

Stalkerware en spyware

De verborgen dreiging van digitale controle

Samenvatting

Dit whitepaper beschrijft de resultaten van een onderzoek door DataExpert naar de werking en risico's van stalkerware. Het onderzoek laat zien dat deze apps in enkele minuten geïnstalleerd kunnen worden, vaak onzichtbaar blijven voor het slachtoffer en diep ingrijpen op de privacy. Functionaliteiten als live meekijken via de camera, meeluisteren met gesprekken en het vastleggen van toetsaanslagen maken complete surveillance mogelijk.

Parental control-apps lijken onschuldig. Ze worden gepresenteerd als hulpmiddelen om kinderen online te beschermen. Maar in de praktijk worden deze apps steeds vaker misbruikt als stalkerware: software waarmee daders slachtoffers volgen, controleren en intimideren.

De ernst van stalking wordt vaak onderschat. Stalking is vaak een voorspeller van ernstiger geweld, vooral tegen vrouwen. Tussen de 2 en 13 procent van de stalking-zaken eindigt in een poging tot moord of daadwerkelijk moord. Het tijdig herkennen en aanpakken van stalkerware is daarom van levensbelang.



“ Voor opsporingsdiensten en hulpverleners is het cruciaal om te weten hoe stalkerware werkt, hoe ze het herkennen en hoe ze veilig handelen. Onvoorzichtig verwijderen kan leiden tot escalatie en fysiek gevaar voor het slachtoffer. ”

De schaduwzijde van monitoringtechnologie

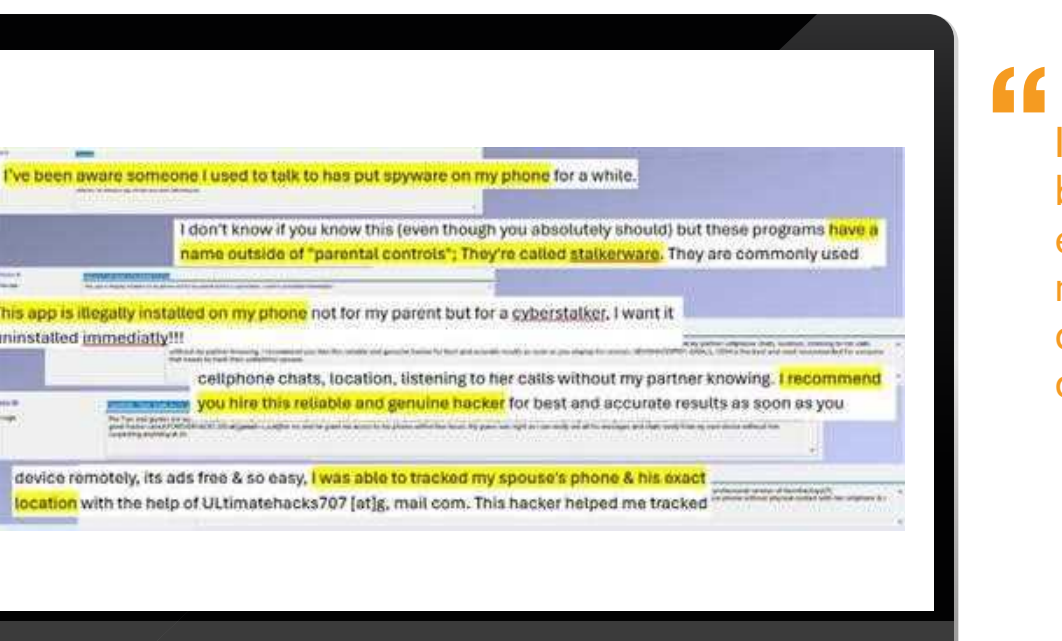
De opkomst van monitoring- en controletechnologie kent een keerzijde. Wereldwijd groeit het gebruik van stalkerware: software dat - vaak heimelijk - op een apparaat wordt geïnstalleerd om iemands activiteiten te volgen, te monitoren of te bespioneren zonder diens expliciete toestemming (Kaspersky, 2024).

