și cine are acces la ele
- Informațiile pe care le deținem, unde le stocăm și cui le oferim
- Grupurile și rețelele din care facem parte
- Contextul în care ne aflăm
- Lipsa de educație digitală

3.2. VIOLENȚA CIBERNETICĂ

3.2.1. DEFINIȚIE

Termenii pe care i-am putea întâlni frecvent sunt violența sexuală și de gen prin intermediul tehnologiei sau în mediul online, violență în mediul online, abuz cibernetic, abuz facilitat de tehnologie, control coercitiv prin intermediul tehnologiei. În cadrul acestui ghid, atunci când facem referire la situațiile în care în relațiile intime agresorul se folosește de tehnologie pentru a abuza, vom folosi termenul de violență cibernetică, în acord cu legislația românească, care o definește ca o formă de violență domestică, cuprinzând orice fapte de **hărțuire online, mesaje online instigatoare la ura pe bază de gen, urmărire online, amenințări online, publicarea non-consensuală de informații și conținut grafic intim, accesul ilegal de interceptare a comunicațiilor și datelor private și orice altă formă de utilizare abuzivă a tehnologiei informației și a comunicațiilor** prin intermediul calculatoarelor, telefoanelor mobile inteligente sau altor dispozitive similare care folosesc telecomunicațiile sau se pot conecta la internet și pot transmite și utiliza platformele sociale sau de e-mail, cu **scopul de a face de rușine, umili, speria, amenința, reduce la tăcere victima.** (L217/2003 pentru prevenirea și combaterea violenței domestice)

Rezoluția 29/14 din 2015 a Consiliului pentru Drepturile Omului afirmă că "violența domestică ar putea include acte precum hărțuirea cibernetică și cyberstalking - consolidând astfel încadrarea violenței online bazate pe gen ca parte a continuumului violenței împotriva femeilor - și că statele au o responsabilitate primară pentru prevenirea și promovarea drepturilor omului femeilor și fetele care se confruntă cu violență, inclusiv cele care se confruntă cu violență domestică."

Violența sexuală și de gen în mediul online reprezintă o manifestare a puterii și controlului, a discriminării existente deja în mediul offline, și o reflectare a valorilor și practicilor existente la nivelul societății împotriva anumitor categorii de persoane. Reprezintă acțiunea uneia sau mai multor persoane împotriva altora pe baza identității lor sexuale sau de gen sau prin aplicarea

normelor de gen dăunătoare, folosind internetul și/sau tehnologia mobilă pentru a-și extinde abuzul dincolo de granițele fizice, fără a fi nevoie de un contact direct cu victimele lor și include: urmărirea, agresiunea, hărțuirea sexuală, defăimarea, discursul de ură și exploatarea.

Oricine poate fi o victimă a violenței în mediul online, totuși anumite categorii sunt mai vulnerabile:

- Copiii, fetele și femeile, persoanele aparținând minorităților etnice și sexuale, persoanele publice au un risc mai mare de a fi ținte ale hărțuirii și amenințărilor în online
- Cei care lucrează în domeniul drepturilor omului, al asistării victimelor violenței sunt o categorie profesională expusă atacurilor online

O anchetă din 2014, realizată de Pew Research Center (Centrul de Cercetare Pew) din Statele Unite a arătat că, dacă probabilitatea de a se confrunta cu forme relativ „ușoare” de hărțuire online (cum ar fi injuriile și insistența) este doar cu puțin mai mare pentru bărbați decât pentru femei, în schimb acestea din urmă (în special tinerele cu vârste cuprinse între 18 și 24 de ani) se confruntă disproporționat mai frecvent cu tipuri grave de hărțuire cibernetică, și anume, urmărirea cibernetică și hărțuirea sexuală online. (Institutul European pentru Egalitatea de Gen, „Violența cibernetică împotriva femeilor și a fetelor” (Cyber Violence against Women and Girls), 23 iunie 2017, <http://eige.europa.eu/rdc/eige-publications/cyber-violence-against-women-and-girls>)

Din perspectiva dimensiunii de gen, violența în mediul online vizează în mod disproporționat femeile și persoanele care se identifică ca femei. Când femeile și fetele au acces la internet, acestea se confruntă cu violența online mai des decât bărbații printr-un continuum de forme multiple, recurente și interdependente de violență bazată pe gen, atacurile sunt susținute, sexualizate și conectate cu violența offline. Femeile se confruntă cu sexism, atitudini conservatoare, patriarhale, standarde duble, obiectificare, stereotipuri, discriminare etc., care sunt exacerbate în mediul online. Este un fenomen intersecțional, care vizează multiple dimensiuni precum rasa, etnia, sexualitatea, dizabilitatea.

Atunci când bărbații sunt victime ale violenței în mediul online, agresiunile au ca scop umilirea, facerea de rușine, contestarea masculinității și a genului. O vulnerabilitate crescută o au persoanele aparținând minorităților sexuale.

În timp ce unele dintre victime sunt vizate de agresori necunoscuți, care le abordează pe diverse canale sau le preiau controlul asupra conturilor de social media pentru informații personale și fotografii, altele sunt ținte ale răzbunării partenerului sau fostului partener.

Violența digitală este o extensie a violenței din viața reală. Datele din raportul din 2014 al Agenției pentru Drepturi Fundamentale a Uniunii Europene (FRA) arată că 77 % dintre femeile care au fost victime ale hărțuirii cibernetice au fost și victime a cel puțin unei forme de violență sexuală sau/ și fizică a partenerului intim, iar șapte din 10 femei (70 %) care au fost victime ale urmării cibernetice au fost și victime a cel puțin unei forme de violență fizică sau/ și sexuală a partenerului intim. Echipamentele, aplicațiile și internetul pot fi folosite de un agresor pentru a-și menține și chiar intensifica controlul asupra partenerii, chiar și atunci când sunt separați fizic, extinzând sfera abuzului dincolo de limitele spațiale.

În cazul a 51% dintre supraviețuitoarele respondente în ”Cercetarea privind nivelul de conștientizare a riscurilor digitale”, partenerii le verificau mesajele și listele de apeluri; 20% din supraviețuitoare au avut e-mailurile verificate de partener, iar în 34% din cazuri, parolele conturilor erau știute și de partener. 19% au declarat că partenerii le cereau să își activeze locația GPS pe telefon și să dea share location ori de câte ori plecau de acasă.

În lucrarea de față, ne vom referi la violența online în cadrul relațiilor intime, adică violența cibernetică, cel mai frecvent având ca victime femeile.

3.2.2. FORME DE MANIFESTARE

În cercetarea adresată supraviețuitoarelor violenței sexuale și de gen din cadrul proiectului TECH-WISE, RISK-FREE, 41% dintre respondente au fost hărțuite prin intermediul telefonului, primind zilnic zeci de apeluri de la partenerul sau fostul partener. 51% au primit mesaje de amenințare și injurii pe WhatsApp, Facebook Messenger, sms. În 23% din cazuri, agresorul suna de pe alte numere de telefon dacă partenera nu îi răspundea, și în 20% din cazuri a folosit conturi false de Facebook pentru a-și urmări victima.

Un studiu realizat în 2017 de Pew Research Center pe tema hărțuirii online a arătat că social media este un teren fertil pentru hărțuire, dar se întâmplă și în alte spații online.

Este de menționat diferența între două forme ale violenței cibernetice.

Violența asistată de tehnologie, în care agresorul folosește tehnologia de diverse tipuri pentru a-și urmări victima, a o controla, hărțui, dar actele au și componentă în mediul offline; ceea ce se întâmplă în mediul online este o prelungire a agresiunilor din viața reală.

și

Violența exclusiv online, în care agresiunile au loc doar în mediul online, fără

componentă de offline, fără să implice și alte agresiuni în viața reală.

În Raportul ONU din 2018 al Raportorului special privind violența împotriva femeilor, cauzele și consecințele violenței online asupra femeilor și fetelor din perspectiva drepturilor omului sunt evidențiate o serie de modalități prin care tehnologiile sunt utilizate pentru a comite agresiuni împotriva femeilor și fetelor. Luând în considerare cifrele agregate din întreaga lume, au fost identificate multiple forme de violență în mediul online, precum amenințările, incitarea la violență de gen, hărțuirea, diseminarea de informații false, impostura, traficul de femei, dezvăluirea informațiilor private (sau amenințarea cu dezvăluirea), doxing, șantajul sexual, trolling, accesul neautorizat la informații sau dispozitive, manipularea imaginilor, mobbing (sau hărțuirea în rețea) și urmărirea.

Tacticile pe care agresorii le folosesc în mediul online sunt diverse, unele dintre ele ilegale, fiind incriminate de Codul Penal, altele reprezintă doar încălcări ale termenilor de furnizare a serviciilor unor platforme.

- **Exploatarea cibernetică, fotografia neconsensuală sau „revenge porn”**

se referă la diseminarea în mediul online a imaginilor sau filmelor cu conținut sexual fără consimțământul persoanei din imagini, în scop de răzbunare, umilire, șantaj. Agresorul a intrat în posesia acestor imagini/filme fie în cadrul unei relații anterioare cu supraviețuitoarea, fie prin accesarea ilegală a computerului, telefonului sau conturilor de social media. Imaginile pot fi obținute și prin sexting consimțit, dar ulterior făcute publice pentru răzbunare. O întâlnim în special în cazurile în care supraviețuitoarea se decide să părăsească relația respectivă, folosită ca metodă de a o convinge să se întoarcă.

Statisticile arată că marea majoritate a celor care fac și dețin poze cu caracter sexual /intim nu le șterg nici când se separă de persoana respectivă. Așa a fost și în cazul Laurei. Fostul partener „știa să îi spună exact ce voia ea să audă, iar ea era o copilă credulă”. Fostul partener a reușit să o convingă treptat că nu este nimic în neregulă cu a fi fotografiată în poziții intime și că pozele sunt în siguranță, pentru că o iubea nespun de mult. Însă în timp, relația a degenerat într-una violentă, iar când separarea a devenit iminentă, fostul partener a început să o amenințe atât verbal, cât și prin mesaje scrise, cu divulgarea acelor poze în mediul online, dacă nu se răzgândea.*

- **Sextingul** se referă la trimiterea consimțită de mesaje, imagini, filme cu conținut intim între două persoane. Este o practică relativ comună între adolescenți, procente variind între 20% și 60%. Utilizarea sextingului în rândul adulților este chiar mai frecventă, un studiu realizat în 2015 de Departamentul de Psihologie al Universității Drexel SUA indicând procente de 88%. În unele state, în funcție de vârsta minorului, sextingul este considerat pornografie infantilă și sancționat penal. O

distincție foarte importantă trebuie făcută între consimțământul de a face/trimitte imaginile cuiva și consimțământul de a fi date mai departe sau făcute publice, ceea ce reprezintă o încălcare a confidențialității. Poate deveni un nou mijloc de perpetuare a violenței domestice, luând forma sextingului abuziv sau coercitiv, în care un partener îl presează pe celălalt pentru a trimite imagini intime sau pornografice din răzbunare, când partenerul amenință sau face publice imaginile respective.

- **Sextortion/șantajul sexual în mediul online** constă în acțiunea unor atacatori asupra unei persoane, pe care o amenință cu publicarea unor presupuse filme cu conținut intim în care apare victima, cu scopul de a o constrânge să facă ceva: să plătească, să obțină favoruri sexuale sau a și mai multor imagini intime.

- **Spionarea și supravegherea cu scop sexual** prin instalarea de camere de supraveghere în cabine de probă, toalete, locuințe, vestiare, săli de clasă etc. În cazul relațiilor intime, unul dintre parteneri poate instala camere de supraveghere în locuința victimei, cu sau fără știința celuilalt, iar imaginile le poate folosi ulterior pentru șantaj sau revenge porn.

- **Obiectificarea sexuală a femeilor și fetelor**, cel mai frecvent, care sunt privite doar ca obiecte sexuale, prin comentarii sexuale la adresa corpurilor acestora, distribuirea imaginilor prelucrate/alterate astfel încât să le prezinte în ipostaze sexuale (de ex. într-o imagine, capul unei persoane cunoscute este pus peste un corp într-o ipostază intimă și este distribuit pe rețelele de socializare), glume sexuale etc.

- **Slut-shaming** se referă la stigmatizarea unei femei sau fete pentru că se angajează în comportamente considerate a fi promiscue sau provocatoare sexual. Este una dintre formele prezente în special între adolescenți. Se intersectează cu revenge porn, spionarea, fotografierea fără consimțământ. În relațiile intime poate fi folosită cu scop de răzbunare și pentru defăimarea partenerei, în special în situațiile în care se judecă custodia copiilor, pentru a aduce atingere imaginii celuilalt părinte.

- **Traficul**, deși nu este în mod tipic văzut ca o formă de violență cibernetică, se folosește de tehnologie și internet pentru a identifica, manipula și a exploata. Social media este cea mai folosită pentru a iniția primul contact cu viitoarea victimă, iar Facebook cea mai utilizată platformă pentru recrutare, atât a minorilor, cât și adulților. Traficanții se folosesc de social media pentru a-și amenința victimele, pentru a le controla, izola și a împrăștia zvonuri despre ele.

Juana, 24 de ani, a plecat din țara ei natală din sudul Americii, în Spania pentru a munci și a-și ajuta familia rămasă acasă. Singură într-o țară străină, Juana era destul de activă pe rețelele de socializare. La un moment dat, a fost abordată pe Facebook de un tânăr din România. S-au conversat vreo 2-3 săptămâni, „nimic serios”, după cum spunea Juana. Apoi, el i-a propus să îi facă cunoștință cu fratele lui. S-au plăcut și câteva luni mai târziu s-au căsătorit și s-au mutat în România, la familia soțului. Pentru o perioadă scurtă*

de timp, lucrurile au mers bine. Treptat, Juana a început să se simtă izolată, pentru că nu mai putea avea conversații telefonice cu familia ei decât în prezența soțului, care îi controla mesajele și apelurile. De fapt, controla tot ce făcea Juana, căreia îi interzisese să meargă la magazin sau să aibă un loc de muncă. Când soțul era la serviciu, mama acestuia o urmărea ca o umbră. Juana a încercat să ia legătura cu Ambasada țării de origine, dar pentru că nu s-a gândit să își „șteargă” urmele, soțul i-a descoperit intențiile. Decizia finală a plecării a luat-o când a înțeles că se afla în riscul de a fi traficată, că relația cu soțul ei nu a fost decât un pretext, iar intenția lui și a fratelui a fost una de racolare încă de când s-au cunoscut pe internet.

- **Pornografia nesolicitată** se referă la transmiterea de imagini statice sau animate (gif) cu conținut sexual explicit, violent, fără ca destinatarul să le fi cerut.
- **Videoclipuri despre viol** sunt folosite pentru șantaj, pentru a face de rușine sau sunt vândute ca pornografie non-consensuală.

30% din tot traficul de pe Internet este reprezentant de pornografie. Cercetările arată, de asemenea, că 88,2% dintre scenele pornografice cu cele mai bune cote conțin acte agresive și în 94% din cazuri, agresiunile sunt îndreptate împotriva unei femei. (Cyber Violence Against Women And Girls: A World-Wide Wake-Up Call. A Report By The Un Broadband Commission For Digital Development Working Group On Broadband And Gender, 2015)

- **Grooming & predation** este o tactică folosită de prădătorii sexuali pentru a stabili o conexiune emoțională cu un copil, de a construi o relație de încredere cu acesta cu scopul de a-l agresa sau exploata sexual, în mediul online sau în viața reală. Pandemia de COVID a crescut numărul copiilor care folosesc tehnologia și au acces la internet, ceea ce a dus și la creșterea numărului celor care ar putea fi expuși la grooming & predation. Cel mai frecvent, agresorii își țintesc victimele pe platformele și rețelele de socializare populare printre copii - Facebook, Instagram sau prin abordarea în chatul jocurilor video în rețea, folosind profiluri false, ale unor copii/adolescenți de vârstă apropiată. Prădătorii le pot cere copiilor să se filmeze sau fotografieze în ipostaze intime sau în timp ce fac lucruri absolut nevinovate, de exemplu dansează, pe care ulterior le prelucrează pentru a le da tentă sexuală. Exploatează teama copiilor și îi șantajează, cerându-le să se expună din ce în ce mai mult sau să se întâlnească în viața reală.

Pandemia a constrâns multă lume la utilizarea tot mai intensivă a mediului online. Copiii au fost în mod special afectați; lipsiți de interacțiunea cu colegii în viața reală, au căutat refugiu în jocuri online. Irina, 10 ani, izolată destul de mult la domiciliu, a început să acceseze tot mai mult jocurile online și să se împrietenească virtual cu copii care aveau aceeași pasiune.*

La un moment dat, fetița i-a povestit mamei că unul dintre prietenii virtuali îi trimitea în privat mesaje nepotrivite, cu tentă sexuală. Mama a descoperit că cel care se ascundea sub identitatea prietenului virtual era un bărbat de cca 45-50 de ani. Din păcate, mama nu a făcut plângere la poliție, doar l-a amenințat pe respectivul bărbat cu acest lucru și a închis contul fetiței.

- **Pornografia infantilă** se referă la imaginile și filmele cu unul sau mai mulți copii în ipostaze intime. Unele materiale sunt folosite de prădătorii sexuali pentru uzul propriu, sunt transmise live sau sunt vândute consumatorilor de astfel de imagini. La nivel global, Statele Unite sunt cel mai mare producător și consumator de pornografie infantilă. Este una dintre cele mai violente și abominabile forme de abuz asupra copiilor.
- **Amenințările în mediul online sau prin intermediul echipamentelor**, chiar dacă din punct de vedere legal nu sunt luate foarte în serios, creează multă anxietate și afectează viața unei persoane. Agresorii amenință cu agresiunea fizică, violul și chiar moartea, uneori acestea fiind orientate și către membrii familiei. Mesajele sunt transmise fie prin WhatsApp, Facebook Messenger, e-mail, postări publice pe rețelele de socializare. Uneori amenințările sunt corelate cu comentarii sexiste sau rasiste. În cazul relațiilor intime, agresorul poate avea acces fizic la victima sa și își poate pune în practică amenințările.
- **Hărțuirea și hărțuirea pe platforme multiple** constă în comportamentul nepotrivit al unui agresor sau grup de agresori față de o persoană căreia îi adresează cuvinte nepotrivite, o jignesc, o amenință cu dezvăluirea unui secret sau, din contră, își manifestă nesolicitat afecțiunea. Dacă agresorul este blocat, încearcă să își contacteze victima pe alte platforme sau rețele de socializare pe care aceasta le folosește. Devine o problemă serioasă când comentariile sunt repetitive, obsesive, excesive și extrem de jignitoare. Cyberbullying-ul, prezent în special între copii și adolescenți, este o formă de hărțuire online și constă în utilizarea tehnologiei și a internetului pentru a intimida o persoană. Reprezintă un comportament abuziv, ținut, deliberat și repetat, menit să facă rău altei persoane. Exemplele de cyberbullying includ mesaje text sau e-mailuri neplăcute, zvonuri trimise prin e-mail sau postate pe site-uri de socializare și imagini, videoclipuri sau site-uri web jenante. Implică de obicei o serie susținută de astfel de mesaje, fie că sunt orchestrate de o singură persoană sau un grup de colegi și impactul cumulativ poate fi destul de devastator, ducând chiar și până la sinuciderea persoanei agresate.
- **Hărțuirea bazată pe gen în mediul online** descrie o conduită nepotrivită care implică folosirea de insulte, batjocuri, stereotipuri, atacuri și comportamente pline de ură, amenințări cu agresiuni fizice orientate împotriva unei persoane și motivate de apartenența persoanei respective la un anumit gen. Atât în mediul online, cât și în viața reală, femeile și fetele sunt frecvent ținta unor astfel de atacuri pentru simplul fapt că sunt de sex feminin; le sunt adresate cuvinte jignitoare, care se referă în

principal la comportamentul lor sexual.

- **Doxing** se referă la publicarea fără consimțământ, neautorizată a datelor personale ale cuiva, de exemplu adresa de domiciliu, numărul de telefon, adresa de e-mail, numele membrilor familiei, a veniturilor, obținute uneori prin accesarea neautorizată a dispozitivelor sau conturilor, cu scopul de a produce teamă, panică, stres. În cazul relațiilor intime, un astfel de comportament are ca scop răzbunarea, rănirea și vulnerabilizarea celuilalt, fiind însoțit și de defăimare. De exemplu, partenerul uneia dintre supraviețuitoare a publicat online fotografia, numele și numărul de telefon al acesteia cu mențiunea că prestează servicii sexuale pentru bani. În alt caz, agresorul a dat un anunț în ziar la rubrica matrimoniale cu numele și numărul de telefon al fostei partenere.
- **Defăimarea** este un act prin care o persoană sau uneori un grup organizat invadează în mod deliberat internetul și rețelele sociale cu informații negative, care aduc atingere imaginii și reputației unei alte persoane sau unei afaceri. De multe ori, agresorii se folosesc de protecția anonimității pentru a posta materialele. În relațiile intime, partenerul agresiv postează informații negative despre victimă pe rețelele de socializare, în grupurile de prieteni sau în grupurile de serviciu pentru a-i afecta credibilitatea și imaginea, a o face de rușine, a pierde custodia copiilor sau locul de muncă.

