Aanbeveling

van het Instituut voor de gelijkheid van vrouwen en mannen nr. 2022/R/002

betreffende het gebruik van stalkerware in het kader van (ex-)partnergeweld

INSTITUUT VOOR
DE GELIJKHEID
VAN VROUWEN
EN MANNEN

I. Bevoegdheid van het Instituut voor de gelijkheid van vrouwen en mannen

Het Instituut werd opgericht door de wet van 16 december 2002 en heeft onder andere als opdracht om te waken over de naleving van de wetgeving inzake de gelijkheid van vrouwen en mannen en om elke vorm van discriminatie of ongelijkheid op grond van geslacht te bestrijden.

II. De context van de aanbeveling

De snelle ontwikkeling van informatie- en communicatietechnologieën biedt geweldplegers nieuwe en bijkomende mogelijkheden. Volgens GREVIO wordt deze digitale dimensie van geweld echter onderbelicht. Zo ook **stalkerware**, een uiterst verontrustende vorm van (ex-)partnergeweld, maar desondanks nog relatief onbekend in België.[2]

Zo stelt GREVIO in hun *General Recommendation No. 1 on the digital dimension of violence against women* dat *"Many domestic laws fail to reflect other important impacts of acts of such violence, including social, economic, psychological and participatory harms. Very few consider and specifically address the compound experiences of women and girls and do not place it in the context of a continuum of violence against women that women and girls are exposed to in all spheres of life, including in the digital sphere. (…) Similarly, national responses to gender-based violence against women rarely include the digital dimension of such violence. This is particularly pronounced in the context of responding to domestic violence."*[3]

1. Wat is stalkerware

Stalkerware omvat alle **commercieel beschikbare software**, vaak in de vorm van een **app**, die een derde in staat stelt om **vanop afstand** het toestel (**smartphone, tablet of computer**) van een persoon en diens activiteit daarop **in de gaten te houden/te gebruiken zonder** de **toestemming** van de persoon in kwestie. Het bespioneren van andermans toestel gebeurt bovendien **heimelijk**. Eenmaal de software op het toestel is geïnstalleerd, krijgt de gebruiker geen notificaties die duidelijk maken dat haar of zijn activiteit in de gaten wordt gehouden of door een ander wordt gemanipuleerd. Naast het begrip 'stalkerware' worden ook de begrippen '**creepware'** of '**spouseware'** gebruikt om dergelijke software aan te duiden.[4]

1.1. Technologische aspecten

In tegenstelling tot het overkoepelende fenomeen 'spyware' is **fysieke toegang** tot het toestel noodzakelijk om stalkerware te installeren. Bij iOS-toestellen kan men zich ook via het iCloud-account van het doelwit toegang tot het toestel verschaffen.[5] Indien fysieke toegang niet mogelijk is, kan de dader ervoor kiezen om een toestel waarop reeds stalkerware is geïnstalleerd, als cadeau aan het

[2] Op 10 maart 2022 nam het Instituut deel aan de online conferentie inzake digitaal geweld tegen vrouwen. Deze conferentie werd georganiseerd door de Fund Operators of the EEA Grants Active Citizens Fund in Greece and Cyprus, in samenwerking met de Raad van Europa en de Noorse Minister van Justitie. Tijdens de conferentie gaf de Raad van Europa onder meer toelichting over digitaal seksueel geweld ten aanzien van vrouwen en lichtte GREVIO hun nieuwe aanbeveling inzake digitaal geweld toe. Deze conferentie voorzag ook in een uiteenzetting omtrent stalkerware.

[3] GREVIO General Recommendation No. 1 on the digital dimension of violence against women. 20 October 2021. Geraadpleegd van https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147.

[4] Coalition Against Stalkerware. (z.d). *Information for tech companies.* Geraadpleegd van https://stopstalkerware.org/information-for-tech-companies

[5] Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm ? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

slachtoffer te geven.[6] Er zijn zelfs bedrijven die hierin gespecialiseerd zijn. Zij installeren de stalkerware op een nieuw toestel naar keuze en leveren het indien gewenst zelfs rechtstreeks aan het slachtoffer. Er wordt daarbij extra aandacht besteed aan de verpakking. Aangezien dezelfde verpakking wordt gebruikt als de fabrieksverpakking, is er geen indicatie dat de verpakking reeds werd geopend en er dergelijke software op het toestel werd geplaatst.[7]

Stalkerware is **commercieel gemakkelijk beschikbaar**. In enkele muisklikken is er via het (reguliere) internet een breed gamma aan softwareprogramma's en apps terug te vinden die eenvoudig en zonder specifieke technologische kennis te installeren zijn.[8] Ze zijn zelfs via de Google Play Store (Android) en Apple App Store (iOS) terug te vinden. Sommige zijn gratis te gebruiken, andere werken via een betalend abonnement. Voor ongeveer 20 tot 30 euro per maand kan je zonder problemen meekijken met iemands digitale activiteiten.[9]

Om onder de radar te blijven, maken bedrijven die stalkerware aanbieden gretig gebruik van een slimme **marketingtruc**: ze profileren zich als **veiligheids- of antidiefstal-app**. Daarbij richten ze zich specifiek op ouders die hun kinderen of werkgevers die hun werknemers in de gaten willen houden.[10] Toch proberen app stores om stalkerware apps te weren uit hun aanbod. In de Google Play Store bijvoorbeeld zijn apps die gebruikers traceren en data naar een ander toestel doorsturen enkel nog toegestaan wanneer ze voortdurend een melding geven dat tracking aanstaat.[11] Desondanks glippen nog steeds een deel van deze apps door de mazen van het net.