De meest bekende monitoringsoftware vallen onder de categorie parental control apps. Dit zijn apps die bedoeld lijken voor ouderlijk toezicht, maar in werkelijkheid ook worden ingezet voor ongeoorloofde surveillance. Waar parental control-apps eigenlijk bedoeld zijn om kinderen (online) te beschermen, bevatten ze steeds vaker functies die diep ingrijpen in iemands privacy. Denk aan live meekijken via de camera, het meeluisteren met gesprekken of het registreren van toetsaanslagen. Deze apps vernemen zich als andere onschuldige apps waardoor iemand niet doorheeft dat die wordt gevolgd (Kaspersky, 2024). De grens tussen bescherming en controle vervaagt.

Het zonder toestemming volgen van iemands telefoonactiviteiten is strafbaar (Art. 285b Sr). Toch wordt stalker-

ware geregeld gebruikt binnen relaties met een patroon van huiselijk geweld of intieme terreur. Slachtoffers voelen zich daardoor continu onveilig. Voor opsporings- en veiligheidsdiensten is het essentieel om te begrijpen hoe deze apps werken, hoe ze zich verspreiden en hoe ze opgespoord kunnen worden.

Het onderzoek naar stalkerapps binnen DataExpert werd opgezet vanuit een maatschappelijke motivatie. Analyse-trainer Michelle Rasch, met een achtergrond in criminologie: "Ik zag steeds vaker berichten in het nieuws en posts op sociale media van slachtoffers die werden gevolgd via dit soort apps." Samen met Jorien Bijlmer (analyse-trainer) en Jenneke Boer (OSINT-trainer) besloot zij te onderzoeken hoe spy- en stalkerapps worden gebruikt, welke risico's ze opleveren en hoe je slachtoffers hiertegen beschermt.



“ Ik zag steeds vaker berichten in het nieuws en posts op sociale media van slachtoffers die werden gevolgd via dit soort apps. ”

Wat is stalking en waarom is het zo ernstig?

De Nederlandse juridische definitie van stalking (belaging) luidt als volgt: het onrechtmatig en systematisch schenden van de persoonlijke levenssfeer van een ander met het doel hem te dwingen iets te doen, iets niet te doen of te tolereren, of hem bang te maken (Art. 285b Sr).

Stalking omvat het herhaaldelijk, opzettelijk en structureel lastigvallen van een andere persoon. Dit kan uiteenlopende vormen aannemen: van fysieke tot digitale intimidatie, zoals ongewenste e-mails, berichten of telefoontjes, het volgen of controleren van iemands doen en laten, of het heimelijk bespioneren van iemands (online) activiteiten (European Institute for Gender Equality, 2019).

Vindt dit gedrag online plaats, dan spreken we van cyberstalking of online stalking. Hierbij zet de dader internet, sociale media, e-mail, GPS en andere digitale middelen in om het slachtoffer te controleren of te intimideren.

Wanneer iemand technologie op een bredere manier inzet om iemand anders te volgen, te beïnvloeden of te bedreigen (bijvoorbeeld via spyware, tracking-apps of slimme apparaten), dan noemen we dit technologie gestuurde stalking (Derksen et al., 2024) (Kaspersky, 2024). Deze vorm van stalking kan zeer indringend zijn, omdat de dader toegang kan verkrijgen tot het dagelijkse leven en digitale sporen van het slachtoffer, zonder fysieke aanwezigheid.

Er worden in de regel vier hoofdvormen onderscheiden:



Bewaking

Het volgen, observeren of monitoren van iemand, ofwel fysiek ofwel digitaal.



Inbreuk op de privacy

Het binnendringen in persoonlijke ruimtes of accounts, bijvoorbeeld via inbraak, hacking of ongeoorloofde toegang tot sociale media.



Intimidatie

bedreigingen, manipulatie of het creëren van angst door herhaald contact of verspreiding van persoonlijke informatie.



Verstoring door sabotage of aanvallen

bijvoorbeeld het beschadigen van eigendommen, reputatie of sociale relaties (Logan & Walker, 2017).



De ernst: stalking als voorspeller van geweld

Stalking is geen onschuldig gedrag. Het is vaak een voorspeller van ernstiger criminaliteit. Tussen de 2 en 13 procent van de stalkingzaken eindigt in een poging tot moord of daadwerkelijke moord (Arends et al., 2025). Vooral femicide (vrouwenmoord) wordt vaak voorafgegaan door stalking (Russell & Van de Ven, 1990).

Dit is precies de reden dat er wetgeving rondom stalking is gekomen: stalking moet vroeg worden gestopt om escalatie naar zwaarder geweld te voorkomen (European Institute for Gender Equality, 2019).