Soțul Alinei trimitea în mod frecvent de pe adresa ei de e-mail mesaje denigratoare și acuzații către colegii ei de serviciu, foștii colegi sau șefii de sex masculin privitoare la existența unei relații intime a acestora cu soția lui. Alina a constatat că soțul îi spărsese parola e-mailului de serviciu. Acesta și-a justificat gestul prin căutarea de dovezi pentru a-și confirma suspiciunile de infidelitate. La fel a motivat și montarea în casă a unor camere de supraveghere. Acesta o agresa deseori, iar dacă Alina riposta, soțul o înregistra pentru a strânge dovezi cu privire la „caracterul” ei.*

- **Restricționarea accesului la servicii** prin atacuri asupra site-urilor organizațiilor activiste pentru drepturile omului sau care oferă servicii de suport supraviețuitoarelor violenței sexuale și de gen, a site-urilor, blogurilor, paginilor de socializare ale unei persoane, excluderea din anumite grupuri online/platforme de jocuri, semnalizarea (flagging) paginii unei persoane în social media pentru a-i suspenda pagina și a-i bloca accesul etc. În relațiile intime, restricționarea accesului la servicii poate fi realizat prin suspendarea abonamentului la internet, abonamentului de telefonie mobilă, confiscarea echipamentelor electronice, monitorizarea istoricului de căutare pe internet, schimbarea parolelor la paginile de socializare.
- **Abuzul financiar prin intermediul dispozitivelor** se referă la folosirea internetului sau a tehnologiei pentru a avea acces la resursele financiare ale unei persoane, în special în relațiile intime, manifestat prin restricționarea accesului la conturile comune și la carduri, retragerea

banilor din conturile comune fără știrea partenerului, însușirea cardului partenerului.

- **Swatting** constă în alertarea autorităților prin reclamații false că la o anumită adresă se întâmplă ceva ilegal, de exemplu un act de violență domestică, un abuz asupra unui copil, trafic și consum de droguri. În relațiile intime, partenerul violent poate face o sesizare la 112 sau la protecția copilului, acuzând partenera/fosta parteneră de abuzuri asupra copiilor, pentru a exercita presiune asupra ei și intimidare în procesele de custodie.
- **Stalking (urmărirea/persecutarea)** reprezintă o formă agravată de hărțuire, repetată, cu o intensitate și o frecvență mai mari, de tipul unei obsesii, fixații. În mediul online presupune monitorizarea utilizării de către cineva a internetului, a platformelor sociale, a e-mailului sau a altor forme de comunicare electronică, utilizând aplicații de urmărire/spionare (spyware), acces la profilul victimei și urmărirea ei prin intermediul prietenilor/cunoscuților/cercului apropiat. În viața reală, implică apariția neanunțată în locurile frecventate de persoana vizată, pătrunderea ilegală în casa ei, amenințarea cu uciderea animalului de companie sau a unei persoane apropiate.
- **Supravegherea și monitorizarea** activităților unei persoane în mediul online și offline, folosind programe de urmărire, programe sau dispozitive fizice cu ajutorul cărora se pot vizualiza toate caracterele care sunt introduse de către un dispozitiv (keylogger), în special a parolelor, monitorizarea prin intermediul GPS-ului sau a altor software-uri de geolocalizare, care oferă informații despre toate mișcările persoanei targetate. Instalarea acestor programe se poate realiza fie prin accesarea fizică a echipamentelor și dispozitivelor victimei, fie prin download-area lor de către aceasta, fără să își dea seama, prin accesarea unor link-uri aparent nevinovate trimise de agresor. În relațiile intime, acest tip de violență poate lua forma accesării fără acordul victimei a conturilor și dispozitivelor sale, prin spargerea parolelor sau instalarea unor programe de monitorizare sau a accesării cu știința victimei, constrânsă sub amenințare să dezvăluie parolele. Frecvente sunt și situațiile în care, la începutul relației, cei doi parteneri fac schimb de parole pentru a-și demonstra încrederea unul în celălalt; neacceptarea împărtășirii parolelor este privită cu suspiciune, la fel ca și încercarea de schimbare a acestora de către utilizatorul conturilor. Când relația devine una abuzivă, partenerul agresiv poate prelua controlul conturilor, restricționând accesul victimei la ele.

Simona a realizat ca are nevoie de mai multe informații privind siguranța în mediul online atunci când a primit cadou un telefon nou de la soț. Soțul era foarte gelos și o agresa frecvent; a "sfătuit-o" să nu își dezactiveze locația, pentru a ști mereu unde se află, justificând cerința lui cu o posibilă situație în care ar fi fost în pericol și ar fi avut nevoie de ajutor. Solicitarea părea plauzibilă, mai ales că momentul a coincis cu cazurile de dispariție de la*

Caracal, ceea ce a mascat pentru o perioadă intențiile reale ale soțului.

„Eu și soțul meu ne-am căsătorit din dragoste”, spune Andreea* la prima întâlnire cu asistentul social. „Îmi plăcea să mă sune mereu, era îngrijorat ca iubita lui ar fi putut păți ceva. Mi s-a părut normal să dau dovadă de iubire, când mi-a spus că între noi nu trebuie să fie secrete, doar suntem soți. El mi-a dat parola de la telefonul lui și am simțit că trebuie să fac la fel, că doar nu aveam nimic de ascuns. La început m-am simțit așa de bine! Cineva se interesa de mine, îmi purta de grijă. Nu o mai făcuse nimeni până atunci. La fel am simțit și când a început să mă sune la muncă, să se intereseze dacă îmi fac probleme colegii sau șeful, ce vorbesc cu ei, dacă se poartă frumos cu mine. Mă suna și de câteva ori pe zi. De cele mai multe ori, mă apela video pe WhatsApp, ca să se asigure că sunt bine, spunea el. A vrut să îmi cunoască colegii. Într-o zi, un coleg a făcut o glumă, iar eu am râs. Când am ajuns acasă, am primit prima palmă doar pentru ca am râs la gluma colegului. De atunci, a început să mă apeleze numai video, să îmi ceara telefonul ca să îmi vadă mesajele; îmi verifica pagina de Facebook, să vadă dacă am prieteni bărbați și îmi spunea că o femeie serioasă nu are de ce să aibă prieteni bărbați...Spunea cuvinte urâte la adresa femeilor care aveau, le considera... știți dumneavoastră cum...”

● **Represaliile împotriva susținătorilor victimelor** se manifestă sub forma amenințărilor sau hărțuirii orientate către familia, prietenii, colegii sau angajatorii victimei, pentru a-și retrace suportul.

După câteva luni de relație, partenerul Tatiane* a început să devină agresiv. Ea luase deja decizia să se separe; în momentul în care i-a spus și partenerului acest lucru, a fost dată afară din casă, fără a-și putea lua lucrurile personale, inclusiv telefonul. Faptul că acesta îi cunoștea parola de la telefon i-a oferit acces la toate informațiile personale ale acesteia. Astfel, a pretins că e partenera lui și a postat pe pagina de Facebook a acesteia diverse mesaje injurioase. De asemenea, a lansat în mediul online amenințări la adresa Tatiane și a celor care ar putea să îi ofere suport.

● **Hate speech/discursul instigator la ură** se referă la incitarea și încurajarea urii, discriminării sau ostilității față de o persoană, pe baza unor prejudecăți împotriva persoanei respective din cauza unei anumite caracteristici, de exemplu orientarea sexuală sau identitatea de gen a acesteia. În mediul online se manifestă printr-un limbaj sau imagini care insultă, denigrează, amenință indivizi sau grupuri de indivizi pe baza unor trăsături specifice, precum genul, orientarea sexuală, rasa, religia, dizabilitatea etc. Homofobia este frica irațională de o persoană lesbiană, homosexuală sau bisexuală, iar transfobia definește teama irațională de o persoană care se declară de un alt gen decât cel atribuit prin naștere, prin tratament hormonal, operații de schimbare a sexului, vestimentație, machiaj etc.

● **Deadnaming** este o formă de hărțuire orientată împotriva celor care

au trecut printr-o schimbare de identitate manifestată prin expunerea în mediul online a numelui real, împotriva dorinței acelei persoane. În mod frecvent, este direcționată către persoanele din comunitatea LGBTQIA, în special transgender, care și-au schimbat numele dat la naștere.

● **Acuzații false de blasfemie** lansate în mediul online, care generează un risc extrem de mare mai ales pentru femeile care trăiesc în țări cu o religie ultraconservatoare, în care blasfemia este împotriva legii, iar crimele în numele onoarei sunt o amenințare la adresa vieții femeilor.

● **Furtul de identitate online și schimbarea identității în scop ilicit** se referă la o infracțiune în care cineva obține în mod ilicit și folosește identitatea unei alte persoane cu scopul de a induce în eroare, de a păcăli, pentru a se răzbuna sau de a obține avantaje financiare.

În România, în anul 2018, un bărbat și-a amenințat fosta iubită că, dacă nu va relua relația cu el, va face publice pe internet mai multe fotografii care o înfățișau nud și filmulețe în care cei doi apăreau întreținând relații intime. Ulterior, bărbatul a creat pe un site de adulți un profil cu numele femeii, unde a postat imaginile și filmele respective, precum și un profil fals pe Facebook cu numele fostei partenere, de pe care a trimis altei persoane fotografii cu femeia dezbrăcată. În acest proces, la începutul anului 2021, Înalta Curte de Casație și Justiție a decis că ”dacă o persoană deschide și folosește un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), cu numele de utilizator și datele reale (informații, fotografii, imagini video etc.) ale altei persoane, atunci se comite infracțiunea de fals informatic prevăzută în art. 325 din Codul penal.”

● **Mobbing/Cyber mobs** descrie atacurile colective ale unui grup mare asupra unei ținte printr-un val de amenințări, insulte și alte tactici abuzive. Sunt frecvente atacurile asupra unor femei și fete care au fost expuse în spațiul public în ipostaze intime sau având relații intime, folosind diverse hashtag-uri, cu scopul de a le face de rușine, de a le umili sau asupra unor persoane publice, activiști, feministe etc. pentru a le descuraja. Nu de puține ori, în mass media, au apărut cazuri ale unor adolescente care s-au sinucis în urma unor astfel de atacuri. Această formă de violență în mediul online este strâns legată de slut-shaming.

● **Atacurile în viața reală** reprezintă punerea în practică a unor amenințări, agresiuni din mediul online, concomitent sau ulterior acestora. Pot face parte dintr-un continuum de hărțuiri și amenințări sau de agresiuni în cuplu. Un agresor poate doar să amenințe cu astfel de atacuri în viața reală, pentru a produce frică, avertizând victima că știe unde locuiește, studiază sau lucrează.

Unele forme au un impact deosebit de grav asupra vieții, siguranței, sănătății fizice și emoționale, bunăstării și imaginii persoanelor afectate. Impactul este cu atât mai devastator, cu cât există o proximitate fizică față

de victime, care poate duce la agresiuni în viața reală. În mediul online, agresorii se pot folosi de anonimitate pentru a-și hărțui victimele, care devin hipervigilente și anxioase, pentru că nu știu care dintre profilele cu care s-au împrietenit sunt false și care reale, cine se ascunde în spatele unui profil, poate cineva cunoscut, care cunoaște detalii intime despre ele sau un agresor necunoscut.

Aceste tactici pot fi folosite independent sau combinate, cum e cazul revenge porn și slut-shaming, videoclipuri despre viol și slut-shaming, doxing și defăimare etc. De asemenea, sunt conectate cu alte forme de violență împotriva femeilor în mediul offline, cum ar fi violența domestică.

În practică, profesioniștii se pot întâlni cu situații în care o persoană solicită suportul serviciilor specializate pentru o situație de violență domestică, de cele mai multe ori manifestată prin violențe fizice, fără să identifice în mod explicit și o formă de violență prin intermediul tehnologiei. Responsabilitatea specialiștilor este de a include violența online în instrumentele de evaluare inițială și complexă și de a ajuta supraviețuitoarea să o recunoască prin întrebări. Identificarea corectă a tacticilor folosite de agresor în mediul online este extrem de importantă pentru identificarea riscurilor și dezvoltarea unui plan de siguranță exhaustiv, care să includă și violența prin intermediul tehnologiei, utilă pentru protecția persoanei afectate. Ascultarea convorbirilor, verificarea apelurilor efectuate (atât prin accesarea listei telefonului, dar și prin consultarea desfășurătorului apelurilor din factura abonamentului), supravegherea și monitorizarea cu aplicații de geolocalizare cresc riscul ca demersurile de a căuta ajutor să fie descoperite de agresor, pot duce la o intensificare a abuzului și la expunerea profesioniștilor care oferă suport.

Dincolo de agresiunea propriu-zisă, autoînvinovățirea este prezentă, supraviețuitoarele simțindu-se responsabile pentru comportamentul agresorilor și se simt nevoite să facă față blamării accentuate în mediul online din partea celorlalți (victim blaming), cunoscuți sau necunoscuți. Aceștia devin **agresori secundari prin re-postarea sau distribuirea informațiilor, contribuind astfel la revictimizare.**

**Pentru a le proteja identitatea, numele și vârstele persoanelor au fost schimbate.*

3.2.3. VIOLENȚA CIBERNETICĂ ȘI DREPTURILE OMULUI

Rezoluția A/HRC/RES/20/8 privind Promovarea, protecția și exercitarea drepturilor omului pe internet, adoptată în anul 2012 de Consiliul ONU pentru Drepturile Omului afirmă că "aceleași drepturi pe care le au oamenii

offline trebuie să fie protejate și online, în special libertatea de exprimare, care este aplicabilă indiferent de frontiere și prin orice mijloc la alegerea cuiva, în conformitate cu articolele 19 din Declarația Universală a Drepturilor Omului și Pactul internațional privind Drepturi civile și politice".

Similar celorlalte tipuri de violență, și cea în mediul online reprezintă o încălcare a drepturilor omului și a drepturilor civile, în special a:

- *Dreptului la viață intimă*, prin accesul la informațiile personale ale supraviețuitoarelor, amprenta digitală pe care respectivele informații o lasă în mediul online, persistentă, greu de îndepărtat. "Memoria" internetului păstrează o perioadă îndelungată de timp ceea ce postează un agresor despre victima sa. În plus, accesul aplicațiilor la datele personale, cum ar fi data nașterii, vârsta, genul, profilul, locația, cardurile de credit, starea de sănătate, tratamentele urmate, preferințele, adresele de e-mail etc., vulnerabilizează persoanele în fața atacurilor cibernetice și agresorilor. De asemenea, dreptul la viață intimă este încălcat prin instalarea programelor și dispozitivelor de monitorizare și supraveghere, violarea corespondenței electronice și a dispozitivelor personale, postarea imaginii fără consimțământ, atingerile aduse reputației și onoarei
- *Libertății de exprimare și la informare*, prin auto-cenzurarea opiniilor politice, religioase etc., pentru a evita agresiunile și represaliile, cenzurarea informațiilor accesibile publicului în țările cu regimuri autoritare, limitarea căutărilor pe internet pentru a nu genera suspiciunea partenerului agresiv
- *Dreptului la siguranță și de a fi protejat de tratamente inumane și degradante*
- *Dreptului la sănătate*, prin impactul pe care violența în mediul online îl are asupra sănătății emoționale, fizice și sociale a supraviețuitoarelor, evitarea accesării serviciilor de suport pentru a nu oferi motive de suspiciune agresorului
- *Dreptului la liberă mișcare*, prin monitorizarea cu ajutorul geolocalizării, urmată de restrângerea arealului de deplasare pentru a nu genera suspiciuni agresorului, urmarea unei rute predefinite, evitarea anumitor zone frecventate de agresor
- *Dreptului de a participa la viața publică*, prin limitarea prezenței online pentru a evita agresiunile, evitarea angajării în dezbateri de teama represaliilor sau a trollingului, izolarea prin restricționarea accesului la echipamente și internet. 18% dintre fetele care au fost hărțuite frecvent în mediul online au încetat să posteze conținut prin care își exprimau opiniile, 16% dintre ele și-au schimbat modul de exprimare și expunere pentru a evita hărțuirea (*Free to be online? The State of the World's Girls Reports, Plan International USA, 2020*)
- *Dreptului de a munci și de a se bucura de condiții de lucru decente*, prin restricționarea accesului la locuri de muncă de către agresor, defăimarea, amenințarea cu expunerea în fața angajatorilor a comportamentului

intim, acceptarea unor locuri de muncă mai prost plătite sau necalificate de teama expunerii

- **Drepturile copiilor** de a fi feriți de violență, de a nu fi discriminați, de a vorbi și a fi ascultați, la viață privată, la corespondență personală, care nu să nu fie deschisă sau citită de alții

Drepturile omului, și mai specific drepturile femeilor, sunt la fel de importante în mediul online ca și în cel offline. Fără o abordare bazată pe drepturile omului și interzicerea violenței online bazate pe gen, integrate încă din faza de design a aplicațiilor, discriminarea sexuală și pe bază pe gen și violența împotriva femeilor și fetelor în societate vor fi încurajate și vor continua să afecteze viețile a miliarde de persoane, cu costuri sociale și personale enorme. Internetul și tehnologia pot fi catalizatori ai capacitării (*empowerment*) sociale, politice și economice a femeilor și mijloace pentru promovarea drepturilor acestora.

3.2.4. LEGISLAȚIA ÎN ROMÂNIA

România a făcut demersuri pentru alinierea legislației naționale la cea internațională, iar ratificarea în 2016 a Convenției de la Istanbul a produs schimbări importante la nivel legislativ, în primul rând, a apărării drepturilor supraviețuitoarelor, a protejării siguranței lor și a dezvoltării de servicii psihosociale. Convenția de la Istanbul a inițiat și a condus la schimbări importante în legislație, cum ar fi înființarea unor servicii mai bune pentru supraviețuitoare, alocarea resurselor și intensificarea eforturilor de instruire a specialiștilor care intervin în aceste cazuri.

Modificarea din 2020 a Legii 217/2003 privind prevenirea și combaterea violenței domestice recunoaște violența cibernetică ca formă de violență domestică.

Legea vine în ajutorul supraviețuitoarelor violenței prin introducerea a două instrumente menite să ofere siguranță și să le protejeze viața, și anume ordinul de protecție provizoriu (OPP) și ordinul de protecție (OP). În primele 8 luni ale anului 2021, au fost emise 7.120 de ordine de protecție provizorii și 6.901 ordine de protecție, dintre care 2.206 ordine de protecție au fost încălcate de agresori.

Ordinul de protecție provizoriu se emite de către polițiștii care, în exercitarea atribuțiilor de serviciu, constată că există un risc iminent ca viața, integritatea fizică ori libertatea unei persoane să fie pusă în pericol printr-un act de violență domestică, în scopul diminuării acestui risc.

Emiterea unui OPP este făcută de polițist în baza unei evaluări de risc, folosind un instrument standard, prevăzut de Legea 217/2003. Ulterior, în maxim 48 de ore, acest ordin este infirmat sau confirmat de procurorul de la

parchetul de pe lângă judecătoria competentă în a cărei rază teritorială a fost emis, dacă se constată că sunt îndeplinite condițiile de risc. Durata maximă a unui OPP este de 5 zile și poate impune **următoarele măsuri**: evacuarea temporară a agresorului din locuința comună; reintegrarea victimei și, după caz, a copiilor în locuința comună; obligarea agresorului la păstrarea unei distanțe minime determinate față de victimă, membrii familiei, reședință, loc de muncă etc.; obligarea agresorului de a purta permanent un dispozitiv electronic de supraveghere; obligarea agresorului de a preda poliției armele deținute. Încălcarea OPP constituie infracțiune.

După confirmarea OPP, procurorul înaintează ordinul de protecție provizoriu, însoțit de documentele care au stat la baza emiterii și confirmării acestuia, judecătoriei competente în a cărei rază teritorială a fost emis, însoțit de o cerere pentru emiterea ordinului de protecție. În acest caz, OPP se transformă în ordin de protecție cu o durată de maxim 6 luni, care poate fi prelungită dacă instanța constată că starea de pericol persistă.