Voor de gebruiker blijven stalkerware software of apps **verborgen**. Ze opereren in **stealth modus** waardoor er bijvoorbeeld geen icoontjes zijn die aan de gebruiker duidelijk maken dat zulke software op het toestel aanwezig is, laat staan op de achtergrond actief is en haar of zijn activiteiten in de gaten houdt.[12] Indien ze niet verborgen zijn, **doen ze zich voor als legitieme apps**. Met namen zoals 'battery saver' of 'system services' wekken ze dikwijls geen argwaan op.[13] Je moet als gebruiker dus al kennis hebben van wat stalkerware is en wat de signalen zijn die wijzen op de aanwezigheid van stalkerware, om het te kunnen detecteren.

1.2. Waarom wordt stalkerware gebruikt door daders van (ex-)partnergeweld

Smartphones, tablets en computers zijn zodanig ingebed in de hedendaagse samenleving dat ze niet meer weg te denken zijn uit onze persoonlijke, sociale en professionele levens. Die inbedding is zo allesomvattend dat "*full access to a person's phone, is the next best thing to full access to a person's*

---

[6] Kaspersky. (2022). *The state of stalkerware in 2021.* Geraadpleegd van https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/04/12075509/EN_The-State-of-Stalkerware-2021.pdf

[7] DeStalk. (2022). E-learning course cyberviolence and stalkerware (intermediate): introduction to stalkerware.

[8] Davidovic, I. (2021, 3 december). How to spot the software that could be spying on you. *BBC News.* Geraadpleegd van https://www.bbc.com/news/business-59390778; Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van ttps://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

[9] Davidovic, I. (2021, 3 december). How to spot the software that could be spying on you. *BBC News.* Geraadpleegd van https://www.bbc.com/news/business-59390778; Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

[10] Clerix, K. (2022, 2 februari). *"In België zijn er duizenden mensen die met stalkerware bespioneerd worden"/Interviewer S. Lemaire.* De wereld van Sofie. Geraadpleegd van https://radio1.be/luister/select/nieuwe-feiten/in-belgie-zijn-er-duizenden-mensen-die-met-stalkerware-bespioneerd-worden

[11] Google. (2020, 16 september). *Developer program policy: September 16, 2020 announcement.* Geraadpleegd van https://support.google.com/googleplay/android-developer/answer/10065487

[12] Kaspersky. (2021). *The state of stalkerware in 2020.* Geraadpleegd op 22 februari 2022, van https://securelist.com/the-state-of-stalkerware-in-2020/100875/

[13] Davidovic, I. (2021, 3 december). How to spot the software that could be spying on you. *BBC News.* Geraadpleegd van https://www.bbc.com/news/business-59390778; Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

mind".[14] Het hoeft dan ook niet te verbazen dat daders van (ex-)partnergeweld hiervan gebruik (proberen te) maken. Dankzij stalkerware krijgen daders niet alleen heel veel informatie over het doen en laten van hun slachtoffer, maar met die informatie kunnen ze ook inzetten om **dwingende controle** ('coercive control') uit te oefenen op hun slachtoffer of om die juist te intensiveren.[15]

Daarnaast kan de verkregen informatie ook gebruikt worden bij **gaslighting,** een heel subtiele manipulatietechniek die het slachtoffer doet twijfelen aan de waarachtigheid van diens eigen woorden, gedachten en herinneringen. Zoals hierna zal worden aangehaald (infra 1.3), biedt sommige stalkerware de mogelijkheid om sms'en te verzenden in naam van het slachtoffer. Er wordt daarbij geen spoor op het toestel van het slachtoffer nagelaten waaraan het slachtoffer kan weten dat een sms is verstuurd. Hierdoor kan het slachtoffer aan zichzelf beginnen twijfelen: *"Heb ik misschien toch dat bericht verstuurd?"*. Op lange termijn resulteert dit in extreme onzekerheid en verlies van zelfvertrouwen. [16]

Zowel **tijdens een relatie als na een breuk of scheiding** maken daders gebruik van stalkerware.[17] Bovendien wordt niet alleen uitsluitend de (ex-)partner in de gaten gehouden. Door de vele mogelijkheden die stalkerware biedt, kan ook heel wat informatie over de (ex-)partner verkregen worden via een toestel van een gezamenlijk **kind**. [18]