Meer dan 50 procent van de slachtoffers kent de dader persoonlijk. Bij vrouwen gaat het in de meeste gevallen om een ex-partner (Derksen et al., 2024).

Stalking heeft ook een hoge mate van recidive. Daders blijven herhaald gedrag vertonen, ook na confrontatie of aangifte. Het vroegtijdig herkennen en aanpakken van stalking is daarom cruciaal (Arends et al., 2025).

De impact van stalkerware op slachtoffers is groot. Het creëert een gevoel van constante onveiligheid. Slachtoffers weten niet wanneer ze worden gevolgd, afgeluisterd of bespied. Dit leidt tot angst, stress en sociaal isolement.

Veel apps maken verregaande inbreuk op de persoonlijke levenssfeer van het slachtoffer. Daarbij kan ook fysiek gevaar ontstaan voor degene die in de gaten wordt gehouden.

Wie lopen risico?

De kans op cyberstalking verschilt per groep. Uit recente cijfers blijkt dat:

- ✓ **vrouwen** ongeveer anderhalf keer zo vaak slachtoffer zijn als mannen;
- ✓ **jongeren van 15 tot 25 jaar** bijna tweemaal zo vaak worden getroffen als andere leeftijdsgroepen;
- ✓ slachtoffers bovengemiddeld vaak wonen in **grotere steden**;
- ✓ **lesbische vrouwen, homoseksuele mannen en biseksuele vrouwen** vaker melding maken van cyberstalking.

In 2024 gaf 1,2 procent van de Nederlandse bevolking aan ooit slachtoffer te zijn geweest van cyberstalking (Akkermans et al., 2024). Daarnaast dacht 20 procent dat zij risico liepen, terwijl 80 procent die kans klein inschatte. De toename van cyberstalking gaat sneller dan bij andere vormen van stalking.

Het profiel van de dader

Wie?

Belangrijke kenmerken van stalkers zijn: jaloezie, weinig vertrouwen in anderen en een sterk controlerend of bezitterig karakter. Online en offline vormen van stalking gaan vaak samen (Miller, 2012) (Kapersky, 2024).

Waarom?

De belangrijkste motivatie van een dader is de behoefte aan controle. Veel stalkers willen hun macht over het slachtoffer behouden of vergroten. Vaak speelt achterdocht een rol; de wens om vermoedens van ontrouw te bevestigen of de angst om verlaten te worden. Ze gebruiken stalkerware om onzekerheid en verlies van grip te compenseren (Miller, 2012).

Wanneer?

Het gebruik van stalkerware piekt vaak in emotioneel beladen periodes: rond een (dreigende) relatiebreuk of tijdens stressvolle levensfasen zoals baanverlies, een verhuizing of zwangerschap. In die periodes neemt de behoefte aan controle en bevestiging toe, wat het risico op misbruik van monitoringtechnologie vergroot (Miller, 2012).

Hoe lastig is het om stalkerware te installeren?

Het onderzoek van DataExpert laat zien dat het opvallend eenvoudig is om een stalkerapp te installeren. In de meeste gevallen duurde de installatie niet langer dan 5 tot 15 minuten. De instructies waren duidelijk, waardoor

“ We waren verrast door het installatiegemak. Alleen gebruikers die totaal geen technische kennis hadden, liepen soms vast. Voor de meesten is het gewoon een kwestie van de instructies volgen. ”

het bijna iedereen lukte om de apps te plaatsen op het toestel van een ander, mits zij fysieke toegang hadden tot de telefoon.

Tijdens de installatie moest de gebruiker uitgebreide toestemmingen geven over bijvoorbeeld locatie-, microfoon- en cameratoegang. In sommige gevallen werd zelfs om administratorrechten gevraagd, waardoor de app volledige controle kreeg over het toestel. Sommige apps verwijderden automatisch hun pictogram of plaatsten het in een verborgen map, waardoor ze voor het slachtoffer onzichtbaar bleven.

Wat kan stalkerware allemaal?

De mogelijkheden van stalkerware-apps zijn de afgelopen jaren sterk uitgebreid. Bijna alle onderzochte apps vertonen dezelfde kernfunctionaliteiten:



Locatiebepaling: realtime volgen van bewegingen en geofencing (melding bij betreden of verlaten van een gebied).



Berichteninzicht: lezen van inkomende en uitgaande tekstberichten.



Oproepgeschiedenis: overzicht van inkomende, uitgaande en gemiste gesprekken.