Dacă viața, integritatea fizică sau psihică ori libertatea este pusă în pericol printr-un act de violență din partea unui membru al familiei, persoana afectată poate solicita direct instanței emiterea unui ordin de protecție, în scopul înlăturării stării de pericol, prin care pot fi prevăzute **următoarele măsuri**: evacuarea temporară a agresorului din locuința familiei; reintegrarea victimei și, după caz, a copiilor, în locuința familiei; limitarea dreptului de folosință al agresorului numai asupra unei părți a locuinței comune; cazarea/plasarea victimei, cu acordul acesteia, și, după caz, a copiilor, într-un centru de asistență; obligarea agresorului la păstrarea unei distanțe minime determinate față de victimă, membrii familiei, reședință, loc de muncă, unitatea de învățământ a persoanei protejate etc.; interdicția pentru agresor de a se deplasa în anumite localități sau zone determinate; obligarea agresorului de a purta permanent un dispozitiv electronic de supraveghere; interzicerea oricărui contact, inclusiv telefonic, prin corespondență sau în orice alt mod, cu victima; obligarea agresorului de a preda poliției armele deținute; încredințarea copiilor minori sau stabilirea reședinței acestora; suportarea de către agresor a chiriei și/sau a întreținerii pentru locuința temporară unde victima, copiii minori sau alți membri de familie locuiesc sau urmează să locuiască; obligarea agresorului să urmeze consiliere psihologică, psihoterapie și poate recomanda internarea voluntară sau, după caz, poate solicita internarea nevoluntară.

Cea mai recentă modificare a Legii 217/2003 prevede introducerea sistemului de supraveghere a agresorilor prin brățară electronică, care ar oferi o mai mare siguranță persoanelor care au un OPP sau OP. Brățările trebuie montate atât persoanei agresate, cât și agresorului, și în cazul încălcării distanței minime prevăzute de ordinul de protecție, este generată o alertă la un dispecerat de urgență al poliției. Sistemul va fi pilotat în anul 2022 în Municipiul București.

De asemenea, Legea 217/2003 prevede și serviciile de care poate beneficia o persoană aflată într-o situație de violență, care pot fi înființate la nivel local sau județean, **în regim rezidențial** (centre de primire în regim de urgență, centre de recuperare, locuințe protejate), **în regim de zi** (centre pentru prevenirea și combaterea violenței domestice, centre pentru servicii de informare și sensibilizare a populației, centre de asistență destinate agresorilor) și **în regim continuu** (servicii de informare și consiliere pentru victimele violenței domestice de tip linie telefonică de urgență - help-line, servicii integrate de urgență destinate victimelor violenței sexuale).

În sprijinul persoanelor care sunt agresate în mediul online sau prin intermediul tehnologiei vin dispozițiile Codului Penal:

amenințarea (art. 206), șantajul (art. 207), hărțuirea (art. 208), traficul de persoane (art. 210), traficul de minori (art. 211), violul (art. 218), agresiunea sexuală (art. 219), actul sexual cu un minor (art. 220), coruperea sexuală a minorilor (art. 221), racolarea minorilor în scopuri sexuale (art. 222), hărțuirea sexuală (art. 223), violarea vieții private (art. 226), accesul neautorizat la informații (art. 228), fraudă informatică (art. 249), violarea secretului corespondenței (art. 302), falsul informatic (art. 325), infracțiuni contra siguranței și integrității sistemelor și datelor informatice (art. 360 - 365) - accesul ilegal la un sistem informatic, interceptarea ilegală a unei transmisii de date informatice, alterarea integrității datelor informatice, perturbarea funcționării sistemelor informatice, transferul neautorizat de date informatice, incitarea la ură și discriminare (art. 369), pornografia infantilă (art. 374), ultrajul contra bunelor moravuri (art. 375)

În cazul anumitor infracțiuni, sancțiunile aplicabile agresorilor sunt majorate dacă faptele au fost comise cu scopul de a produce materiale pornografice, inclusiv pornografie infantilă.

Pentru cele mai multe dintre infracțiunile de mai sus, victima are dreptul de a face plângere sau denunț la organele poliției și organele de urmărire penală.

La acest moment, Codul Penal nu incriminează în mod specific pornografia din răzbunare (revenge porn). O propunere legislativă inițiată în anul 2019, menită să completeze art. 226 din Codul Penal referitor la violarea vieții private, a fost adoptată în unanimitate de Senatul României, și a primit punct de vedere favorabil din partea Guvernului României, în aprilie 2020. Forma la care a ajuns inițiativa legislativă în urma observațiilor Guvernului face referire la scopul pentru care agresorul a divulgat imaginile intime, și anume *”răzbunare, umilire, intimidare sau hărțuire”*, ceea ce poate ridica probleme serioase în practică, făcând inoperabilă legea și, implicit, nesancționarea autorului, care poate nega că a avut aceste intenții.

Supraviețuitoarele sunt ezitante în a raporta violența sexuală și de gen, mai cu seamă violența cibernetică, iar tentativele lor de a căuta ajutor ar putea conduce la o escaladare a abuzului. În special în cazul violenței cibernetice, fluiditatea fenomenului face dificilă identificarea agresorilor și adunarea dovezilor. Uneori, se lovesc și de lipsa de înțelegere și suport din partea autorităților și de cadrul legislativ neacoperitor și insuficient de suportiv, în special în situațiile de agresiuni online transfrontaliere.

În ”Cercetarea privind nivelul de conștientizare a riscurilor digitale”, 53% dintre respondente au afirmat că au semnalat cuiva abuzul online - prieten, autorități, asistentului social/psihoterapeutului. Doar 40% dintre acestea au depus și o plângere oficială. În 69% din cazuri au primit ajutorul de care aveau nevoie.

Profesioniștii din mediul social au un rol extrem de important în a susține și orienta supraviețuitoarele în demersurile lor de accesare a serviciilor legale, de a le oferi informații, atât despre instrumentele legale, cât și despre modalitățile în care pot folosi în siguranță mediul online și tehnologia. Odată ce se vor simți în siguranță, nejudicate, credute, susținute și împuternicite (*empowered*), supraviețuitoarele vor avea suficient curaj pentru a face demersurile legale împotriva agresorilor. *Participantele la focus-grupurile organizate de Fundația Sensiblu în cadrul proiectului TECH-WISE, RISK-FREE au concluzionat ”Fără susținere, nu poți să faci față”.*

COMPORTAMENTUL
AGRESORULUI
ÎN MEDIUL ONLINE.
SPECIFICITĂȚILE VIOLENȚEI
CIBERNETICE ÎN CAZUL
RELAȚIILOR INTIME



4.1. AGRESORUL ȘI MOTIVELE LUI

Mediul online oferă agresorilor protecție sub mantia anonimității, acces facil și de la distanță la victimele lor, posibilitatea de a propaga imaginile și informațiile, care pot rămâne acolo pe termen nedefinit. Tehnologia este accesibilă, la îndemână, fie că vorbim despre dispozitive sau despre aplicații, și le permit să își mențină controlul și să agrezeze de la distanță.

În mediul online, în funcție de relația pe care o au cu persoana vizată, agresorii pot fi:

- **Partener sau fost partener** care vrea să își extindă și să își mențină controlul, dincolo de viața offline, uneori chiar și după ce relația s-a încheiat. Cele mai frecvente, constante și distructive forme de agresiune online, la fel ca și în offline, sunt comise de cineva apropiat victimelor, care are acces la informații despre ele, rețea de prieteni, date sensibile, fotografii etc. Urmărirea și controlul în mediul online din partea partenerului intim sau a fostului partener urmează aceleași tipare ca și în mediul offline, doar că se folosesc de tehnologie. Agresiunile în mediul online sunt, de cele mai multe ori, repetate, direcționate specific împotriva aceleiași persoane și pot continua în mediul offline.
- **Agresor cunoscut, dar nu partener** - poate fi un coleg de școală sau de serviciu, un vecin, un partener de afaceri, cu care victima a interacționat la un anumit moment, online și/sau offline.
- **Agresor necunoscut** - "crime of opportunity" - hărțuirea din partea unui necunoscut este mai frecventă decât am putea crede și mai înspăimântătoare decât din partea cuiva cunoscut. Agresorul este protejat de anonimitate, poate folosi conturi și platforme multiple, poate avea un comportament singular sau repetitiv, obsesiv, întins pe o perioadă mai lungă de timp. Anonimitatea contribuie la dezechilibrul de putere între victimă și agresor. Când interacționează cu un agresor necunoscut, persoanele targetate se simt lipsite de putere și se tem că amenințările din mediul online ar putea fi transpuse în viața reală. Victimele pot fi multiple și diverse, în funcție de factorul declanșator: aspect, idei emise în spațiul public, rasă, etnie, identitate sexuală, religie, profesie etc.

Raportul "Free to be online? - State of the World's Girls", realizat în 2020 de Plan International USA în 31 de țări, cu 14.000 de fete și femei tinere, arată că, în ciuda anonimității, în cele mai multe cazuri supraviețuitorii cunosc anumite detalii despre agresorii lor:

- 76% dintre respondenți cred că agresorul lor este bărbat;
- 29% cred că agresorul este de sex feminin;
- 47% afirmă că intuiesc care este vârsta agresorului;
- 18% consideră că agresorul/agresoarea din mediul online are credințe

religioase puternice;

- 6% dintre respondenți au oferit informații despre opiniile politice și rasa agresorului;
- Fetele și tinerele femei intervievate au afirmat că, cel mai frecvent, agresorul lor era de sex masculin.

• **Agresori secundari** sunt toți aceia care vizualizează, apreciază, distribuie imaginile sau informațiile, susțin și încurajează prin comentarii agresorii, contribuind la amplificarea abuzului și la revictimizare.

Pentru participantele la focus-grupurile organizate de Fundația Sensiblu în cadrul proiectului TECH-WISE, RISK-FREE, de mare ajutor a fost sprijinul primit din partea prietenilor, care au făcut front comun, au oferit suport, au blocat distribuirea.

Motivale și scopurile agresorilor online sunt:

- De a câștiga statut, demonstrând putere socială
- De a face de rușine
- De a denigra, a defăima
- De a umili
- De a-i determina pe ceilalți să acționeze împotriva unei persoane (*cyber mobbing*)
- De a produce frică, a intimidă, domina și de a menține controlul
- De a amenința, a reduce la tăcere victima
- De a izola victima
- De a se răzbuna
- Gelozia
- Agenda politică și ideologică
- Dorința sexuală
- De a obține avantaje financiare, prin șantaj sau trafic

Aceste agresiuni au ca scop producerea de suferință fizică, emoțională, coerciția și controlul și sancționarea comportamentului care deviază de la norma socială (*ansamblu de norme care reglementează relațiile sociale, conduita și acțiunile colectivităților umane*).

4.2. COMPORTAMENTUL AGRESORULUI

În mod specific în cazul relațiilor intime, sunt anumite semnale de alarmă la care ar trebui să fie atentă o persoană, care i-ar putea da de înțeles că partenerul folosește tehnologia și internetul pentru a o hărțui, urmări și controla.

- Vrea să știe permanent cu cine vorbește victima, o interoghează despre persoana de la telefon

- Sună în mod constant ca să îi spună unde e, uneori motivând că este preocupat de siguranța ei
- Dacă iese fără el, îi cere să transmită video pe WhatsApp, messenger sau îi cere fotografii pentru a vedea cu cine se întâlnește
- Pare că știe tot timpul unde se află victima și ulterior o interoghează despre motivele vizitelor în respectivele locuri
- Știe informații pe care victima nu i le-a spus, precum site-uri vizitate, locuri în care a fost, cu cine a vorbit, cui i-a trimis mesaje/e-mailuri etc.
- Interoghează despre prietenii de pe diverse platforme sociale
- Știe ce site-uri a vizitat, cu cine a schimbat mesaje
- Dispar contactele din agenda telefonică, adresele de e-mail
- Îi cunoaște parolele, chiar dacă nu i le-a împărtășit, parolele nu mai merg sau se schimbă permanent
- Mesajele și e-mailurile apar ca citite, trimise sau șterse
- Dispar bani din cont, persoana abuzată nu mai are acces la cont, sunt schimbate elementele de siguranță
- Contactează cercul de cunoscuți pentru a o verifica, pentru a afla informații sau pentru a-i amenința
- Răspândește zvonuri, informații neadevărate, face comentarii nepotrivite în mediul online despre victimă
- Trimite mesaje amenințătoare sau agresive
- Sună insistent și în mod repetat până i se răspunde sau folosește alte numere de telefon

51% dintre respondentele la "Cercetarea privind nivelul de conștientizare a riscurilor digitale" au afirmat că partenerul le verifica apelurile și mesajele pe ascuns, 41% aveau zeci de apeluri de la partener în fiecare zi, iar 23% erau apelate de pe alte numere de telefon, dacă nu mai răspundeau.

Agresorul poate să ofere niște explicații foarte plauzibile pentru comportamentul lui, invocând preocuparea pentru siguranța partenerei, în offline și în mediul online, nevoia de a o cunoaște mai bine, necesitatea unei transparențe totale în relație (inclusiv în ceea ce privește parolele sau conversațiile) și încredere reciprocă. De asemenea, când răspândește zvonuri despre victimă, se poate justifica spunând "asta este adevărul!"

În cazul unei persoane necunoscute sau cunosțințe, următoarele comportamente ar putea avertiza femeia că ar putea fi într-o relație virtuală abuzivă:

- Profilul nu pare real, este creat recent, puține postări și prieteni
- Contactează victima în mod constant, uneori și de câteva ori pe zi
- Vrea să știe cât mai multe detalii personale despre victimă: unde învață, unde locuiește, unde lucrează, numele animalului de companie, numele părinților etc.
- Pare mult prea implicat și interesat de persoană, mult prea repede

- Este de acord cu tot ceea ce îi spune victima, le plac aceleași lucruri, de parcă ar fi "sufilete pereche"
- Declară că e îndrăgostit sau că o place foarte tare după numai câteva discuții
- Își dorește să treacă foarte repede la un alt nivel al relației, să facă schimb de numere de telefon, să se întâlnească în viața reală
- Folosește alte conturi, dacă e blocat
- Vine constant cu alte versiuni ale poveștii lui
- Vrea să știe unde e, cu cine, de ce nu a mai intrat online
- Pare că știe când și pe ce platformă online se află victima sa
- Știe lucruri despre victimă pe care ea nu le-a spus
- Se împrietenește online cu prietenii și familia
- Inventează povești despre el și victimă, le povestește în online

Nu întotdeauna victima poate identifica aceste comportamente ca fiind abuzive, argumentele agresorului îi pot crea confuzie. De aceea, în evaluarea inițială a cazului făcută de un profesionist în domeniul social, întrebările referitoare la violența cibernetică și comportamentul agresorului ajută supraviețuitoarea în a identifica semnalele de alarmă de mai sus și de a conștientiza relația abuzivă.

4.3. SPECIFICITĂȚILE VIOLENȚEI CIBERNETICE ÎN CAZUL RELAȚIILOR INTIME

Când agresorul din mediul online este un partener sau fost partener, violența cibernetică nu este decât o prelungire a violențelor din viața reală. Agresorul se folosește de tehnologie și internet pentru a-și menține controlul asupra partenerii, pentru a o izola, amenința, pentru a o intimida, domina, extinzându-și controlul și abuzul dincolo de limitele spațiale și temporale.

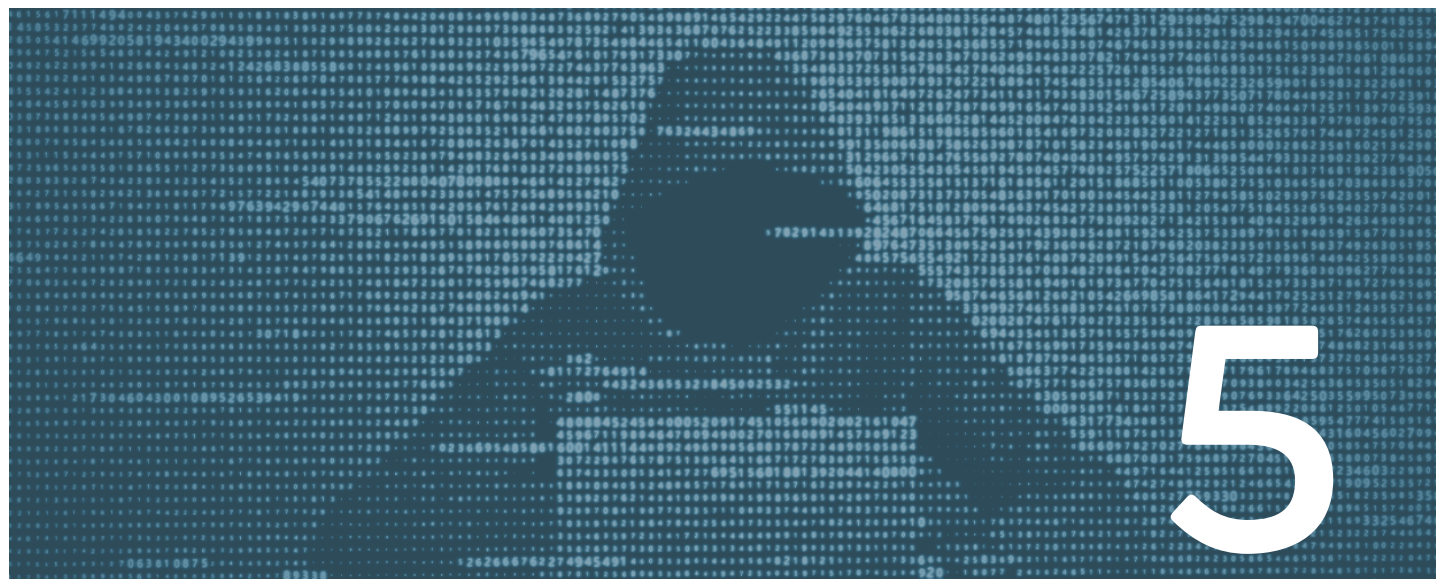
Factori care facilitează violența online:

- Existența unor relații intime, conviețuirea în același spațiu, complică păstrarea confidențialității. Agresorul este omniprezent, atât în mediul online, cât și offline.
- Împart prieteni, bunuri, copii, spațiu.
- Agresorul are acces fizic la victimă și amenințările pot fi puse în practică, în viața reală, în mod repetat.
- Are acces la informații despre victimă, cunoaște aspecte intime, parole, întrebări de siguranță.
- Are acces la dispozitivele pe care le folosește partenera: victima i-a oferit parolele pentru că "nu are nimic de ascuns", fie pentru că a fost forțată, i-au fost luate cu forța dispozitivele sau au fost verificate în timp ce dormea sau făcea duș.

- Are acces la rețeaua socială a victimei, la prieteni, familie extinsă, colegi, angajatori, ceea ce face dificilă excluderea/eliminarea agresorului. Impactul se extinde și asupra rețelei sociale și profesionale a victimei, ceea ce poate accentua izolarea acesteia, pierderea locului de muncă, afectarea imaginii și reputației. Partenerul poate manipula și controla cercul social al victimei, chiar înainte ca aceasta să își dea seama că este într-o relație violentă, ceea ce îi limitează posibilitatea de a căuta și găsi ajutor.
- Poate să o controleze prin diverse mijloace - GPS, instalarea de camere video, microfoane, chiar și după ce relația s-a încheiat, folosind copii.
- Informații ușor accesibile online, aplicații care pot fi descărcate și instalate, dispozitive care pot fi cumpărate.

Diversitatea tacticilor utilizate de agresor, a mijloacelor pe care le poate folosi pentru monitorizare și control, precum și dificultatea identificării lor și a probării abuzului cresc și mai mult hipervigilența și anxietatea victimei și generează o stare permanentă de frică. Agresorul este cu ea, chiar și când fizic nu e aproape.

IMPACTUL ASUPRA VICTIMELOR



O consecință majoră a violenței sexuale și de gen în mediul online este crearea unei societăți în care femeile nu se mai simt în siguranță online și/sau offline. Potrivit Internet **Governance Forum - Best Practice Forum** abuzul online contribuie, de asemenea, la o cultură a sexismului și misoginiei online și, în spațiile offline, la inegalitatea de gen existentă. În ceea ce privește acestea din urmă, abuzul online și violența de gen limitează capacitatea femeilor de a beneficia de aceleași oportunități online de care beneficiază în mod frecvent bărbații, de exemplu, la angajare, autopromovare și/sau auto-exprimare.

Similar celorlalte forme de violență sexuală și de gen din offline, violența cibernetică afectează viața victimelor la toate nivelurile: emoțional, fizic, psihologic, sexual, profesional, afectând bunăstarea economică și limitând implicarea socială, civică și politică.

La persoanele care s-au confruntat cu violența cibernetică, pot fi identificate următoarele consecințe:

- Tulburări emoționale și psihologice: anxietate, depresie, furie, stres post-traumatic și hipervigilență, frică, rușine, învinovățire, vulnerabilitate, gânduri suicidare
- Permanent sentiment de nesiguranță, online și offline
- Îngrijorări legate de siguranța fizică
- Îngrijorări legate de siguranța familiei sau că vor afla informațiile postate sau apărute în mediul virtual
- Izolare socială, retragerea din viața publică, îndepărtarea de familie
- Reducerea libertății de mișcare prin evitarea anumitor zone, restricții din partea familiei
- Auto-cenzura din teama de a mai utiliza internetul și pierderea încrederii în tehnologie
- Creșterea riscului de agresiune fizică
- Sentiment de lipsă de putere

Într-unul dintre focus-grupurile organizate în cadrul programul TECH-WISE, RISK-FREE, una dintre participante a descris toată această imixtiune a agresorilor din mediul online în viața lor ca "un viol".