Toegang tot foto's: volledige inzage in opgeslagen beeldmateriaal.



Social media monitoring: meekijken met activiteiten en interacties op platforms.



Browsergeschiedenis en zoekgeschiedenis: inzicht in wat het slachtoffer online opzoekt.

Deze functies maken het mogelijk om niet alleen het gedrag, maar ook het sociale netwerk en de dagelijkse routines van een slachtoffer te reconstrueren en te controleren. Daarmee overschrijdt de dader de scheidslijn tussen toezicht en inbreuk op privacy volledig. En is het lastig voor het slachtoffer om uit deze situatie te komen.

Naast deze kernfuncties bieden sommige stalkerware-apps geavanceerdere mogelijkheden die diepgaande inbreuk maken op privacy en veiligheid:



Scheruweergave (screen mirroring): in realtime zien wat er op het scherm gebeurt.



Camera activeren: de camera van het toestel inschakelen om mee te kijken.



Microfoon activeren: het toestel als af luisterapparaat gebruiken.



Toetsaanslagregistratie (keylogs): vastleggen van ingetikte tekst, inclusief wachtwoorden en berichten die nog niet zijn verstuurd.



Parental control-apps als stalkerware

Een opvallend technisch aspect is het gebruik van zogenoemde parental control-apps. Deze toepassingen behoren tot de meest gebruikte vormen van stalkerware in cyberstalkingzaken (Kapersky, 2024).

“ De onschuldige positionering van parental control-apps als toezichtsoftware maakt ze moeilijk te onderscheiden van legitieme beveiligingsapps, terwijl ze in de praktijk vaak worden misbruikt voor digitale controle. ”

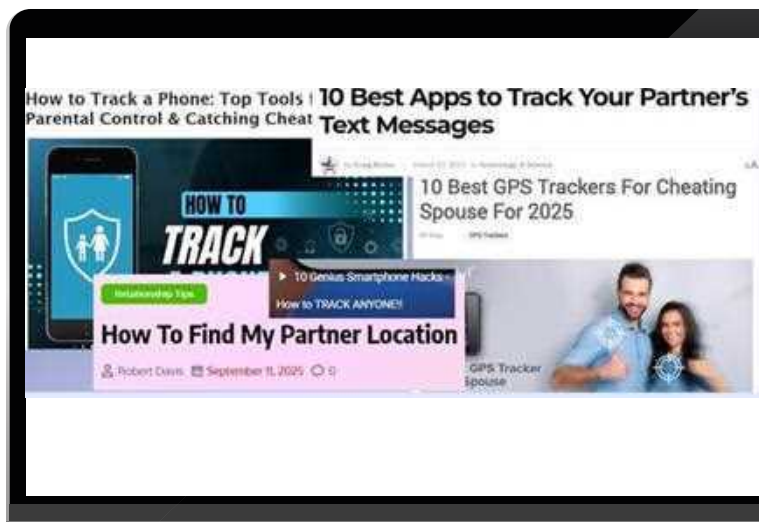
Naast de parental control-apps zijn er ook apps en software beschikbaar op alternatieve websites en op het darkweb. Veel hiervan zijn zo ontworpen dat ze moeilijk te herkennen en verwijderen zijn. Stalkerware op het darkweb is geavanceerder en risicovoller dan de versies in officiële appstores. Daar bestaan geen beperkingen op functies, waardoor de tools vaak stabielere werken en soms zelfs zonder fysieke toegang op de telefoon kunnen worden geïnstalleerd (Kapersky, 2024).

Herkenning: signalen van stalkerware

De aanwezigheid van stalkerware is niet altijd zichtbaar. Op het toestel van het slachtoffer blijven deze activiteiten vaak onzichtbaar. Apps verbergen zichzelf of gebruiken misleidende pictogrammen. Daardoor kunnen slachtoffers langdurig gevolgd worden zonder het te weten.

Mogelijke aanwijzingen voor stalkerware zijn:

- ✔ **Prestatieproblemen:** apps lopen vast of reageren traag doordat stalkerware op de achtergrond systeembronnen gebruikt. Bij krachtigere telefoons blijven deze vertragingen soms onopgemerkt.
- ✔ **Ongewone batterijduur:** de batterij raakt sneller leeg dan normaal.
- ✔ **Verhoogd dataverbruik:** plotselinge stijging van dataverbruik zonder duidelijke oorzaak.
- ✔ **Oververhitting:** het toestel voelt warm aan, zelfs bij beperkt gebruik.
- ✔ **Onbekende meldingen of pictogrammen:** vreemde meldingen of icoontjes zonder herleidbare bron.