În mediul online, linia de demarcație între privat și public se estompează. Ceea ce se întâmplă între două persoane, în privat, devine foarte repede accesibil tuturor, doar printr-un click. La nivel profesional, violența cibernetică afectează reputația, capacitatea de a-și îndeplini sarcinile de serviciu, productivitatea, abilitatea de a-și găsi și păstra un loc de muncă, afectează resursele financiare și capacitatea de a se întreține. Persoanele care au fost victimele unui act de violență în mediul online sunt îngrijorate că angajatorii pot afla că ele sunt hărțuite, șantajate și consideră că aceste acte pot afecta imaginea angajatorilor, sunt îngrijorate că își pot pierde locul de muncă și mijloacele de trai, ca urmare

a presiunilor pe care un agresor le poate face asupra colegilor, șefilor sau a dezvăluirii unor imagini cu conținut intim în colectivul de muncă.

Violența cibernetică este însoțită de costuri financiare ridicate, aferente încercării de a evita sau a compensa hărțuirea și abuzul. Victimele sunt nevoite să apeleze la serviciile unor avocați și psihologi pentru a ieși din situația de violență, precum și să solicite serviciile unor companii specializate în securitate pentru detectarea unor programe de urmărire și ascultare a telefonului, de identificare a dispozitivelor de urmărire de pe mașină sau a virușilor dintr-un computer, de exemplu.

Frecvent, persoanele care au fost agresate sunt nevoite să facă față atitudinii de blamare din partea celorlalți, fiind considerate vinovate pentru abuzul care s-a comis asupra lor. De exemplu, victima este considerată vinovată că a trimis imagini intime agresorului, nicidecum acesta pentru că le-a distribuit fără consimțământ, că se expune prea mult, că nu s-a gândit, că merită tot ceea ce i se întâmplă.

Facebook este una dintre platformele pe care astfel de atitudini pot fi identificate cu ușurință în comentariile utilizatorilor la diverse postări. De exemplu, în ianuarie, pe pagina unei emisiuni de știri a fost postată fotografia unei fete de 12 ani dispărută de acasă. Câteva dintre comentariile făcute ilustrează atitudinea de blamare a victimei:

Dzeu sa o aiba in paza! Dar la 12 ani.arata cam pensata, machiata, buze conturate...

Ce mă?

Am văzut comentarii că este vina autorităților

La 12 ani ce caută ea cu facebook,machiata etc..

Puteți să îmi dați cât hate vreți voi dar în maxim o săptămână o găsește poliția acasă la iubit

Vai și amar de părinții de azi că nu știu să aibă grijă de copii și să le interzică anumite lucruri

Îmi place · Răspunde · 44săpt.



4

Cine le pune să se îmbrace în colanți și fac câte și mai câte cum să nu fie băgate la prostituție dacă ele au un metru și un pic și le trebe câte și mai câte

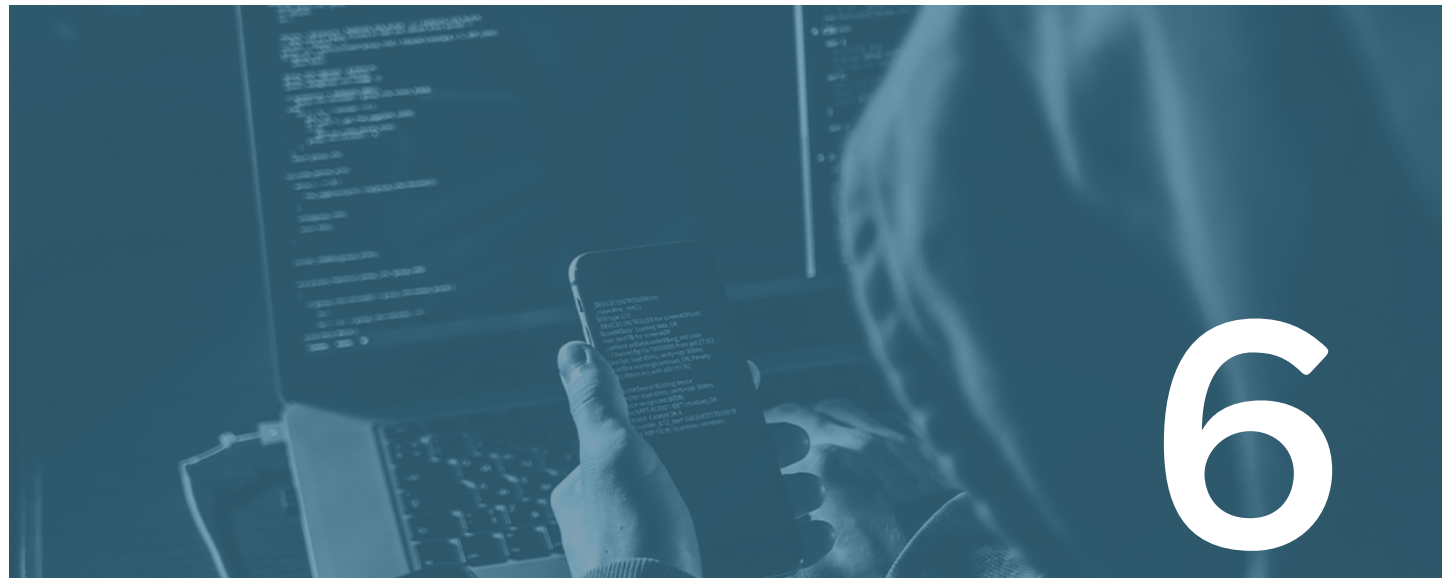
Îmi place · Răspunde · 44săpt.



1

Victimele violenței, indiferent dacă violențele se petrec în mediul online sau offline, se învinovățesc frecvent pentru ceea ce s-a întâmplat, iar atitudinea celorlalți creează suferință și revictimizare.

INTERVENȚIA PSIHO-SOCIALĂ ÎN CAZURILE DE VIOLENȚĂ CIBERNETICĂ



6.1. TRAUMA SI IMPACTUL ASUPRA SUPRAVIETUIȚOARELOR

Fiecare persoană este unică și atunci răspunsul la situațiile de violență este unul individual, determinat de nivelul de reziliență al fiecăreia, precum și de contextul socio-cultural în care se întâmplă, considerând *reziliența ca abilitatea unei persoane de a se recupera într-o situație dificilă, de a depăși și a face față provocărilor*.

Principiul fundamental în lucrul cu oamenii, în special cu persoanele aflate în situații de risc, care necesită protecție, este acela de „a nu face rău”, un principiu care poate crea nesiguranță și îngrijorare în rândul practicienilor, deoarece limitele sunt determinate de valorile personale, de percepții și de interpretări subiective a ceea ce înseamnă „a ajuta”. De aceea, serviciile specializate pentru supraviețuitoarele violenței sexuale și de gen au fost dezvoltate în acord cu principiile abordării centrată pe supraviețuitor. Deoarece peste 90% dintre persoanele afectate de violență sexuală și de gen manifestă semne și simptome specifice traumei, în acord cu statisticile, intervenția în astfel de cazuri trebuie să pună trauma în centrul lucrului cu supraviețuitorul.

Definiția traumei

- O reacție emoțională la un eveniment traumatizant, care include pierderea
- Reacție emoțională la un eveniment care este atât de traumatizant și stresant, încât zguduie ipotezele unei persoane despre viață, care îi dau înțeles și consistență
- Modalitatea psihicului de a face față
- Este caracterizată de sentimente ca: frică intensă, neputință, pierderea controlului, teama de anihilare

Evenimentul traumatic

- Acel eveniment care este interpretat drept o amenințare gravă la adresa existenței, siguranței și identității unei persoane, aceasta fiind copleșită mental, emoțional și fizic.

Tipuri de evenimente traumatizante

- experiențe privind amenințarea reprezentată de o pierdere
- experiențe privind amenințarea indusă de violență sau abuz
- supraviețuirea în urma unui dezastru sau unui război

Reacții emoționale la traumă	Reacții psihologice și cognitive la traumă	Reacții fizice și comportamentele la traumă
Șoc și neîncredere Frică și /sau anxietate Durere Vinovăție sau rușine Negare sau minimizare Depresie sau tristețe Furie sau iritabilitate Panică Reținere Disperare Deznădejde Detașare emoțională Sentiment de pierdere sau de abandon Nevoie crescută de control Amorțeală emoțională Dificultate de a avea încredere Schimbări de dispoziție Senzație de izolare Emoții intense sau inadecvate Izbucniri emoționale Senzație de copleșire Diminuarea interesului pentru activități Hipervigilență Retrăirea traumei Dorința de retragere Plâns spontan Tresărire exagerată Sentiment de neputință	Dificultăți de concentrare Gândire înceată Dificultate în luarea deciziilor Confuzie Dificultate în a opera cu cifrele Blamarea altora sau autotblamare Atenție redusă Rigiditate mentală Dezorientare Incertitudine Probleme cu memoria Dificultăți în rezolvarea problemelor Coșmaruri Flashback-uri/retrairi Gânduri intruzive Vise tulburătoare Suspiciune	Tulburări ale somnului Tulburări ale apetitului Oboseală Incapacitatea de a se odihni Izbucniri furioase Schimbare în interacțiunea cu alții Retragere sau izolare Bătăi rapide ale inimii Greață sau stomac deranjat Dureri Sensibilitate crescută la îmbolnăvire Pierderea simțului umorului Leșin Amețeală Slăbiciune Scrâșnirea dinților

Reacțiile la traumă se suprapun cu consecințele violenței sexuale și de gen și sunt normale în context traumatic.

6.2. ABORDAREA CENTRATĂ PE SUPRAVIEȚUITOR*

Modelul de intervenție în cazurile de violență sexuală și de gen pe care îl propunem folosește o abordare centrată pe supraviețuitor, care urmărește împuternicirea/capacitarea acestuia, prioritizând drepturile, nevoile și dorințele lui.

Rolul practicienilor care interacționează cu supraviețuitorul este **de a crea o relație în care acesta să fie privit dincolo de condiția de victimă, în care să se simtă în siguranță și susținut într-un mod adecvat, în acord cu nevoile și dorințele sale; de a-i vedea capacitățile și resursele**, având un rol determinant în dezvoltarea rezilienței; **de a susține persoana atât într-un mod practic - oferă informații adecvate despre drepturi, obligații, servicii în comunitate pe care aceasta le poate accesa; de a acorda suport psihosocial - bazat pe o viziune holistică asupra persoanei și a situației în care se află.**

Abordarea încurajează recuperarea supraviețuitorului și dezvoltă capacitatea acestuia de a identifica și exprima nevoile și dorințele. De asemenea, încurajează consolidarea abilității acestuia de a lua decizii cu privire la posibile intervenții.

Principiul siguranței și al protecției

- Siguranța psihică și fizică a supraviețuitorului, a copiilor și a familiei este prioritară pentru orice program de intervenție și este avută în vedere încă de la primul contact cu acesta, pe tot parcursul intervenției, indiferent de alegerile acestuia
- Atunci când vorbim despre siguranța supraviețuitorului este necesar să avem în vedere dacă acesta este în risc de a fi agresat, atât offline, cât și online, ucis sau se poate sinucide. În consecință, are nevoie de un plan de siguranță, realizat în urma evaluării situației și a contextului de viață în care se află, în vederea prevenirii riscului de recidivă și pericol
- Implicarea supraviețuitorului în identificarea factorilor de risc online și offline, precum și în crearea și respectarea planului de siguranță este esențială
- Aspectele menționate în planul de siguranță sunt confidențiale și trebuie respectate de către toți profesioniștii cu care acesta intră în contact
- Orice schimbare în deciziile și viața supraviețuitorului implică reevaluarea planului de siguranță

Recomandări pentru practicieni

- Identificați factorii de risc pe care îi implică dispozitivele tehnologice, precum și activitatea online a supraviețuitorului
- Explicați rolul măsurilor de siguranță
- Identificați în comunitate servicii care să răspundă acestei nevoi
- Implicați ceilalți practicieni și autoritățile în realizarea planului de siguranță (cooperare multidisciplinară și interinstituțională), cu acordul informat al supraviețuitorului
- Solicitați sprijinul practicienilor cu competențe în realizarea unor demersuri juridice pentru securizarea supraviețuitorului (ordin de protecție, plângere penală etc.)

Ce să faceți	Ce să NU faceți
Păstrați confidențialitatea și respectați dorințele supraviețuitorului.	Nu forțați supraviețuitorul să ia decizii pentru care nu este pregătit.
Întotdeauna cereți acordul supraviețuitorului pentru orice acțiune.	Nu presupuneți că supraviețuitorul este de acord cu acțiunile voastre.
Evaluati potențialele riscuri în fiecare etapă când sprijiniți supraviețuitorul.	Nu luați decizii pentru supraviețuitor și nu grăbiți acțiunile fără a evalua consecințele.
Ajutați supraviețuitorii în prevenirea riscurilor folosind serviciile și soluțiile disponibile în comunitate.	Nu referiți supraviețuitorul imediat către un adăpost fără a evalua atent consecințele.
Nu pierdeți din vedere siguranța celorlalți implicați - copii, membri ai familiei și cei care au ajutat supraviețuitorul.	Nu vă concentrați doar pe siguranța supraviețuitorului. Și siguranța altor persoane poate fi afectată!

Principiul confidențialității

- Este un principiu prioritar, reprezentând un drept al supraviețuitorului și o responsabilitate a profesionistului în cadrul intervenției, menit să consolideze sentimentul de siguranță, încrederea și relația acestora.

Limitele confidențialității:

- Când persoana vrea să se sinucidă sau vrea să facă rău altei persoane;
- Când o solicită instanța de judecată;

Dincolo de cerințele legale, organizațiile/instituțiile trebuie să aibă politici și proceduri cu privire la modul în care utilizează informațiile confidențiale. Politicile și procedurile la care se raportează practicianul ar trebui să includă linii directoare pentru:

- comunicarea verbală (între supraviețuitor și practician)
- documentația scrisă (dosare, acte, rapoarte etc.)
- comunicarea electronică
- furnizarea de informații terților
- înregistrarea datelor și stocarea acestora

Recomandări pentru practicieni

- Acest principiu trebuie prezentat de la începutul discuției, inclusiv situațiile în care poate fi încălcat. Atunci când situația o impune, acest lucru se va face cu acordul informat al persoanei în cauză.
- Nu împărtășiți informații despre supraviețuitor cu alte persoane sau autorități decât cu acordul său informat.

Consimțământul informat

- Consimțământul informat este dat în mod voluntar și liber pe baza

unei aprecieri clare și a înțelegerii faptelor, implicațiilor și consecințelor viitoare ale unei acțiuni.

- Pentru a-și da consimțământul informat, persoana în cauză trebuie să aibă toate informațiile relevante la momentul acordării consimțământului și să fie capabilă să evalueze și să înțeleagă consecințele unei acțiuni.
- De asemenea, trebuie să fie conștienți și să aibă puterea de a-și exercita dreptul de a refuza angajarea într-o acțiune și/sau sau de a nu fi constrânși (folosind forța sau amenințările) sau a face pe plac specialiștilor.
- În general, copiii sunt considerați incapabili de consimțământ informat, deoarece nu au capacitatea și/sau experiența de a anticipa implicațiile unei acțiuni și este posibil să nu înțeleagă sau să nu aibă puterea de a-și exercita dreptul de a refuza. Se recomandă informarea copiilor și implicarea în deciziile care îi privesc, în acord cu capacitatea lor de a înțelege și a decide.
- Există, de asemenea, cazuri în care consimțământul ar putea să nu fie posibil din cauza deficiențelor cognitive și/sau dizabilităților fizice, senzoriale sau de dezvoltare. (Institutional Framework for Addressing Gender-Based Violence in Crises, Organizația Internațională pentru Migrație, 2017)

Ce să faceți	Ce să NU faceți
Realizați interviul fără a fi prezente alte persoane sau fără a fi auzit de alte persoane.	Nu intervievați supraviețuitorul în prezența altor persoane. Nu vorbiți public despre supraviețuitor.
Intervievați supraviețuitorul singur, nu în prezența rudelor, prietenilor sau aparținătorilor. Acest aspect este valabil și când acest lucru se întâmplă telefonic sau online.	Nu presupuneți faptul că minorii vor să fie intervievați în prezența îngrijitorilor. Nu presupuneți că pentru persoanele vârstnice sau cu dizabilități este ușor să vorbească cu practicienii.
Cereți acordul supraviețuitorului sau îngrijitorului când este în interesul copilului, înainte de a transmite informații relevante celorlalți. Asigurați-vă că supraviețuitorul înțelege riscurile și consecințele transmiterii informațiilor, înainte de a-și da sau nu acordul.	Nu presupuneți că supraviețuitorii înțeleg ce înseamnă transmiterea de informații.
Păstrați documentele într-un loc sigur.	Nu lăsați dosarele supraviețuitorilor în locuri în care au acces și alte persoane (în afara practicienilor) și nu le luați acasă.
Folosiți un cod atunci când transmiteți informații despre supraviețuitor.	Nu împărtășiți informații despre supraviețuitor (etnie, vârstă, identitate sexuală sau de gen, situația familiei), chiar dacă numele nu este spus. Există riscul ca acesta să fie recunoscut!

Principiul respectului

- Supraviețuitorul este actorul principal în cadrul intervenției, astfel nevoile, dorințele și drepturile sale trebuie respectate în orice moment.
- Violența sexuală și de gen implică pierderea controlului supraviețuitorului asupra propriei vieți; în procesul de recuperare, implicarea în identificarea propriilor soluții, luarea deciziilor în funcție de propriile dorințe și nevoi, contribuie la redobândirea încrederii în sine și a sentimentului propriei valori.

Recomandări pentru practicieni

- Nu insistați ca o persoană să vorbească sau să se destăinuie
- Nu judecați cele spuse
- Oferiți-i informații despre drepturi și servicii utile, însă respectați dreptul de a alege să le acceseze sau nu
- Respectați alegerile chiar dacă nu sunteți de acord cu ele (de ex. supraviețuitorul alege să rămână în relația abuzivă)
- Acceptați și normalizați trăirile, emoțiile, sentimentele
- Cereți permisiunea pentru a solicita informații despre situații dificile, sensibile și asigurați persoana că are dreptul de a nu răspunde
- Pentru orice acțiune sau demers în interesul supraviețuitorului este necesar acordul acestuia

Ce să faceți	Ce să NU faceți
Transmiteți faptul că îl credeți pe supraviețuitor.	Nu cereți dovezi și nu minimizați comportamentele violente.
Reduceți numărul situațiilor în care supraviețuitorul trebuie să repete povestirea situației experimentate.	Nu cereți supraviețuitorului să repete povestirea situației de violență.
Exprimați disponibilitatea de a asculta experiențele supraviețuitorului și oferiți-i oportunitatea de a vorbi.	Nu subapreciați sentimentele supraviețuitorului.
Arătați faptul că vă pasă de supraviețuitor și normalizați sentimentele acestuia.	Nu acuzați și nu judecați supraviețuitorul. Nu întrebați „De ce?”
Exprimați clar faptul că nu este vina supraviețuitorului pentru ce s-a întâmplat.	Nu-i spuneți supraviețuitorului ce să facă.
Asistați supraviețuitorul în luarea propriilor decizii.	Nu forțați supraviețuitorul să solicite servicii.
Prezentați modurile în care poate fi ajutat, inclusiv beneficiile și riscurile și încurajați supraviețuitorul să ia propriile decizii.	Nu cereți detalii și nu forțați supraviețuitorul să vorbească.
Abordați supraviețuitorul într-un mod deschis, cu atenție la contextul cultural și social.	Nu judecați. Nu faceți presupuneri despre istoria de viață a supraviețuitorului. Nu vă lăsați opiniile să vă determine modul în care abordați supraviețuitorul.

Principiul nediscriminării

- Fiecare persoană are dreptul la servicii de asistență fără discriminare pe bază de gen, vârstă, dizabilități, rasă, culoare, limbă, identitate sexuală și de gen, statut social etc.

Recomandări pentru practicieni

Ce să faceți	Ce să NU faceți
Asigurați-vă că serviciile răspund nevoilor tuturor grupurilor de supraviețuitori, inclusiv băieți și bărbați, persoane cu dizabilități, persoane vârstnice, persoane LGBTQIA.	Nu presupuneți că toți supraviețuitorii au aceleași convingeri.
Demonstrați faptul că serviciile pot răspunde nevoilor tuturor grupurilor, prin distribuirea unor materiale educative.	Nu folosiți materiale educaționale care abordează doar supraviețuitoare femei.
Promovați valori, atitudini și convingeri care susțin nediscriminarea.	Nu presupuneți că toți practicienii au aceleași valori.

*Material preluat din *Ghid privind violența sexuală și de gen pentru practicieni care lucrează în domeniul azilului*, realizat de Fundația Sensiblu pentru Asociația Serviciul Iezuiților pentru Refugiați din România (JRS România).

6.3. EVALUAREA CAZURILOR DE VIOLENȚĂ

Frecvent, serviciile sociale pot fi punctul de intrare al unei persoane aflate într-o situație de violență în sistemul de protecție și asistență. Profesioniștii folosesc managementul de caz ca principală metodă de lucru cu cazurile, parcurgând următoarele etape (conform OG 68/2003 privind serviciile sociale), interdependente:

- a) evaluarea inițială;
- b) elaborarea planului de intervenție;
- c) evaluarea complexă;
- d) elaborarea planului individualizat de asistență și îngrijire;
- e) implementarea măsurilor prevăzute în planul de intervenție și în planul individualizat;
- f) monitorizarea;
- g) reevaluarea;
- h) evaluarea opiniei beneficiarului.

În furnizarea de servicii specializate, profesionistul poate întâlni beneficiare care au informații despre violența cibernetică comisă de către partenerul intim, o cunoștință sau o persoană necunoscută. La fel de bine, mai ales în situațiile de violență domestică, persoana care solicită ajutorul poate să nu conștientizeze modul abuziv în care partenerul/fostul partener folosește

tehnologia pentru a o controla, urmări sau hărțui și este responsabilitatea profesionistului de a explora, împreună cu beneficiara, posibilitatea existenței unor astfel de agresiuni.

Din cauza riscului mare la adresa vieții și siguranței supraviețuitoarei, prin accesul fizic permanent al agresorului la victimă și a piedicilor puse în căutarea ajutorului, o atenție deosebită ar trebui acordată cazurilor în care violența cibernetică este exercitată de partenerul intim.

În lucrul cu cazurile de violență, este foarte importantă etapa evaluării inițiale, în care sunt colectate date și informații despre abuz, având în centru nevoile imediate de protecție și siguranță, corelate cu evaluarea riscului și abordate în planul de siguranță.

În procesul de evaluare a unei situații de violență domestică, sunt colectate următoarele tipuri de informații:

- Date cu caracter personal despre victimă: identitate, CNP, domiciliu, ocupație, venituri, studii, stare de sănătate fizică și mintală
- Date cu caracter personal despre agresor: identitate, vârstă, ocupație, venituri, studii, stare de sănătate fizică și mintală, antecedente penale, permis port-armă
- Date despre copii: identitate, vârstă, studii, stare de sănătate
- Certificate INML, dacă agresiunea s-a petrecut și în viața reală
- Consum de alcool, substanțe interzise, medicamente fără rețetă
- Descrierea abuzului (formele, frecvența, când a început abuzul, ultimul incident violent)
- Istoricul relației dintre parteneri/victimă și agresor și explicații ale comportamentului violent al agresorului
- Abuzul asupra copiilor, în cazul în care agresorul este partenerul intim
- Relația părinți-copii (mamă-copii; tată-copii)
- Demersurile întreprinse în vederea soluționării situației de abuz (plângere penală, ordin de protecție, ordin de protecție provizoriu, sesizări la DGASPC, alte ONG-uri)
- Informații despre familia de origine a victimei și a agresorului
- Evaluarea gradului de risc
- Nevoile și resursele identificate de către persoana agresată
- Nevoile și resursele identificate de către consilier

Se folosesc instrumente proprii organizației/serviciului, în acord cu reglementările în vigoare.

Violența cibernetică fiind o formă de violență domestică, așa cum profesionistul ia în considerare aspectele legate de violența fizică, emoțională, socială, economică, sexuală, considerăm necesar ca orice fișă de evaluare inițială și complexă a unui caz să conțină întrebări referitoare și la

violența cibernetică, care pot ajuta atât profesionistul, cât și supraviețuitorul în identificarea formelor, riscurilor și includerea lor în planul de siguranță.

În cazul unui agresor necunoscut din mediul online, detaliile despre agresor pot să nu fie cunoscute sau accesibile victimei, dar pot oferi informații despre interacțiunea dintre ei, tacticile și platformele pe care le folosește agresorul, demersurile făcute de victimă.

Evaluarea inițială și complexă reprezintă un proces care o ajută pe persoana afectată de violență să înțeleagă, să identifice și să clarifice nevoile, precum și la structurarea și identificarea resurselor de care dispune pentru a ieși din situația abuzivă. Se creează un cadru în care ea poate să își exprime propriile credințe, percepții, temeri, ipoteze, convingeri despre ea, despre agresor și relația lor.

În procesul de colectare a datelor, sunt de interes experiențele pe care persoana asistată le-a avut în mediul online sau în utilizarea tehnologiei - dacă primește mesaje repetate, obsesive, din partea aceleiași persoane; dacă a fost hărțuită sau monitorizată în vreun fel, dacă a fost amenințată de cineva prin mesaje sau pe platformele sociale că îi va face rău ei sau cuiva apropiat, dacă a fost șantajată cu expunerea unor imagini cu conținut intim, dacă i s-a întâmplat vreodată ca cineva să îi adreseze comentarii răutăcioase sau care i-au adus atingere reputației, dacă a accesat link-uri necunoscute primite prin sms/messenger etc.

6.3.1. EVALUAREA RISCULUI

Informațiile colectate în procesul de evaluare inițială și complexă sunt esențiale în evaluarea riscului în care se află persoana agresată. Acesta este un proces complex, prin care sunt identificați factorii de risc și de protecție într-o situație de violență, precum și percepția victimei legată de riscul în care se află.

În acest proces de evaluare a riscului, sunt avute în vedere următoarele elemente:

- estimarea gradului de pericol actual în care se află persoana agresată
- istoricul abuzului
- frecvența actelor de violență și severitatea leziunilor
- comportamentul agresiv, în general
- comportamentele bizare ale agresorului, care atrag atenția
- comportamentul agresiv față de copii
- comportamentul agresiv față de persoanele din afara familiei
- fluctuațiile de comportament ale agresorului
- deținerea și folosirea de arme.

Unul dintre cei mai puternici indicatori ai riscului este reprezentat de comportamentul trecut și prezent al agresorului. În evaluarea standard pot fi introduse întrebări care să indice riscul imediat pentru siguranța victimei.

Un instrument care poate fi folosit este reprezentat de **FIȘA pentru evaluarea gradului de risc și măsuri de siguranță necesare pentru victimele violenței domestice**, stabilită prin Ordinul nr. 2525/2018 privind aprobarea Procedurii pentru intervenția de urgență în cazurile de violență domestică, a cărei itemi vin în ajutorul profesioniștilor pentru determinarea nivelului de risc.

În mod specific, în situațiile de violență cibernetică, întrebările pe care le adresăm sunt legate de elementele care vulnerabilizează în mediul online (pag. 16): obiceiurile și comportamentele în online - ce postează, cu ce regularitate, dacă socializează online cu persoane necunoscute etc.; dispozitivele, platformele folosite și cine are acces la ele; informațiile pe care le deține, unde le stochează și cine are acces la ele; grupurile și rețelele din care face parte; momentul din viață în care se află - într-o relație, locuiește cu agresorul, se pregătește să plece de acasă etc.

Cu cât o persoană utilizează mai multe dispozitive și platforme, are un cerc mai mare de "prieteni" virtuali, pe care nu îi cunoaște neapărat din viața reală, cu care interacționează frecvent, cu atât probabilitatea de a fi victimă crește.

Sunt explorate îngrijorările despre riscul utilizării tehnologiei, prin întrebări precum:

- Posibilitatea ca cineva să îți facă rău fizic te preocupă? Există vreun risc ca agresorul să aibă acces la tine, în viața reală?
- Cum te contactează agresorul? Cum interacționează cu tine în mediul online? Ce platforme folosește?
- Cum s-a schimbat comportamentul agresorului în timp? Observi o diferență între mesajele primite anterior și cele de acum - conținut, frecvență?
- Ești îngrijorată că partenerul/agresorul știe tot timpul unde ești? Cum crezi că poate afla acest lucru?
- Ești îngrijorată că partenerul/agresorul poate accesa conversațiile tale cu alte persoane/că îți monitorizează conversațiile? Ce metode ar putea folosi?
- Ești îngrijorată de informațiile despre tine în mediul online? Prin ce canale ar putea fi făcute publice?
- Ești îngrijorată că modul în care prietenii/familia/copiii folosesc tehnologia te-ar putea pune în pericol? Cum s-ar putea întâmpla asta?
- Te îngrijorează că modul în care folosești tehnologia îți pune în pericol siguranța și intimitatea? Care sunt îngrijorările tale principale legate de siguranță și intimitate/confidențialitate?

Siguranța persoanei afectată de violență este prioritizată încă de la momentul primului contact cu serviciile specializate, care uneori poate să

aibă loc telefonic. Profesionistul are responsabilitatea de a se asigura că telefonul este o metodă sigură de contact prin întrebări țintite: E cineva lângă dumneavoastră care aude convorbirea? Aveți suspiciuni că cineva ar putea asculta telefonul? Partenerul obișnuiește să vă verifice mesajele și listele de apeluri?

După cum e precizat mai sus, nu întotdeauna beneficiara are cunoștință de existența unei monitorizări telefonice, dar responsabilitatea profesionistului este de a nu o pune în pericol, prin urmare o recomandare pe care o poate face în discuția telefonică este de a șterge numărul de telefon al centrului/ serviciului din lista de apeluri sau de a-l salva sub o denumire care nu poate trezi suspiciuni agresorului.

6.3.2. PLANUL DE SIGURANȚĂ

Planul de siguranță este un instrument indispensabil în lucrul cu supraviețuitoarele violenței de orice fel - sexuală și de gen, domestică sau cibernetică.

Cazurile de violență domestică implică unele dintre cele mai dificile categorii de probleme din domeniul social, femeile și copiii fiind cei mai vulnerabili. În cazurile de violență domestică, nevoile de siguranță și securitate pot depăși nevoile fiziologice, motiv pentru care aceste două nevoi se află în centrul serviciilor oferite.

Colectarea informațiilor în procesul de evaluare inițială și complexă, precum și evaluarea riscului, sunt esențiale pentru construirea unui plan de siguranță adaptat situației în care se află persoana afectată de violență. Atunci când partenerul folosește și tehnologia sau internetul pentru a-și menține controlul asupra victimei sale, planul trebuie să ia în considerare și acest aspect.

Mai mult decât atât, câteva aspecte legate de siguranță sunt discutate de la primul contact cu beneficiara, fie că este față în față sau telefonic. De reținut că momentul plecării de acasă este unul dintre cele mai periculoase pentru o victimă, când riscul de a fi ucisă crește, de aceea necesită o pregătire prealabilă foarte atentă și un plan de siguranță complex.

Scopurile întocmirii planului de siguranță

- Ajută persoana să anticipeze și să planifice
- O pregătește ca în situații critice să reacționeze într-un mod care conferă mai multă protecție pentru ea și copiii ei
- O ajută să se focalizeze pe siguranța și bunăstarea ei și a copiilor pe termen lung
- O ajută să conștientizeze ce puțin poate să facă pentru a se proteja pe ea și pe copiii ei
- Este vital pentru o victimă, dar nu e general valabil pentru toate. Se va ține cont în întocmirea planului de tipul de violență (fizică, emoțională,

socială, cibernetică etc.) și de relația cu agresorul (partener, locuiesc sau nu împreună, agresor necunoscut, cunoștință)

- Acoperă orice locație/situație în care se poate afla victima
 - o Acasă, serviciu, stradă, școală, judecătorie, internet etc.
- Este un document dinamic, viu
 - o Este actualizat ori de câte ori se schimbă circumstanțele
 - o Victima este încurajată să aibă încredere în propriile instincte și să modifice planul în timp real
- Este individualizat
 - o Identifică elementele care vulnerabilizează victima
 - o la în considerare contextul - dacă este vorba despre violență sexuală și de gen, violență domestică sau violență cibernetică
 - o la în considerare etapa în care se află victima: locuiește cu partenerul, se pregătește să plece de acasă, a plecat de acasă
 - o Identifică resursele specifice pentru fiecare victimă
 - o Include și copiii, dacă e cazul
- Este securizat și securizant
 - o Documentele, inclusiv cele cu planul de siguranță sunt păstrate în loc sigur, la care agresorul nu are acces
 - o Se stabilesc semnale de siguranță confidențiale cu rudele, prietenii, colegii etc.

Pașii planului de siguranță

- *Evaluarea pericolului:* este important ca victima să conștientizeze gradul de pericol în care se află ea și copiii ei și să acționeze în consecință
- *Reducerea vulnerabilității față de violență:* transmiterea de informații privind tacticile abuzatorilor și strategiile de supraviețuire pentru a crește încrederea în sine
- *Creșterea autonomiei victimei* - victima este susținută de către profesioniști în toate demersurile pe care le întreprinde, dar deciziile îi aparțin în totalitate
- *Identificarea unui loc în care victima să fie în siguranță*
- *Includerea copiilor în planul de siguranță*
- *Pregătirea pentru plecarea de acasă* - bani, numere de telefon, acte, haine pentru ea și copil, alte lucruri care ar putea să-i fie utile
- *Protecție legală* - oferirea de informații juridice
- *Dezvoltarea unei rețele de suport.*

Un plan de siguranță complex, elaborat de Fundația Sensiblu, care acoperă multiple situații în care s-ar putea afla o supraviețuitoare a violenței domestice poate fi consultat la finalul ghidului. Acesta ar trebui personalizat în funcție de situația specifică în care se află persoana agresată.

Ca un model de bună practică, Direcția de Asistență Socială (DAS) Bistrița, unul dintre serviciile înrolate în programul de coaching, a colaborat cu Serviciul Ordine Publică la crearea planului de siguranță. Colaborarea a avut ca rezultat întocmirea unei hărți a spațiilor sigure în care femeile cărora le

oferă asistență se pot refugia în cazul în care sunt urmărite de partener pe stradă - spații comerciale cu camere de luat vederi sau pază, secțiile de poliție rurale. De asemenea, în construirea planului de siguranță individualizat, specialiștii DAS stabilesc împreună cu beneficiara o zonă sigură pentru rutina zilnică - mersul la serviciu, la școala copiilor, pentru activitate fizică sau pentru cumpărături, diferită de cea avută înainte de părăsirea partenerului agresiv, pentru a reduce riscul întâlnirii cu acesta.

Această abordare este de ajutor și beneficiarelor care nu sunt din localitate și cunosc prea puțin zona, oferindu-le siguranță și control asupra spațiului în care se deplasează.

În planul de siguranță este luată în calcul și o potențială întâlnire cu agresorul într-un spațiu public. Împreună cu beneficiara este stabilită o procedură care prevede identificarea unui spațiu sigur în care să se refugieze, apelarea 112 și semnalarea situației reprezentantului serviciilor sociale.

Securitatea digitală, parte a planului de siguranță

În lucrul cu cazurile de violență, fie că sunt de violență sexuală și de gen sau violență domestică, siguranța și securitatea cibernetică/în mediul online ar trebui integrate în planul de siguranță general.

Evaluarea de risc făcută anterior și identificarea elementelor care vulnerabilizează în mediul online reprezintă punctul de pornire pentru construirea unui plan de utilizare în siguranță a mediului online și a tehnologiei, astfel încât să nu fie pusă în pericol securitatea datelor și a persoanelor, fie că vorbim despre beneficiara de servicii sau despre personal.

Astfel, în construirea planului de siguranță cibernetică, sunt avute în vedere aspecte legate de:

- Securitatea documentelor - identificarea unor locuri sigure în care să fie păstrate, fie că sunt documente fizice, fie electronice (fotografii, înregistrări)
- Securitatea comunicării - utilizarea telefonului și a aplicațiilor în siguranță, menținerea legăturii cu serviciile și persoanele apropiate fără să se pună în pericol pe sine sau pe ceilalți
- Securitatea dispozitivelor - parolarea dispozitivelor, restricționarea accesului celorlalți la echipamente, virușii, aplicațiile de monitorizare, geolocalizarea
- Utilizarea sigură a internetului - cum poate să se bucure de accesul la internet fără să se pună în pericol, să nu descarce aplicații din surse nesigure sau să caute în siguranță informații necesare pentru ieșirea din relația abuzivă (servicii, informații juridice, specialiști etc.)
- Utilizarea sigură a social media - prezența în social media, prietenii, profilurile și postări publice și private, geolocalizarea, etichetarea etc.

MĂSURI DE CREȘTERE A SIGURANȚEI ÎN MEDIUL ONLINE



7

Mediul online și tehnologia sunt într-o evoluție constantă, care depășește capacitatea utilizatorului de a ține pasul cu schimbările, de a descoperi și înțelege toate riscurile și de a-și integra metodele de utilizare sigură. Nu e suficient să învățăm modul de utilizare al unui echipament, aplicații sau platforme, avem nevoie să înțelegem și care sunt termenii și condițiile de utilizare, ce este permis și ce nu este permis să facem online, felul în care suntem expuși când folosim aplicațiile și dispozitivele și cum putem fi în siguranță.

În cazul unor agresiuni în mediul online, recomandarea de a renunța la telefon, de a-și închide conturile sau de a se retrage din mediul online nu este o soluție, supraviețuirea fiind cea care trebuie să suporte din nou consecințele unui comportament nepotrivit al agresorului și al modului în care acesta alege să folosească tehnologia. O astfel de măsură izolează supraviețuirea de grupul de prieteni, de familie, îi afectează viața socială și profesională. Nu este o garanție că renunțarea la tehnologie va face ca abuzul să înceteze, ci poate determina agresorul să găsească noi modalități de a hărțui și să afecteze capacitatea victimei de a căuta și găsi ajutor. Schimbarea numărului de telefon, a adresei de e-mail sau conturilor sunt strategii protective, dar nu soluții, întrucât nu supraviețuirea ar trebui să fie cea care să își schimbe viața pentru a se adapta hărțuirii și controlului abuziv al altcuiva. De asemenea, accesul la tehnologie și conturi poate fi util și în procesul de strângere a dovezilor și monitorizării agresorului, permițând astfel supraviețuitorii să fie cu un pas înaintea.

Stabiliți cu beneficiara modalități sigure de contact, eventual de pe telefonul unui prieten sau oferiți-i pentru utilizare un telefon cu cartela prepaid sau cu butoane.

Pentru profesioniștii care oferă servicii specializate persoanelor aflate într-o relație violentă e necesară cunoașterea măsurilor de creștere a siguranței online, pentru a reduce vulnerabilitatea beneficiarei în mediul online și pentru a o sprijini în construirea unui plan de siguranță eficient.

Parolele

Parolarea reprezintă una dintre primele măsuri pe care le putem lua pentru protejarea conturilor și dispozitivelor. Anumite site-uri care cer conectarea cu cont specifică criteriile pe care trebuie să le îndeplinească o parolă pentru a fi sigură: minim 8 caractere, obligatoriu o literă mare și un caracter special.

De reținut despre parole:

- Recomandarea e de minim 16 caractere, 26 e și mai bine. Cu cât este mai lungă parola, cu atât e mai dificil de spart. De exemplu, puteți să vă verificați propria parolă pe site-ul <https://howsecureismypassword.net/>, care vă indică în cât timp un computer ar putea sparge parola utilizată.

Puteți verifica dacă parolele sau conturile utilizate au fost implicate într-un furt de date pe <https://haveibeenpwned.com/>

- Folosiți parole diferite pentru fiecare cont sau dispozitiv
- Folosiți combinații de litere mari, litere mici, cifre și caractere speciale
- Puteți înlocui vocalele cu caractere speciale (de exemplu, a cu @)
- Puteți folosi o frază, un vers, un citat preferat
- Parolele trebuie să fie confidențiale, cunoscute doar de utilizator
- Pot fi stocate într-un password manager (Keychain pentru iOS, LastPass, Dashlane etc.), care se accesează cu o parolă unică
- Nu le salvați în browserul de internet, de exemplu Google password manager, mai ales când o altă persoană are acces la dispozitivul respectiv, întrucât poate accesa și conturile fără dificultate prin completarea automată a userului și parolei

Profioniștii care lucrează cu cazuri de violență cibernetică pot fi tentați să recomande beneficiarilor să schimbe parolele conturilor pentru a restricționa accesul partenerului agresiv la acestea. Recomandabil este să se ia în considerare situația specifică în care se află supraviețuitoarea. De exemplu, dacă aceasta continuă să locuiască împreună cu agresorul, orice schimbare de comportament poate trezi suspiciunile partenerului agresiv, ceea ce ar putea duce la o intensificare a abuzului și presiunilor asupra victimei pentru împărtășirea noilor parole, precum și a motivului pentru care le-a schimbat.

Să reținem că a păstra confidențialitatea asupra parolelor nu înseamnă că există ceva de ascuns, ci e despre a avea posibilitatea de a alege ce informații oferi altora despre tine, autonomie, putere și control asupra mediului online.