- ✔ **Apps met buitensporige toestemmingen:** toegang tot contacten, locatie of microfoon zonder logische reden.
- ✔ **Bijsluisteren tijdens gesprekken:** klikken of ruis kunnen wijzen op meeluisteren.
- ✔ **Onbekende apps:** aanwezigheid van applicaties die niet bewust zijn geïnstalleerd.
- ✔ **Cydia op iOS:** alternatieve appstore voor 'jailbroken' toestellen waarmee stalkerware kan worden geïnstalleerd.
- ✔ **Onverklaarbare kennis:** iemand weet details over locaties of gesprekken die alleen via het toestel te achterhalen zijn.
- ✔ **Verdwijnen van het toestel:** een telefoon die tijdelijk weg is geweest, kan zijn gebruikt voor installatie.

Let op: deze signalen zijn geen sluitend bewijs voor de aanwezigheid van stalkerware. Veel van deze verschijnselen kunnen ook een andere oorzaak hebben. Bespreek vermoedens daarom bij voorkeur met een hulpverlener of politie, en confronteer een (ex-)partner niet impulsief met deze vermoedens. Dat kan de veiligheid verder in gevaar brengen.

“ Apps maken bewust reclame voor het tracken van een partner of het betrappen van een partner die vreemdgaat. Dit terwijl het gebruik van dergelijke apps bij volwassenen zonder toestemming niet is toegestaan. ”



Wat te doen bij vermoedens van stalkerware?

Bij een vermoeden van stalkerware is het cruciaal om niet impulsief te handelen. Onvoorzichtige acties kunnen het risico op escalatie voor het slachtoffer vergroten, zeker wanneer de stalker meekijkt.

Aanbevolen stappen:

- ✓ **Verwijder de stalkingapp niet als je niet veilig bent van de (mogelijke) dader(s).**
- ✓ **Maak een veiligheidsplan:** overleg met hulpinstanties of politie voordat je stappen zet.
- ✓ **Verwijder de app op een neutrale locatie:** dus niet vlak bij een vrouwenopvang of een politiebureau.
- ✓ **Verwijderen via factory reset:** in veel gevallen kan stalkerware hiermee worden verwijderd. Maak eerst een kopie van de simkaart of noodzakelijke gegevens.
- ✓ **Let op bij geavanceerde malware:** sommige varianten kunnen een factory reset omzeilen of stappen overslaan. In die gevallen is een nieuw toestel de enige oplossing.
- ✓ **Wees voorzichtig met accounts op een nieuw toestel:** controleer instellingen van Google, iCloud en sociale media om te voorkomen dat oude koppelingen opnieuw toegang geven.
- ✓ **Documenteer en rapporteer:** noteer waargenomen signalen, maak waar mogelijk screenshots en meld het bij de politie.

Conclusies en aanbevelingen

Dit onderzoek toont aan dat apps die zichzelf profileren als parental control-apps kunnen worden misbruikt in huiselijk geweld- en stalkingsituaties.

De drempel om deze apps te installeren is laag, terwijl de impact op slachtoffers vaak enorm is.

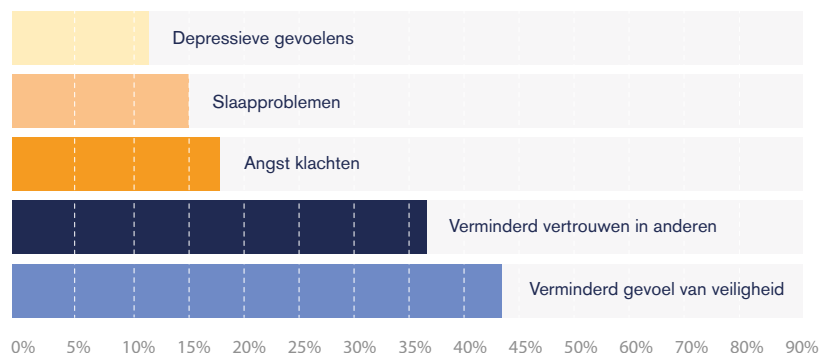
Naast de parental control-apps zijn er ook apps en software beschikbaar op alternatieve websites en op het darkweb. Het merendeel hiervan is zo ontworpen dat ze moeilijk te herkennen en verwijderen zijn. Veel apps maken bewust reclame voor het tracken van een partner of het betrappen van een partner die vreemdgaat. Dit

terwijl het gebruik van dergelijke apps bij volwassenen zonder toestemming niet is toegestaan.