Managerul de parole / password manager

Când utilizăm conturi multiple de e-mail sau aplicații, poate fi dificil să reținem fiecare parolă, cu atât mai mult cu cât acestea ar trebui să fie unice. Pentru a păstra toate parolele în siguranță sau pentru a genera unele foarte sigure, poate fi utilizat un manager de parole. Este similar unui seif în care sunt stocate parolele, pentru accesarea căruia e necesar un cifru, reprezentat de parola unică (master password).

Managerul de parole poate fi browser-based (o aplicație care rulează direct în browserul de internet, fără să fie nevoie de descărcare pe dispozitiv, ci doar de acces la internet) sau software-based (necesită descărcare și instalare pe dispozitiv): LastPass <https://www.lastpass.com/> - browser-based sau Dashlane <https://www.dashlane.com/> - software-based. Pot fi gratuite sau cu plată.

De reținut despre managerul de parole:

- Stocază parolele într-o formă criptată, neinteligibilă
- Poate genera parole complexe, sigure

- Vă reamintește când trebuie schimbate parolele
- Vă avertizează dacă refoșiți o parolă mai veche sau utilizată deja la un alt cont
- O singură parolă unică - master password - trebuie reținută, cea care permite accesul la managerul de parole și permite completarea automată a datelor de logare la conturi și aplicații

Autentificarea cu doi factori / în doi pași

Autentificarea cu doi factori/în doi pași (two-factor authentication - 2FA) reprezintă o măsură suplimentară de siguranță, care dublează securizarea cu parolă și minimizează riscul ca datele sau conturile să fie compromise, chiar dacă cineva cunoaște parola acestora.

Există trei modalități pentru autentificare: ceva ce știi (parola), ceva ce ai (telefon sau token bancar) și ceva ce ești (amprentă, voce, față). Autentificarea cu doi factori folosește o combinație a două dintre aceste modalități. Poate fi utilizată atât pentru e-mail, cât și pentru aplicații, de exemplu Facebook, Twitter, Instagram, WhatsApp, Telegram etc.

De reținut despre autentificarea cu doi factori:

- Autentificarea cu doi factori poate fi realizată fie prin trimiterea un cod unic prin sms, e-mail sau se dă un cod de recuperare, în funcție de opțiunea setată
- Avantajul acestei metode este că avertizează în momentul în care s-a încercat o conectare la cont de pe alt dispozitiv sau dintr-un alt browser, solicitând un cod și/sau parola de conectare pentru a confirma că utilizatorul este cel care accesează contul
- Poate oferi informații de pe ce tip de dispozitiv și din ce locație s-a încercat accesarea
- Activarea opțiunii poate fi utilă persoanelor care au părăsit partenerul agresiv pentru a se asigura că acesta nu îi accesează conturile în mod abuziv

Geolocalizarea

Geolocalizarea este una dintre modalitățile frecvente prin care o persoană oferă informații despre locul în care se află la un moment dat, fără intenție. Și asta se întâmplă pentru că atât aplicațiile, cât și browserele au acces la locație, precum și sistemele sau aplicațiile de urmărire.

De reținut despre geolocalizare:

- Poate oferi informații agresorului despre locația în care se află victima sau
 - o Din fotografiile publicate în social media care au activată localizarea, prin identificarea longitudinii și latitudinii sau căutând imagini similare pe Google

- o Din eticheta aplicată locației atunci când fotografia este publicată în social media de către victimă sau prietenii acesteia
- o Din accesarea istoricului locațiilor în Google, în cazul în care conturile de pe telefonul mobil al victimei și cel de pe computerul de familie sunt sincronizate
- o Prin instalarea unei aplicații - fie prin acces direct la telefon, fie instalarea de la distanță (remote) prin accesarea unui link - care pot accesa atât GPS-ul telefonului, cât și listele de apeluri, conversațiile tip text, parolele, conversațiile telefonice (de exemplu Celltrack, Go&Find, flexispy, Auto Forward etc.). Cele mai multe dintre ele sunt contra cost, dar oferă posibilitatea de utilizare gratuită pentru o perioadă de testare
- o Prin instalarea unui dispozitiv de urmărire pe mașină, în poșetă sau haine
- o Google monitorizează și contul, nu doar dispozitivul, așadar informații precum istoricul locațiilor, istoricul căutărilor pot fi accesate de agresor de pe un computer comun

● Google poate identifica poziția

- o În funcție de adresa de IP pe care vă conectați
- o Din activitatea anterioară, în funcție de căutarea pe internet
- o Din locațiile etichetate
- o De pe dispozitiv, dacă aveți activat GPS-ul pentru hVrți
- o Dacă este activat Serviciul de localizare
- o Chiar dacă dezactivați serviciile de localizare, poziția dispozitivului tot va fi afișată, dacă este GPS-ul activat

Recomandări pentru creșterea siguranței supraviețuitoarelor:

- Verificați în setările telefonului ce permisiuni au aplicațiile instalate și dezactivați accesul la ceea ce nu este necesar (de exemplu, dezactivarea accesului camerei foto la locație, dezactivarea accesului Google la fotografii, telefon, locație, microfon etc.), cu mențiunea că anumite setări pot afecta funcționarea aplicațiilor - dezactivarea accesului WhatsApp la microfon afectează apelurile făcute prin intermediul acestei aplicații, dezactivarea accesului WhatsApp la fotografii împiedică transmiterea lor
- Dezactivați locația din setările telefonului. *Atenție! Acest lucru ar putea afecta modul în care funcționează hărțile (Google maps, Waze)*
- Eliminați etichetarea locației la camera foto, întrucât poate conține longitudinea și latitudinea locului în care a fost făcută o fotografie, conducând agresorul la victimă. *Se recomandă atenție sporită la fotografiile pe care o supraviețuitoare le face într-o locuință protejată sau adăpost cu adresă confidențială și pe care le postează ulterior în mediul online, putând face posibilă recunoașterea locației prin căutarea unor imagini similare pe Google sau prin identificarea longitudinii și latitudinii fotografiei (din Properties ale fotografiei sau folosind aplicații speciale)*

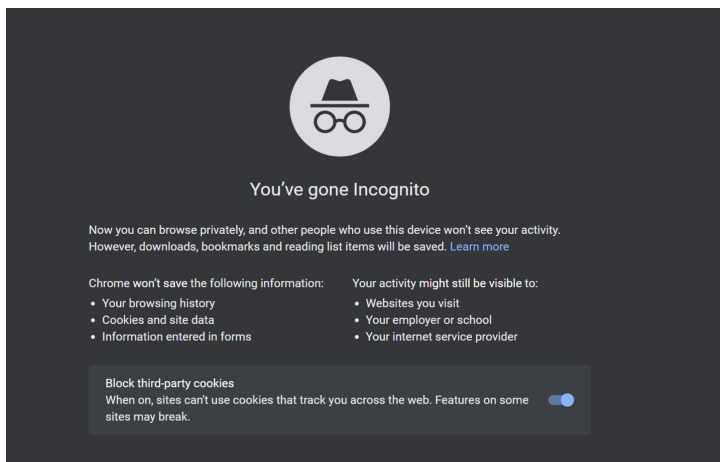
- Nu folosiți geolocalizarea la niciuna dintre aplicații sau site-uri accesate
- Nu folosiți dispozitive la care are acces altcineva, dacă nu vreți să aibă acces la informații despre locurile în care ați fost - va găsi o metodă să le vadă, dacă are un nivel mediu de cunoștințe despre internet
- Setări aplicațiile la cel mai înalt nivel de securitate
- Blocați aplicațiile și site-urile când solicitați accesarea locației
- Nu sincronizați conturile de pe dispozitive
- Ștergeți istoricul din browser, inclusiv de la Google maps. *Atenție! Se poate opta pentru ștergerea istoricului pe anumite perioade de timp (3 luni, 18 luni, 36 luni), dar dacă agresorul obișnuiește să verifice locațiile anterioare, îi poate trezi suspiciuni ștergerea totală a istoricului.*
- Pentru mai multă siguranță, în cazul în care setările par dificil de făcut, alte două opțiuni sunt închiderea telefonului sau scoaterea bateriei de la telefon pentru a evita înregistrarea locației
- Atenție la sms-urile care par venite din partea unui cunoscut/partener, care conțin link-uri care ar trebui accesate. Se poate instala astfel o aplicație de supraveghere la distanță
- Verificați lista de aplicații instalate și dacă nu sunt cunoscute posesorului telefonului, dezinstalați-le

Navigarea pe internet în siguranță

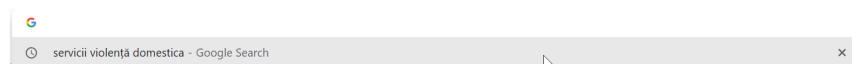
Utilizarea internetului și comportamentul în mediul online sunt două elemente care vulnerabilizează în fața agresorilor, de aceea este important ca profesioniștii să ofere informații beneficiarilor cu care lucrează despre măsurile pe care le pot adopta pentru a-și păstra confidențialitatea și siguranța, mai ales dacă suspectează că cineva le urmărește activitatea în mediul online.

Recomandări pentru creșterea siguranței supraviețuitoarelor:

- Actualizați (update) browserele
- Accesați pagini HTTPS (Hypertext Transfer Protocol Secure), care au un lacăt în fața numelui site-ului, și care asigură utilizatorul că datele sale sunt în siguranță, cum ar fi informațiile despre cardurile bancare (*Atenție! În ultima perioadă, atacatorii creează pagini HTTPS pentru a păcăli utilizatorul că sunt site-uri sigure, în special cele cu vânzare de produse. O măsură de siguranță suplimentară ar fi introducerea manuală a website-ului în loc de accesarea link-ului trimis*)
- Activați opțiunea "Do not track" când accesați anumite pagini (unele dintre ele întreabă)
- Folosiți Incognito mode/Navigare privată când accesați pagini Google/Safari/Internet Explorer/Mozilla pentru ca activitatea în mediul online să nu poată fi detectată pe dispozitiv în istoricul de navigare. Cu toate acestea, dacă sunt descărcate sau marcate anumite pagini, acestea vor fi vizibile. Activarea opțiunii este diferită în funcție de sistemul de operare folosit - iOS, Android, Windows sau macOS.



- Ștergeți istoricul de navigare/history. Atenție la cazurile în care agresorul obișnuiește să verifice activitatea din mediul online, situație în care se recomandă ștergerea fiecărei căutări individual, prin apăsarea literei X care apare în dreapta site-ului căutat



- Folosiți antivirus și firewall - protejează de malware (virusi, trojani, spyware)
- Ștergeți cookie-urile

Cookie-urile sunt fișiere create de site-urile pe care le vizitați. Acestea vă ușurează experiența online salvând informații de navigare. Cu ajutorul cookie-urilor, site-urile pot:

- să vă mențină conectat(ă);
- să memoreze preferințele voastre pentru site-uri;
- să vă ofere conținut relevant la nivel local.

Cookie-urile sunt folosite pentru a îmbunătăți serviciile. Dezactivarea lor depinde de sistemul de operare și browserul folosit.

- Nu salvați parolele în browser - vezi capitolul referitor la **parole**
- Nu apăsați pe link-uri suspecte, bannere, pop-ups care apar la navigarea pe o pagină de internet
- Nu sincronizați conturile între dispozitive, pentru că atunci agresorul poate accesa activitatea din mediul online de pe dispozitivul sincronizat cu cel al supraviețuitoareii

Siguranța în social media

În această eră digitală, este de așteptat ca rețelele sociale să fie folosite de agresori pentru a amenința și hărțui. Abuzatorii își pot crea conturi false sau adrese de e-mail în acest scop, bazându-se pe faptul că nu vor fi prinși, chiar dacă există un ordin de protecție care le interzice să-și contacteze victima.

Utilizarea diferitelor platforme variază în funcție de vârstă: WhatsApp este una dintre cele mai utilizate platforme de mesagerie de persoane de toate vârstele; femeile tinere folosesc Facebook mai des decât adolescențele, care preferă Instagram. Adolescențele folosesc mult mai mult decât alte categorii de vârstă Snapchat și tot mai popularul TikTok. Nu toate aceste platforme sunt spații publice de chat deschise: WhatsApp, de exemplu, este un serviciu de mesagerie închis, în timp ce Facebook, TikTok și Instagram permit interacțiuni deschise și prezintă un risc mai mare de hărțuire din partea unor necunoscuți.

Raportul "Free to be online? - State of the World's Girls", realizat în 2020 de Plan International USA pe 14.000 de persoane tinere a arătat că 23% dintre fete și tinere au raportat că hărțuirea a avut loc pe Instagram și 14% pe WhatsApp, dar pe Facebook se simt deosebit de nesigure: 39% dintre fete au raportat că se confruntă cu hărțuirea.

Rețelele sociale încurajează utilizarea de noi funcții și aplicații, expunând utilizatorii la și mai multe scurgeri de date. Facebook este rețeaua socială dominantă, cu 2.9 miliarde de utilizatori în 2021.

Profesioniștii care lucrează cu supraviețuitoare ale violenței nu pot face din social media un spațiu sigur pentru utilizatori, dar pot să îi îndrume cum să o folosească în siguranță.

Recomandări pentru creșterea siguranței supraviețuitoarelor:

Setări de securitate

- Faceți setările de securitate ale contului la cel mai înalt nivel
- Întrebați-vă cine mai are acces la contul meu? Este un cont împărțit? Cine e administrator? Cine mai poate posta pe el?
- Nu vă folosiți numele real
- Creați o adresă de e-mail separată specială pentru social media/pentru fiecare cont online
- Folosiți o parolă puternică
- Setări autentificare cu 2 factori
- Setări alerte despre conectări neautorizate
- Setări profilul pe "privat"
- Dezactivați locația
- Dezactivați "Vizibilitatea prezenței" la messenger pentru ca un agresor

să nu știe când sunteți online. Și WhatsApp are această opțiune (Setări - Cont - Confidențialitate - Confirmări de citire) care, odată activată, nu mai permite expeditorului să vadă dacă mesajul a fost citit. *Regula nu se aplică și conversațiilor din grupuri sau mesajelor vocale, care, chiar dacă opțiunea "Confirmare de citire" este dezactivată, vor fi bifate ca citite când destinatarul va asculta mesajul*

- Limitați accesul celorlalți la datele voastre personale prin selectarea informațiilor de profil care să fie cunoscute celorlalți
- Setați profilul și etichetarea la nivel maxim de siguranță
- Activați notificarea pentru etichetare și revizuirea etichetării
- Setați postările implicit pentru "prieteni"
- Nu folosiți Facebook pentru conectarea la alte aplicații și site-uri

NB! În noiembrie 2021, Facebook a dezactivat recunoașterea facială în fotografii și videoclipuri

Comportamentul în social media

- Conținutul este în acord cu politicile platformei
- Faceți fotografii și postări doar cu acordul celorlalți care vor fi incluși
- Etichetați cu precauție persoanele, după ce le-ați obținut acordul
- Nu etichetați locația în care vă aflați
- Asigurați-vă că nu e activată locația la camera foto
- Nu dați check-in
- Nu postați fotografii care pot duce la identificarea locației și persoanelor
- Nu postați și nu trimiteți pe messenger/chat fotografii intime

Construirea comunității de prieteni din online

- Împrieteniți-vă doar cu oameni pe care îi cunoașteți în viața reală
- Verificați ce prieteni aveți în comun, verificați-le profilul și postările anterioare (dacă au cont public)
- Dacă nu sunteți sigură că profilul aparține persoanei pe care o cunoașteți în viața reală, sunați-o, verificați informația direct
- Blocați și raportați agresorii și conturile false
- Avertizați familia, prietenii despre agresori care folosesc un anumit cont pentru a se împrieteni cu ei și astfel pentru a avea acces la persoana în cauză

Specialiștii Direcției de Asistență Socială Bistrița și ai locuinței protejate Venus Pitești discută cu fiecare dintre beneficiarele din asistență despre parolarea telefoanelor mobile, titularul abonamentelor mobile, setările de siguranță ale conturilor de social media, postările în social media, permisiunile acordate aplicațiilor și aplicațiile instalate pe telefonul mobil, mesajele cu link-uri suspecte.

Sexting, Tinder și viața reală

Sexting în siguranță

Sextingul este din ce în ce mai popular, inclusiv în rândul adolescenților. Dacă tot mai multă lume îl practică, nu înseamnă că este lipsit de riscuri, cum ar fi expunerea în spațiul public a imaginilor intime fără consimțământ, cu un efect devastator asupra vieții personale și profesionale a victimei. O distincție trebuie făcută între consimțământul de a trimite imaginile cu conținut intim și consimțământul de a le face publice. Sunt două lucruri total diferite, iar neînțelegerea acestei diferențe duce, de cele mai multe ori, la blamarea victimei pentru trimiterea fotografiilor și nicidecum a agresorului pentru expunerea lor.

Recomandări pentru creșterea siguranței supraviețuitoarelor:

- Nu trimiteți fotografii din care puteți fi recunoscut/ă
- Nu faceți sexting în stare de ebrietate
- Distrageți fotografiile
- Protejați fotografiile și telefonul cu parolă
- Salvați fotografiile într-un folder criptat, securizat, la care nu poate avea acces altcineva care utilizează telefonul/computerul
- Ștergeți fotografiile definitiv cu Eraser sau Permanent Eraser, inclusiv din recycle bin/coșul de gunoi
- Nu trimiteți fotografii persoanelor în care nu aveți încredere

Tinder și aplicațiile de online dating

Aplicațiile pentru întâlniri online vulnerabilizează cel mai mult în fața hărțuirii cibernetice. Spre deosebire de majoritatea rețelelor sociale, site-urile de întâlniri sunt folosite cu scopul expres de a întâlni și, potențial, de a deveni intim cu persoane necunoscute. În timp ce pe alte site-uri setările stricte de confidențialitate ar putea servi drept protecție, pe site-urile de întâlniri acele tactici de a rămâne în siguranță ar avea ca rezultat lipsa de interacțiune. Deși aplicațiile de întâlniri ar trebui să fie distractive, există riscul ca aceste întâlniri să devină neplăcute și chiar să se transforme în agresiuni.

Recomandări pentru creșterea siguranței supraviețuitoarelor:

- Verificați profilul celor cu care comunicați. *Catfishing* este una dintre strategiile folosite de agresorii din online prin asumarea unor identități și fotografii de profil false
- Folosiți aplicația pentru a vă cunoaște mai bine, înainte de a muta conversația pe o altă platformă - WhatsApp, Telegram, Signal, messenger, Instagram, care presupun accesul la mult mai multe informații despre

sine, cum ar fi numărul de telefon, lista de prieteni, evenimente din viață

- Setează profilul și fotografiile la ”privat”
- Nu trimiteți fotografii intime din care ați putea fi recunoscute
- Întâlniți-vă în spații publice, cu martori

Din online în viața reală

- Întâlnirile să aibă loc în spații publice, cu martori
- Informați un/o prieten/ă unde mergeți, cu cine, cât estimați că veți sta acolo, inclusiv despre schimbările de planuri/a locației. Dați un share location, dacă mergeți cu persoana respectivă în locuința acesteia sau la un hotel
- Nu lăsați telefonul sau calculatorul nesupravegheate, neparolate

În cazul folosirii aplicațiilor de taxi, în special noaptea

- Asigurați-vă că vă urcați în mașina anunțată
- Nu spuneți șoferului ce reprezintă destinația voastră
- Verificați review-urile șoferului
- Urmăriți ruta
- Dacă simțiți că este ceva în neregulă, coborâți la un semafor
- Distribuți către 1-2 prieteni ruta, ca să urmărească în timp real

Informațiile prezentate mai sus sunt utile profesioniștilor în realizarea planului de siguranță cu supraviețuitoarele violenței, pentru reducerea vulnerabilităților acestora în mediul online și offline și educarea lor pentru folosirea sigură a tehnologiei și internetului.

DOCUMENTAREA ABUZULUI ÎN MEDIUL ONLINE



8

O persoană care se confruntă cu violența cibernetică este preocupată pentru propria siguranță și pentru expunere. Orice sesizare a instituțiilor abilitate, care pot investiga situația respectivă și sancționa agresorul, trebuie susținută de dovezi ale agresiunii, care pot fi obținute astfel:

- Țineți un jurnal cu data, ora, locația, martori, tehnologia/dispozitivul implicat, o scurtă descriere a ceea ce a făcut sau spus agresorul
- Rețineți că informațiile pe care le furnizați și dispozitivele vor fi verificate de polițiști, poate chiar să fie puse sub ascultare, pentru înregistrarea convorbirilor
- Un e-mail de hărțuire sau amenințare include, de asemenea, o adresă IP, care ar putea dezvălui adresa IP de origine și ar putea identifica expeditorul după latitudine și longitudine. Redirecționarea e-mailului către altcineva duce la pierderea acestor informații. Conținutul e-mailului se salvează imprimând sau realizând capturi de ecran cu antetul e-mailului (adesea ascuns, acesta poate fi găsit în setări) unde sunt stocate informațiile IP. (la Yahoo - View raw message X-Originating-Ip, la Outlook - properties, Gmail - afișează originalul)
- Faceți screenshots ale mesajelor text primite, inclusiv cu informațiile de contact (poate fi depusă și o cerere la furnizor pentru obținerea lor, dacă utilizatorul telefonului este și titularul abonamentului)
- Înregistrați audio sau video conversația, folosind aplicații gratuite, cu plată sau opțiuni implicite ale telefoanelor (ASUS, Xiaomi)
- Solicitați sms-urile primite furnizorului de telefonie mobilă, în cazul în care au fost șterse
- Transmiteți solicitare către compania de social media pentru ștergerea postărilor, blocarea conturilor agresorilor
- Faceți screenshots ale postărilor din social media
- Activați verificarea în 2 pași pentru a identifica încercările de conectare de pe alt dispozitiv
- Descărcați informațiile de pe Facebook “Download Your Information”, care permite accesarea tuturor conversațiilor și postărilor făcute vreodată. Conversațiile șterse sunt păstrate de Facebook pentru 90 de zile.
- Raportați către dezvoltatorii platformelor încălcarea termenilor și condițiilor
- Dacă suspectați instalarea unui dispozitiv de urmărire pe mașină, puteți apela la servicii specializate pentru descoperirea lor. În cazul descoperirii unui GPS tracker în mașină sau poșetă sau camere de supraveghere de care nu știți - anunțați poliția, pentru că astfel de dispozitive sunt ilegale
- Cereți sprijinul autorităților

Rețineți că blocarea agresorului poate limita accesul la informațiile pe care acesta continuă să le posteze în online și implicit la dovezi.

**PROCEDURI
ORGANIZAȚIONALE PENTRU
CREȘTEREA SIGURANȚEI**



Abordarea centrată pe supraviețuitor ne pune în centrul intervenției principiul siguranței. Prin urmare, toate serviciile specializate și procedurile de lucru trebuie construite în jurul acestui principiu, pentru a crește încrederea beneficiarului în servicii, a se simți protejat, ascultat, înțeles și crezut.

Persoanelor aflate într-o relație violentă li se spune frecvent că ”nimeni nu te poate ajuta”, ”nimeni nu o să te creadă”, ”nu o să mi se întâmple nimic”, ceea ce le subminează încrederea în autorități, în serviciile și profesioniștii cu care interacționează. Totodată, îl percepe pe agresor ca omnipotent, capabil să influențeze și să manipuleze prietenii, poliția, magistrații, astfel încât să nu fie crezută. Victima se simte fără scăpare, captivă, fără ajutor și are o mare neîncredere în capacitatea celorlalți de a o ajuta și proteja, uneori chiar suspectându-i de alianță cu agresorul.

Pentru creșterea încrederii și asigurarea beneficiarei că informațiile pe care le oferă în cadrul sesiunilor de consiliere sunt confidențiale, că agresorul nu are acces la dosar, iar detaliile nu sunt cunoscute decât de echipa care lucrează în serviciul respectiv și pot fi dezvăluite terților doar cu acordul beneficiarei sau în limitele confidențialității (vezi principiile abordării centrate pe supraviețuitor), recomandarea este ca profesionistul din serviciile specializate să împărtășească beneficiarei politicile și procedurile interne referitoare la securitate și confidențialitate.

La nivelul serviciilor care lucrează cu supraviețuitoarele violenței pot fi implementate politici și proceduri care să reflecte principiul siguranței și protecției și care vizează următoarele aspecte:

- Securitatea spațiului în care se oferă servicii (de consiliere sau în sistem rezidențial)
 - Securitatea echipamentelor, a dispozitivelor pe care le folosim
 - Securitatea dosarelor beneficiarelor, a bazelor de date și a documentelor electronice privitoare la cazuri
 - Securitatea comunicării (telefon, e-mail, WhatsApp, Telegram, messenger etc.)
 - Securitatea și starea de bine a angajaților care lucrează cu beneficiarele, protecția lor împotriva agresiunilor din partea beneficiarelor sau agresorilor
- În funcționarea unui serviciu, existența și respectarea politicilor și procedurilor interne este foarte importantă, întrucât oferă repere echipei și setează un cadru sigur pentru oferirea serviciilor, atât pentru beneficiare, cât și pentru profesioniști.

Securitatea spațiului în care se desfășoară activitatea de consiliere/găzduirea

- Clădire sigură, fără risc seismic, geamuri securizate, cu gratii, fără trepte periculoase pentru copii, accesibilă persoanelor cu dizabilități fizice
- Păstrarea confidențialității adresei, în funcție de specificul activității
 - o Bună practică pentru centrele de consiliere: promovarea doar a

numărului de telefon, adresa este dată doar persoanei programate la consiliere

- De preferat să fie 2 intrări, astfel încât beneficiara să poată evita o întâlnire cu agresorul, dacă a identificat că se află în acea locație
- Existența unui serviciu de pază sau a unui buton de panică, care să fie acționat în cazul unei vizite inoportune a agresorului
- Lucru pe bază de programare pentru a evita întâlnirile între beneficiare în același spațiu și încălcarea confidențialității
- Dotarea spațiului cu extintoare
- Securizarea prizelor, întrerupătoarelor pentru a limita accesul copiilor, în special în spațiile rezidențiale
- Schimbați broasca și cheile la anumite intervale de timp, mai ales dacă este un spațiu rezidențial confidențial

Securizarea echipamentelor

Computere

- Parolarea computerelor cu parole sigure, confidențiale
- Folosirea și actualizarea antivirusului și firewall
- Actualizarea constantă a sistemului de operare și a software-ului
- Folosirea criptării pentru a împiedica sustragerea informațiilor electronice despre cazuri sau în cazul furtului/pierderii echipamentului. Poate fi folosit full disk encryption, care face o criptare integrală a hard-disk-ului (transformă informația într-un cod care nu poate fi citit de altcineva decât cu o cheie de criptare)
- Faceți backup periodic pe server sau harduri externe
- Protejați informațiile confidențiale cu parole. Pot fi parolate fișiere sau foldere
- Nu deschideți documente atașate suspecte, care ar putea conține viruși, spyware, ransomware etc.
- Folosiți o conexiune VPN (Virtual Private Network), care protejează accesul la internet și confidențialitatea în mediul online, inclusiv față de furnizorul de internet, oferă protecție împotriva atacurilor cibernetice, împiedică hackerii să sustragă parolele sau alte informații (mai ales în cazul conectării la rețele publice), maschează adresa de IP reală de unde vă conectați la internet.

Router și rețea wifi

- Folosiți o parolă puternică
- Dați un nume rețelei care să nu poată fi asociat cu utilizatorul/spațiul respectiv. De exemplu, dacă rețeaua respectivă este într-o locuință protejată sau adăpost cu adresă confidențială, nu denumiți rețeaua "Locuința protejată 1" sau "Adăpost", întrucât locația poate fi identificată de un agresor prin scanarea rețelelor wi-fi din zona respectivă

- Creați o rețea Guest pentru vizitatori, la care să le permiteți conectarea și căreia să îi schimbați parola la un anumit interval de timp. O astfel de precauție este foarte importantă în cazul centrelor rezidențiale cu adresă confidențială, întrucât la părăsirea adăpostului beneficiarei pleacă cu datele de conectare la rețeaua wi-fi
- Nu afișați datele de conectare la rețeaua wi-fi principală într-un loc vizibil, doar pe cele de la rețeaua Guest

Dosarele și datele beneficiarelor

- Dosarele și datele se păstrează cu maximă confidențialitate, în dulapuri încuiate, în spații la care au acces doar angajații
- Se poate adopta o politică de anonimizare a datelor sau pseudo-anonimizare prin acordarea unui cod fiecărui nume și folosirea lui în toate actele/documentele referitoare la beneficiară. Într-un document/dosar separat, se înregistrează asocierea codului cu numele beneficiarei
- Se recomandă stocarea informațiilor electronice pe un computer neconectat la internet, parolat, criptat, pentru a preveni accesarea datelor confidențiale de către persoane neautorizate
- Salvați informațiile pe un hard extern, parolat și criptat
- Stabiliți o politică de accesare a dosarelor și datelor beneficiarelor
- Stabiliți o politică de distrugere a documentelor vechi

În urma procesului de coaching în care a fost implicată, Direcția de Asistență Socială Bistrița a implementat măsuri interne menite să crească siguranța persoanelor asistate și a datelor acestora. Astfel, s-a securizat accesul la internet prin instalarea unei conexiuni VPN pe toate computerele instituției, au schimbat parolele tuturor echipamentelor și au parolat telefoanele personale, instruind și beneficiarele aflate în asistență cum să facă acest lucru. Au introdus politică de criptare a documentelor stocate pe computere. Având o imprimantă comună la nivel de instituție, pentru a evita accesul altora la documentele personale ale beneficiarelor și neexistând posibilitatea tipăririi securizate (opțiunea Secure print, care presupune introducerea unui cod pe imprimantă, în momentul tipăririi), s-a optat pentru salvarea lor pe un stick, care ulterior este introdus în copiator pentru printare.

Toate serviciile implicate în programul de coaching păstrează dosarele beneficiarilor în format fizic, în fișete încuiate, la care au acces doar membrii echipei care lucrează cu cazurile. Dosarele vechi sunt arhivate conform unei politici specifice fiecărui serviciu.

Comunicarea în siguranță cu beneficiarele

Interacțiunea cu beneficiarele de servicii sociale nu presupune doar contact direct, ci și prin intermediul dispozitivelor electronice și internetului. Profesioniștii care lucrează cu supraviețuitoarele violenței trebuie să stabilească politici și proceduri interne care reduc riscul de intensificare a abuzului.

Comunicarea la telefon

- Primul contact:
 - o Vă asigurați că poate folosi telefonul în siguranță, că nu ascultă nimeni convorbirea, că nu suspectează că ar putea avea ceva instalat pe telefon
 - o Cereți-i să ștergă numărul de telefon din lista de apeluri sau să nu salveze numărul în agendă cu un nume care poate fi ușor identificat de agresor, de exemplu "centrul de consiliere", "psiholog" etc.
- În monitorizare
 - o Stabiliți împreună cu beneficiara care este modul în care se va păstra legătura, dacă își dorește acest lucru
 - o Explorați dacă pot fi transmise mesaje sms, WhatsApp în siguranță
 - o Stabiliți intervalul orar în care poate fi contactată în siguranță
 - o Stabiliți dacă e sigur să fie sunată sau preferă să fie cea care inițiază contactul
 - o Dacă nu e sigur să folosească telefonul propriu, explorați alternative
- Folosiți telefoane cu numere de serviciu pentru angajați/telefon organizațional, pentru a nu se expune personal
- Conversațiile telefonice nu se înregistrează fără informarea prealabilă

Echipa DGASPC Sector 2 care lucrează în serviciul violență domestică nu comunică beneficiarilor numerele de telefon personale, folosesc doar telefonul de serviciu.

Comunicarea prin mesaje

- Se stabilește împreună cu beneficiara dacă e o metodă sigură de contact
- Se stabilește aplicația preferată sau sigură -sms, WhatsApp, Signal, Telegram
- Se stabilesc ce tipuri de informații pot fi transmise, de care ar putea avea nevoie ulterior, precum numere de telefon, adresă, ora și ziua programării, anularea programării etc.
- Se poate stabili un cod de siguranță/o parolă, un anumit răspuns la o întrebare specifică, pentru a evita ca agresorul să comunice pretinzând că este beneficiara
- Recomandați ștergerea mesajelor, dacă altcineva are acces la dispozitiv
- Verificați din când în când dacă a rămas o metodă sigură
- Dacă în echipă lucrează mai multe persoane cu același caz - asistent social, psiholog, avocat etc. - se comunică direct cu specialiștii pentru chestiuni specifice
- Dacă persoana are o dizabilitate auditivă, poate fi o metodă de comunicare pentru furnizarea serviciilor

Comunicarea prin e-mail

- Se stabilește împreună cu beneficiara dacă e o metodă sigură de contact
- Folosiți adrese de e-mail de serviciu
- Asigurați persoana că informațiile oferite sunt confidențiale, precizați-i

cine are acces la adresa de e-mail pe care transmite informațiile (de exemplu, poate fi o adresă de office sau de registratură la care au acces mai multe persoane, ceea ce poate duce la încălcarea confidențialității și crearea unui sentiment de nesiguranță pentru beneficiară)

- Se poate stabili un cod de siguranță/o parolă, un anumit răspuns la o întrebare specifică, pentru a evita ca agresorul să comunice pretinzând că este beneficiara
- Nu păstrați în mesaje tot istoricul anterior, nu dați reply la reply
- Recomandați ștergerea e-mailurilor
- Nu dați mesajele mai departe unor terți externi organizației, fără acordul persoanei, conform politicii de confidențialitate
- Verificați din când în când dacă este în continuare o metodă sigură
- Dacă în echipă lucrează mai multe persoane cu același caz - asistent social, psiholog, avocat etc. - se comunică direct cu specialiștii pentru chestiuni specifice
- Dacă persoana are o dizabilitate auditivă, poate fi o metodă de comunicare pentru furnizarea serviciilor

DAS Bistrița a creat adrese de e-mail pentru fiecare angajat, utilizate pentru comunicarea cu beneficiarii și cu partenerii externi.

Comunicarea în social media

- Nu postați în social media informații care ar putea duce la identificarea unei persoane asistate - fotografii, nume, indicii personale
- Nu etichetați o beneficiară într-o postare în social media, chiar dacă nu mai e în asistența serviciului de mult timp
- Etichetarea angajaților din serviciul respectiv se face doar cu acordul lor, pentru a reduce expunerea și targetarea de către agresori. Recomandabil ar fi să nu fie făcută!
- Nu vă împrieteniți pe conturi de socializare cu persoanele asistate
- Dacă e absolut necesară comunicarea prin messenger sau Instagram, folosiți contul de organizație, nu pe cel personal
- Se poate stabili un cod de siguranță/o parolă, un anumit răspuns la o întrebare specifică, pentru a evita ca agresorul să comunice pretinzând că este beneficiara
- Recomandați ștergerea conversațiilor private avute cu profesioniștii
- Recomandați ferm să nu posteze în social media numele serviciului sau profesioniștilor care îi oferă servicii
- Interziceți postarea fotografiilor din adăposturi sau cu celelalte beneficiare

Comunicarea video

- Stabiliți dacă este o metodă sigură de comunicare și ce tip de dispozitiv va fi folosit
- Asigurați-vă că e o conexiune la internet stabilă și că persoana are resursele necesare pentru a-și permite acest tip de comunicare: dispozitiv, suficient trafic de internet

- Beneficiara să se afle într-un loc sigur, iar specialistul într-un cadru în care să nu existe întreruperi sau distrageri
- Oferiți asistență pentru a se familiariza cu platforma și pentru a se simți confortabil
- Stabiliți ce faceți în cazul în care se pierde conexiunea
- Folosiți o platformă ușor de utilizat, care să nu necesite conectare cu cont (Zoom, Webex), pentru a nu fi descoperite de agresor
- Folosiți conturi de organizație
- Nu înregistrați conversația
- Recomandați ștergerea istoricului din browser, mai ales dacă este un dispozitiv folosit în comun cu alți membri ai familiei

Grupurile online

- Asigurați-vă că este o metodă sigură pentru beneficiare
- Asigurați-vă că este o modalitate de contact pe care și-o pot permite
- Folosiți o platformă care nu necesită cont și poate fi accesată ca Guest (Zoom, Webex)
- Stabiliți cum transmiteți datele de logare
- Puteți agreea modul în care se afișează fiecare - cu numele real sau nu. Atât Zoom, cât și Webex permit alegerea unui nume dacă participarea nu se face prin logarea cu cont, ci doar ca Guest.
- Stabiliți o regulă referitoare la folosirea camerei
- Stabiliți ca regulă a grupului interdicția de a face print screen/screenshot în timpul grupului
- Agreeați formatul grupului - grup închis sau deschis, în care mai puteți include ulterior alte persoane. E important să le cereți acordul înainte.
- Nu formați un grup online cu persoane pe care nu le-ați evaluat niciodată și cu care nu ați interacționat în consiliere
- Folosiți cont de organizație (de preferat conturi plătite pentru a nu avea o limită de timp. De exemplu, în cazul grupurilor mai mari de 2 persoane, Zoom în varianta gratuită se întrerupe la fiecare 40 minute)
- Nu înregistrați convorbirea și stabiliți ca regulă a grupului
- Nu transmiteți live discuția pe Facebook sau Youtube
- Recomandați să șteargă istoricul din browser
- Stabiliți o durată pentru grup

**SECURITATEA
ȘI STAREA DE BINE
A PROFESIONIȘTILOR
CARE LUCREAZĂ
CU CAZURI DE VIOLENȚĂ**



Un aspect care necesită atenție din partea organizațiilor și instituțiilor care oferă servicii specializate supraviețuitoarelor violenței sexuale și de gen, este cel al securității profesioniștilor care lucrează direct cu beneficiarele, atât din perspectiva siguranței fizice, cât și a stării de bine emoționale.

Nu de puține ori, profesioniștii din domeniul social sunt expuși intimidării, amenințărilor sau abuzurilor din partea unui agresor, fiind considerați responsabili pentru demersurile pe care o supraviețuitoare le-a făcut pentru a ieși din relația violentă, pentru serviciile oferite sau pentru modul în care s-au soluționat anumite cazuri.

Siguranța fizică a angajaților poate fi asigurată prin implementarea unor măsuri specifice, după cum este precizat în capitolul Politici și proceduri organizaționale - securitatea spațiului, securizarea echipamentelor, dar și prin introducerea unor prevederi referitoare la modul în care se intervine în momentul în care un agresor sau un beneficiar are un comportament amenințător sau când o persoană neautorizată pătrunde în spațiul rezidențial. Existența, cunoașterea și respectarea procedurilor interne pentru aceste situații ajută profesioniștii în gestionarea riscului și în propria protecție.

Profesioniștii din domeniul social au un rol cheie în a ajuta supraviețuitoarele violenței sexuale și de gen să se recupereze din traumă, fiind expuși, în același timp, riscului de a suferi traume indirecte. Trauma indirectă este definită ca o consecință negativă asociată lucrului cu supraviețuitoarii traumei, în care bunăstarea emoțională a profesioniștilor este afectată. Lucrul cu supraviețuitoarii unei traume poate provoca stabilitatea emoțională a celor mai experimentați dintre profesioniști, de aceea este nevoie de supervizare, abilități de adaptare sau strategii de a face față. Expunerea prelungită și lipsa cunoștințelor asupra efectelor traumei indirecte pot duce, de asemenea, la burnout sau la decizia de a părăsi locul de muncă.

În acest context, devine și mai importantă înțelegerea traumei și a reacțiilor emoționale, cognitive și fizice, nu doar pentru a oferi servicii adecvate beneficiarilor, dar și pentru a gestiona riscul de traumă secundară.

Trauma secundară	Burnout
Apare când persoanele care au profesii în care intră frecvent în contact cu diferitele forme ale suferinței umane (medici, polițiști, pompieri, asistenți sociali, psihologi, preoți, jurnaliști) încep să manifeste simptome de traumă la rândul lor. Trauma unei supraviețuitoare devine un eveniment traumatic pentru profesionist.	Sindromul epuizării profesionale reprezintă o stare de epuizare, atât fizică, cât și psihică și mentală, care apare în special la persoanele a căror profesie implică o responsabilitate deosebită și interacțiuni frecvente cu oamenii. Resursele personale sunt epuizate în efortul de a face față unui număr mare de stresori, corelați inclusiv cu locul de muncă, ceea ce îl vulnerabilizează pe profesionist în fața expunerii permanente la trauma supraviețuitoarelor.

Simptome ● Flashback-uri, coșmaruri ● Iritabilitate, răspunsuri comportamentale exagerate ● Dificultăți în a dormi, schimbări în apetit ● Senzație de amorțeală, lipsă de energie ● Depresie, stări de melancolie ● Sentiment de vină, anxietate ● Disociere ● Nevoia de retragere, conflicte interpersonale ● Probleme în stabilirea limitelor personale ● Pierderea plăcerii în activitățile zilnice ● Somatizări	Simptome ● Stres fizic și emoțional ● Oboseală ● Iritabilitate, furie ● Demotivare ● Scăderea performanței la locul de muncă ● Scăderea satisfacției profesionale ● Sentiment de presiune, neputință și copleșire ● Pesimism/cinism ● Depersonalizare ● Concediu medical sau de odihnă frecvent
Trauma este o afecțiune somatică și mentală, care nu se schimbă odată cu schimbarea mediului	Burnout-ul este o stare care se poate schimba odată cu schimbarea locului de muncă sau a practicilor din organizație

Dacă vă confrunțați cu aceste simptome, este important să recunoașteți că nu reprezintă o măsură a abilităților voastre profesionale, ci un răspuns normal la natura provocatoare a acestei munci în domeniul social.