Veel apps maken verregaande inbreuk op de persoonlijke levenssfeer. Daarbij kan ook een fysiek gevaar ontstaan voor degene die in de gaten wordt gehouden. Bij vermoedens van de aanwezigheid van stalkingsapps of -software moet er veel aandacht zijn voor de veiligheid van het slachtoffer. Het verwijderen van een app kan leiden tot escalatie van gedrag en mogelijk geweld triggeren.

Meer dan 30% van de slachtoffers van cyberstalking gaf aan emotionele en psychologische gevolgen te ervaren.

Gevolgen van cyberstalking



Aanbevelingen voor opsporingsdiensten en hulpverleners:

- ✓ Ontwikkel kennis over de werking van stalkerware en de risico's voor slachtoffers.
- ✓ Werk samen met slachtofferhulp en andere instanties om een veilige verwijdering te waarborgen.
- ✓ Stel veiligheidsplannen op voordat stalkerware wordt verwijderd.
- ✓ Documenteer en rapporteer gevallen van stalkerware om patroonherkenning mogelijk te maken.
- ✓ Wees alert op signalen van stalkerware bij meldingen van huiselijk geweld of stalking.

Technische aanpak van het onderzoek

Tijdens het onderzoek werkten de onderzoekers met eigen tooling. Ze schreven Python-scripts voor het analyseren van reviews en Reddit-discussies en gebruikten i2 iBase voor dataverwerking. Dit maakte het mogelijk om patronen te identificeren in hoe stalkerware wordt aangeprezen, besproken en gebruikt.

Over de onderzoekers

Het onderzoek is uitgevoerd door drie specialisten binnen DataExpert, een kennispartner op het snijvlak van OSINT, digitale forensics en data-analyseonderzoek.

Michelle Rasch

Analyse-trainer met een achtergrond in criminologie en psychologie. Ervaring met wetenschappelijk onderzoek, slachtofferhulp, huiselijk geweld, stalking en zeden.

Jorien Bijlmer

Analyse-trainer met ervaring in het relationeel doorzoeken en visualiseren van gegevens in iBase en Analyst's Notebook.

Jenneke Boer

OSINT-trainer met een achtergrond in forensisch onderzoek en een sterke interesse in programmeren en het dark web.

Bronnen

Akkermans, M., Derksen, E.L.J., Kennis, M.I.J., Kloosterman, J.G., & Moons, E.A.L.M.G. (2024). Veiligheidsmonitor 2023, Centraal Bureau van de Statistiek, 1-118.

Arends, J., Derksen, E.L.J., & Morren, M. (2025). Online Veiligheid en Criminaliteit 2024, Centraal Bureau van de Statistiek, 1-59.

Derksen, E.L.J., Kennis, M.I.J., Kloosterman, J.G., Moons, E.A.L.M.G., & Peters, V.B.M. (2024). Prevalentiemonitor Huiselijk Geweld en Seksueel Grensoverschrijdend gedrag 2024, Centraal Bureau van de Statistiek, 1-68.

European Institute for Gender Equality (2019). Legal definitions in the EU member states. <https://eige.europa.eu/gender-based-violence/regulatory-and-legal-framework/legal-definitions-in-the-eu>

Kaspersky. (2024). The state of stalkerware in 2023. <https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2024/03/07160820/The-State-of-Stalkerware-in-2023.pdf>

Logan, T. K., & Walker, R. (2017). Stalking: A multidimensional framework for assessment and safety planning. Trauma, Violence, & Abuse, 18(2), 200–222. <https://doi.org/10.1177/1524838015603210>

Miller, L. (2012). Stalking: Patterns, motives and intervention strategies. Aggression and Violent Behavior, 17, 495–506. <https://doi.org/10.1016/j.avb.2012.07.001>

Russell, D. E. H., & Van de Ven, N. (1990). Crimes against women: Proceedings of the international tribunal. Russell Publications.

Wetboek van Strafrecht. (n.d.). Art. 285b (Titel XVIII). <https://wetten.overheid.nl/BWBR0001854>