Facilitatori ai burnout-ului la nivel organizațional ● Absența oricărui control asupra propriei munci ● Excluderea de la luarea deciziilor ● Inechități în sarcinile de muncă, salarizare, oportunități de promovare ● Nu există oportunități de feedback ● Mediu profesional negativ/conflicte ● Locul de muncă este foarte diferit de ceea ce personalul a înțeles la angajare	Facilitatori ai burnout-ului la nivel personal ● Perfecționism ● Munca excesivă este considerată o valoare ● Teama de a exprima propriile nevoi, emoții ● Dificultate în stabilirea limitelor de teama consecințelor ● Locul de muncă nu se potrivește cu viziunea ideală cu privire la rolul lor în lume
--	--

Locurile de muncă puternice, sănătoase și reziliente sunt caracterizate de siguranța spațiului și a angajaților și de construirea unor relații de încredere, având un management suportiv, empatic, capabil să înțeleagă situația specifică în care se află fiecare angajat, și colegi care pot oferi suport. În aceste locuri de muncă, supervizarea și interviziunea sunt disponibile angajaților, pentru a-i ajuta să facă față burnout-ului și traumei secundare.

Recomandări pentru gestionarea simptomelor de traumă secundară și burnout

- Starea de bine la locul de muncă începe cu construirea propriei reziliențe, prin echilibrarea vieții profesionale cu cea privată
- Identificați proprii declanșatori de stress (stress triggers)
- Creați un plan de auto-îngrijire - fizică, psihologică, emoțională, spirituală. Îngrijirea de sine e ceva ce trebuie trăit și practicat zilnic, include orice obiceiuri deliberate și consecvente pe care le creați pentru a vă spori starea de bine generală
- Aduceți această stare de bine și la locul de muncă, alegând un mic obicei de îngrijire de sine și încurajați-i și pe ceilalți din organizație să facă același lucru
- Creați un spațiu "sigur" la locul de muncă, în care să puteți lua masa sau lua o pauză, decorați cu plante, flori, lumini plăcute
- Cereți ajutor - managerului, unui coleg, unui terapeut

Membrii echipei se pot ajuta reciproc prin:

- Verificări periodice, întâlniri, intervizări, informări
- Crearea de oportunități pentru pauză
- Recunoașterea semnalelor/simptomelor de burnout
- Susținerea acelei culturi organizaționale care recunoaște că epuizarea și stresul traumatic sunt răspunsuri la stresul cronic
- Recunoașterea traumei secundare ca răspuns normal la situații terifiante
- Susținerea și normalizarea ideii că uneori nu putem să facem tot ceea ce dorim pentru un beneficiar
- Sărbătorirea succesului

Pentru a preveni apariția burnout-ului

- Faceți-vă timp pentru sine și familie/prieteni
- Nu neglijați somnul, alimentația, sportul, pauzele/vacanțele
- Fiți în contact cu propriul corp
- Grounding
- Exerciții de respirație
- Acordați-vă timp liber, faceți plimbări
- Practicați meditația, yoga/stretching, cântat, dansat, pictat, orice vă face plăcere

Ca model de bună practică, DAS Bistrița a creat o cameră de pauză pentru angajați, vinerea este Casual Friday, săptămânal echipa are o ședință de ventilare.

Managerul serviciului de violență domestică al DGASPC Sector 2 ține cont de nivelul de încărcare cu sarcini a fiecărui angajat și distribuie cazurile în mod echitabil, iar echipa locuinței protejate Pitești are ședințe de interviziune în fiecare zi de luni cu colegii din DGASPC.

BIBLIOGRAFIE ȘI RESURSE



1. Patchin, J. W., Hinduja, S. (2006). *Bullies move beyond the schoolyard: A preliminary look at cyberbullying*. *Youth Violence and Juvenile Justice*, 4, 148-169
2. Young, R., Miles, S. & Alhabash, S. (2018). *Attacks by Anons: A Content Analysis of Aggressive Posts, Victim Responses and Bystander Interventions on a Social Media Site*. Sage journals
3. Suzie Dunn (2020), Centre for International Governance Innovation. *Technology-Facilitated Gender-Based Violence: An Overview*
4. Fundația Sensibilu pentru Asociația Serviciul lezuiților pentru Refugiați din România (JRS România) (2020). *Ghid privind violența sexuală și de gen pentru practicieni care lucrează în domeniul azilului*
5. Association for Progressive Communications (APC) (2017). *Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences*
6. The Un Broadband Commission For Digital Development Working Group On Broadband And Gender (2015). *Cyber Violence Against Women And Girls: A World-Wide Wake-Up Call*
7. Council of Europe (2018), *Mapping study on cyberviolence with recommendations adopted by the T-CY*
8. Agenția pentru Drepturi Fundamentale a Uniunii Europene (2014). *Violence against women: an EU-wide survey - Main results (Violența împotriva femeilor: o anchetă la nivelul UE - Principalele rezultate)*. Luxemburg: Oficiul pentru Publicații al Uniunii Europene. Disponibil la adresa: <http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report>
9. World Health Organization, on behalf of the United Nations Inter-Agency Working Group on Violence Against Women Estimation and Data (2021). *Violence against women prevalence estimates, 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* <https://en.unesco.org/sites/default/files/highlightdocumentenglish.pdf>
10. European Women's Lobby (2017). *#HerNetHerRights Resource Pack on ending online violence against women & girls in Europe*. Disponibil la adresa https://www.womenlobby.org/IMG/pdf/hernetherights_report_2017_for_web.pdf
11. UNICEF Regional Office for South Asia (2017). *Gender Equality: Glossary of Terms and Concepts*. Disponibil la adresa <https://www.unicef.org/rosa/reports/gender-equality>
12. Canadian Institutes of Health Research (2020). *What is gender? What is sex?*. Disponibil la adresa <https://cihr-irsc.gc.ca/e/48642.html>
13. Convenția Consiliului Europei privind prevenirea și combaterea violenței împotriva femeilor și a violenței domestice (2011) (Convenția de la Istanbul)
14. Rezoluția Consiliului pentru Drepturile Omului HRC/RES/20/8 pentru promovarea, protecția și exercitarea drepturilor omului pe internet. Disponibil la adresa <https://undocs.org/en/A/HRC/RES/20/8>
15. Rezoluția Consiliului pentru Drepturile Omului A/HRC/RES/29/14 privind accelerarea eforturilor pentru eliminarea tuturor formelor de

violență împotriva femeii: eliminarea violenței domestice. Disponibil la adresa <https://documents-ddsny.un.org/doc/UNDOC/LTD/G15/140/16/PDF/G1514016.pdf?OpenElement>

16. Raportul Înaltului Comisar al Națiunilor Unite pentru Drepturile Omului A/HRC/35/9 privind promovarea, protecția și exercitarea drepturilor omului pe internet: modalități de a reduce decalajul digital de gen din perspectiva drepturilor omului. Disponibil la adresa <https://undocs.org/A/HRC/35/9>
17. Plan International (2020). Free to be online? A report on girls' and young women's experiences of online harassment. Disponibil la adresa <https://plan-international.org/publications/freetobeeonline>
18. World Health Organization (2021). Devastatingly pervasive: 1 in 3 women globally experience violence. Disponibil la adresa <https://www.who.int/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence>
19. CYBERSAFE project - Changing Attitudes among teenagers on Cyber Violence against Women and Girls. Disponibil la adresa <https://www.stoponlineviolence.eu/>
20. eSafety Commissioner. Disponibil la adresa: <https://www.esafety.gov.au/women/connecting-safely>
21. National Network to End Domestic Violence NNEDV. Disponibil la adresa: <https://nnedv.org/>
22. Technology safety. Exploring technology in context of intimate partner violence, sexual assault, and violence against women. Disponibil la adresa: <https://www.techsafety.org/>
23. The Women's Service Network WESNET. Disponibil la adresa: <https://wesnet.org.au/>
24. Vital Voices Global Partnership. Disponibil la adresa: <https://www.vitalvoices.org/>
25. Take back the tech. Take control of technology to end gender-based violence. Disponibil la adresa: <https://www.takebackthetech.net/>
26. Women's Media Center. Disponibil la adresa: <https://www.womensmediacenter.com/>

PLAN DE SIGURANȚĂ - MĂSURI DE CREȘTERE A SECURITĂȚII PERSOANELOR AFECTATE DE VIOLENȚĂ DOMESTICĂ

Plan de siguranță - măsuri de creștere a securității fizice a femeilor și copiilor victime ale violenței domestice

1. *Înainte ori în timpul episodului de violență*
 - Strigă după ajutor.
 - Fii atentă la semnele care pot declanșa un nou episod violent și folosește orice motiv pentru a încerca să scapi, să fugi din casă.
 - Identifică zonele sigure din casă unde te poți refugia. Evită locurile periculoase din casă - spațiile mici, fără ieșire sau camerele cu posibile arme (bucătărie, baie, hol).
 - Păstrează cât mai multe dovezi (fotografii cu răni, camera deranjată, mesaje audio-video).
 - Stabilește un cod (cuvânt, frază, semnal) pentru situațiile grave, astfel încât copiii, vecinii, familia, prietenii să știe că te afli în pericol și să solicite intervenția poliției. *sesizarea poate fi făcută și anonim
 - Stabilește un plan unde să te refugiezi atunci când situația o va impune, chiar dacă acum crezi că nu va fi nevoie niciodată să pleci de acasă.
 - Încearcă să ajungi la cea mai apropiată secție de poliție sau patrulă stradală.
 - Prefă-te că mergi la o farmacie, magazine. Anunță farmacistul, vânzătoarea că ești în pericol și cere-i să sune la 112.
 - În situația în care ai mașină, verifică în permanență dacă este alimentată și parcată într-un loc din care poți ieși cu ușurință.
 - Dacă agresorul nu locuiește cu tine în casă, schimbă încuietorile de la ușă și geamuri. Este indicată montarea unor dispozitive de siguranță (sistem de securitate, detectoare de mișcare, lumini în exteriorul casei, gratii la ferestre sau încuietori suplimentare).
2. *Dacă vrei să pleci de acasă*
 - Dacă în păstrare unei persoane de încredere și disponibilă: o sumă de bani, un set de copii după cheile locuinței și mașinii, copii ale actelor importante - certificate de naștere, certificatul de căsătorie, diplome, buletinul sau cartea de identitate, etc., câteva haine și încălțăminte, jucării ale copiilor, medicamente, rechizite.
 - Dacă pregătești un bagaj cu toate lucrurile menționate mai sus, plasează-l cât mai curând în afara locuinței pentru ca el să nu îți dea seama de intențiile tale de plecare; părăsirea abuzatorului prezintă un risc crescut ca tu să fii în pericol.
 - Asigură-ți din timp o rezervă de bani pentru situații critice.
 - Stabilește din timp la cine vei apela în caz de nevoie pentru găzduire de urgență, împrumut de bani, solicitarea intervenției poliției.

Planul de securitate digitală

- Nu folosi computerul de acasă pentru a căuta informații sau pentru a solicita ajutor online. Utilizează calculatorul de la locul de muncă, calculatorul unui vecin/rudă etc.
- Șterge istoricul căutărilor.
- Nu folosi adresa de e-mail pe care o știe agresorul.
- Creează un nou cont de e-mail, pe care să NU îl accesezi de pe computerul de acasă.
- Încearcă pe cât posibil să folosești pentru apelare o cartelă preplătită de telefon sau telefonul copiilor.
- Verifică-ți mașina pentru dispozitive de urmărire.

3. Dacă deja ai plecat de acasă

- Găsește-ți o locuință în care tu și copiii tăi să fiți în siguranță și pe care el să nu o cunoască.
- Nu divulga nimănui noua adresă unde te-ai mutat. Ca să ajungă la tine, este posibil ca agresorul să-ți urmărească și rudele, prietenii.
- Schimbă rutina zilnică, dacă ai rămas în aceeași zonă cu agresorul. Folosește un alt drum, alte mijloace de transport pentru a putea ajunge la serviciu, fă-ți cumpărăturile la alte magazine/piețe, evită locurile în care mergeați împreună.
- la în considerare posibilitatea de a transfera copiii la o altă școală.
- Schimbă-ți medicul de familie.

Plan de siguranță digitală

- Verifică-ți setările telefonului mobil. Există aplicații pentru telefonie mobilă pe care agresorul le poate utiliza pentru a asculta convorbirile sau pentru a urmări locația în care te afli. Agresorul poate folosi telefonul mobil ca un dispozitiv de urmărire în cazul în care acesta are GPS, este în "modul silențios", sau este setat pe funcția "răspuns automat." Închide telefonul atunci când nu-l folosești.
- la în considerare cumpărarea unui alt telefon mobil.
- Limitează comunicările cu agresorul doar la cele strict legate de copii sau procese, dacă e cazul și nu există un OP.
- Blochează apelurile necunoscute.
- Deoarece există posibilitatea ca agresorul să știe cum să-ți acceseze contul, să-ți cunoască parola de acces în cont, creează-ți conturi de e-mail folosind nume de utilizator și parole noi. Alege parole care nu pot fi ghicite de către agresor (evită orice informație personală - zilele de naștere ale voastre sau ale copiilor, porecle, nume, alte date comune).
- Folosește adrese de e-mail diferite în funcție de persoanele cu care comunic.
- Dacă soliciți ajutor online, folosește laptopul vechi doar după o atentă verificare, instalare de antivirus, firewall.

- Închide vechile conturi de social media, creează unele noi, cu o altă identitate.
- Anulează conturile bancare vechi și cardurile de credit, mai ales dacă acestea au fost comune cu agresorul. Folosește o altă bancă în eventualitatea în care dorești să-ți deschizi un alt cont.
- Schimbă parolele la serviciile bancare online sau la alte conturi de interes pentru tine.
- Strânge dovezi, dacă abuzul continuă - printscreen, înregistrări audio-video etc.
- Verifică jucăriile și telefonul copiilor pentru programe de monitorizare, GPS, camere video, după vizitele la celălalt părinte.
- Instruiește copiii să nu trimită către partener fotografii cu noua locație sau cu alte persoane care sunt cazate împreună cu voi.
- Dă-i/preia copiii într-un loc public (cât mai departe cu putință de noua locuință), cu martori.
- Pentru facturi și corespondență folosește adresa de la serviciu sau mai bine o cutie de oficiu poștal, decât adresa de acasă.
- Asigură-te că ai tot timpul telefonul mobil încărcat pentru situația în care ești nevoită să apelezi 112.
- Avertizează persoanele de încredere despre aceste schimbări.

Aspecte juridice

- Poți suna oricând la 112 pentru a solicita ajutor.

Ordinul de protecție provizoriu

- Poliția intervine la solicitarea ta și poate emite imediat un ordin de protecție provizoriu pe o perioadă de 5 zile.
- Evacuarea temporară a agresorului din locuința comună, indiferent dacă acesta este titularul dreptului de proprietate.
- Reintegrarea victimei și, după caz, a copiilor în locuința comună.
- Obligarea agresorului la păstrarea unei distanțe minime determinate față de victimă, față de membrii familiei acesteia, ori față de reședința, locul de muncă sau unitatea de învățământ a persoanei protejate.
- Obligarea agresorului de a preda poliției armele deținute.
- Ordinul de protecție provizoriu va cuprinde și mențiunea că încălcarea oricăreia dintre măsurile dispuse constituie infracțiune și se pedepsește cu închisoare de la o lună la un an.
- Instanța poate prelungi ordinul provizoriu emis de polițist.

Ordinul de protecție

- Persoana a cărei viață, integritate fizică sau psihică ori libertate este pusă în pericol printr-un act de violență din partea unui membru al familiei poate solicita instanței ca, în scopul înlăturării stării de pericol, să emită un ordin de protecție.
- Ordinul de protecție poate cuprinde evacuarea temporară a agresorului din locuința familiei, indiferent dacă acesta este titularul dreptului de

proprietate, reintegrarea victimei și, după caz, a copiilor, în locuința familiei,

- Ordinul poate stabili limitarea dreptului de folosință al agresorului numai asupra unei părți a locuinței comune atunci când aceasta poate fi astfel partajată încât agresorul să nu vină în contact cu victima.
- Obligarea agresorului la păstrarea unei distanțe minime determinate față de victimă, față de copiii acesteia sau față de alte rude ale acesteia ori față de reședința, locul de muncă sau unitatea de învățământ a persoanei protejate. Întrucât legea nu stabilește o anumită distanță, aceasta urmează să fie indicată expres de către instanță în ordinul de protecție.
- Interdicția pentru agresor de a se deplasa în anumite localități sau zone determinate pe care persoana protejată le frecventează sau le vizitează periodic.
- Interzicerea oricărui contact, inclusiv telefonic, prin corespondență sau în orice alt mod, cu victima.
- Obligarea agresorului de a preda poliției armele deținute.
- Încredințarea copiilor minori sau stabilirea reședinței acestora.
- Durata măsurilor de protecție dispuse de instanța de judecată este determinată în mod explicit de către judecător, dar nu poate fi mai mare de șase luni de la data emiterii ordinului. Chiar dacă decizia nu indică în mod expres durata măsurilor luate, ele vor intra în vigoare pentru o perioadă de șase luni de la data emiterii.
- Competența de emitere a ordinului de protecție aparține judecătorei în a cărei rază teritorială își are domiciliul sau reședința victima.
- Titularul cererii de emitere a unui astfel de ordin este însăși victima. Cererea poate fi introdusă personal sau prin reprezentant legal și este scutită de taxa de timbru judiciar.
- Cererile pentru emiterea ordinului de protecție se judecă de urgență și, în orice situație (inclusiv pe perioada stării de urgență), soluționarea acestora nu poate depăși un termen de 72 de ore de la depunerea cererii. Cererile se judecă în camera de consiliu, participarea procurorului fiind obligatorie.
- Ordinul de protecție este executoriu.
- Încălcarea oricăreia dintre măsurile dispuse prin ordinul de protecție constituie infracțiunea de nerespectare a hotărârii judecătorești și se pedepsește cu închisoare de la o lună la un an. Împăcarea înlătură răspunderea penală.

Plângerea prealabilă

- Poți depune o plângere prealabilă fie la poliție, fie la parchet. Pentru a-și produce efectele, plângerea prealabilă trebuie introdusă în termen de 3 luni de la data săvârșirii faptei.

Cererea de divorț și ordonanța președințială

- Poți depune o cerere de divorț și poți cere o ordonanță președințială care să aibă ca rezultat stabilirea domiciliului minorilor și evacuarea temporară

a agresorului din locuință.

Solicită sprijin

- Sună la 112 și să solicite sprijin atunci când viața și sănătatea ta și a copiilor tăi sunt puse în pericol!
- Solicită ajutor medical deoarece rănilor se pot agrava rapid.
- Solicită consult medico-legal și eliberarea unui certificat constatator, indiferent de gravitatea loviturilor. Faptul că, din punctul tău de vedere, nu există urme vizibile ale abuzului, nu înseamnă că un specialist din cadrul IMNL nu poate constata, analiza și declara abuzul. Acest act poate fi o dovadă importantă în demersurile legale pe care le poți întreprinde.
- De asemenea, unele organizații non-guvernamentale care au dezvoltat programe pentru susținerea femeilor victime ale violenței domestice, pe baza chitanței în original, pot deconta această taxă.
- Depune o plângere penală împotriva agresorului. Deși plângerea poate fi făcută și verbal, totuși este mai bine să formulezi o plângere în scris, deoarece aceasta poate fi depusă direct la registratura secției de poliție sau a parchetului și să primești un număr de înregistrare, cu ajutorul căruia vei putea urmări stadiul cercetărilor penale.
- Dacă solicite intervenția echipajului de poliție la domiciliu pentru constatarea unei agresiuni și obiectele sunt răvășite, există pete de sânge, nu face ordine deoarece polițiștii trebuie să observe locul faptei așa cum este.
- În cazul unei agresiuni sexuale, nu te spăla și nu-ți schimba hainele, pentru a nu distruge probele necesare medicilor legiști.

Numere de telefon utile

- Serviciul unic de urgență -112
- Numărul unic național de urgență pentru victimele violenței domestice - 0800.500.333. Serviciul este asigurat 24/24 ore, 7/7 zile. Numărul este apelabil gratuit din orice rețea cu acoperire națională.
- Secțiile de poliție
- Direcțiile Generale de Asistență Socială și Protecția Copilului/ Serviciile Publice de Asistență Socială
- Centrele de urgență
- Centrele de consiliere
- Locuințele protejate

FUNDAȚIA SENSIBLU

CENTRUL DE CONSILIERE CASA BLU

Telefon / Fax: 021 - 311 46 36

Mobil : 0787 54 18 54

fundatia.sensiblu@adpharma.com

www.fundatiasensiblu.ro

<https://www.facebook.com/Fundatia.Sensiblu>

Ghid realizat de **Fundația Sensiblu**
Copyright @ 2021