Het is belangrijk om te vermelden dat bij (ex-)partnergeweld altijd aandachtig moet gekeken worden naar de volledige context waarin het geweld plaatsvindt. Digitale vormen van geweld staan namelijk niet op zichzelf, maar gaan **vaak gepaard met** uitingen van geweld in de 'fysieke' wereld zoals **emotioneel, verbaal, psychologisch, fysiek of seksueel geweld**.[19] Zo blijkt uit gegevens van de Europese FRA-enquête (2014) over geweld tegen vrouwen dat 7 op 10 vrouwen die een vorm van cyberstalking hebben meegemaakt, ook minstens één vorm van fysiek en/of seksueel geweld door een partner hebben ondervonden.[20]

1.3. Hoe wordt stalkerware gebruikt door daders van (ex-)partnergeweld?

Wat een dader precies in de gaten kan houden, is afhankelijk van het type software en voor welk besturingssysteem (Android of iOS) de stalkerware wordt ontwikkeld. In het algemeen kan stalkerware gebruikmaken van **alle sensoren** (geluid, camera, *touch screen*, enz.) van een toestel. [21]

---

[14] Gasperin, E. (2019, december). *What you need to know about stalkerware* [Video]. Ted Conferenties. Geraadpleegd van https://www.ted.com/talks/eva_galperin_what_you_need_to_know_about_stalkerware

[15] Chan, S. (2021). Hidden but deadly: stalkerware usage in intimate partner stalking. In M. Khader, W.X.T. Chai & L.S. Neo (Eds.), *Cyber forensic psychology: understanding the mind of cyber deviant perpetrators* (pp. 45-66). World Scientific.; Dragiewicz, M., Woodlock, D., Harris, B. A., & Reid, C. (2019). Technology-facilitated coercive control. In W. S. De Keseredy, C. M. Rennison, & A. K. Hall-Sanchez (Eds.), *The Routledge International Handbook of Violence Studies* (pp. 244-253). Routledge. https://doi.org/10.4324/9781315270265-23

[16] York Morris, S., & Raypole, C. (2022, 24 november). *How to recognize gaslighting and get help. https://www.healthline.com/health/gaslighting#:~:text=Gaslighting%20is%20a%20form%20of,they%20question%20their%20own%20sanity)*

[17] Chan, S. (2021). Hidden but deadly: stalkerware usage in intimate partner stalking. In M. Khader, W.X.T. Chai & L.S. Neo (Eds.), *Cyber forensic psychology: understanding the mind of cyber deviant perpetrators* (pp. 45-66). World Scientific.

[18] Dragiewicz, M., Woodlock, D., Harris, B. A., & Reid, C. (2019). Technology-facilitated coercive control. In W. S. De Keseredy, C. M. Rennison, & A. K. Hall-Sanchez (Eds.), *The Routledge International Handbook of Violence Studies* (pp. 244-253). Routledge. https://doi.org/10.4324/9781315270265-23

[19] GREVIO. (2021). *General recommendation no. 1: On the digital dimension of violence against women.* Adopted on October 20, 2021). Geraadpleegd van https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

[20] FRA (2014). *Violence against women: an EU-wide survey.* Rapport van de resultaten te raadplegen via http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report; European Institute for Gender Equality. (2017). *Cybergeweld tegen vrouwen en meisjes.* Geraadpleegd van file:///C:/Users/ellen/Downloads/ti_pubpdf_mh0417543nln_pdfweb_20171026164003%20(2).pdf

[21] Davidovic, I. (2021, 3 december). How to spot the software that could be spying on you. *BBC News.* Geraadpleegd van https://www.bbc.com/news/business-59390778

Stalkerware specifiek ontwikkeld voor **Android toestellen** biedt meer mogelijkheden aan daders om hun (ex-)partner in de gaten te houden. Volgende zaken kunnen onder meer door daders gecontroleerd worden[22]:

- Locatie
- Spraakoproepen (meeluisteren in real life en opnames)
- Foto's
- Zoekopdrachten via het internet (via *keystroke logging*)
- Sms-berichten
- Camera (ook vanop afstand foto's nemen)
- Geluid
- Activiteiten op andere apps zoals sociale media apps (vb. Whatsapp) of email apps

Naast passief meevolgen kan een dader via stalkerware ook de functies van het geïnfecteerde toestel beperken. Een dader kan onder meer[23]:

- Inkomende oproepen weigeren vanop afstand
- Bepaalde websites blokkeren
- Berichten verzenden in naam van het slachtoffer (sms-spoofing) waarbij de verzonden berichten verborgen zijn voor het slachtoffer en niet terug te vinden zijn in de berichtengeschiedenis

iOS-stalkerware is doorgaans beperkter in mogelijkheden. Door het meer 'gesloten systeem' van iOS-toestellen is stalkerware installeren op iPhones ook moeilijker. Stalkerware gericht op iOS-toestellen maakt dan ook hoofdzakelijk gebruik van het iCloud-account van het slachtoffer om gegevens te verzamelen. Nadat de inloggegevens en het wachtwoord van het iCloud-account van het slachtoffer zijn ingegeven in de stalkerware app, wordt **alle data van de iCloud beschikbaar** gesteld aan de dader. Deze data omvat onder andere[24]:

- Contactgegevens
- Foto's
- Kalender
- Notities
- Geolocatie
- Documenten opgeslagen in de iCloud

Om toch gebruik te kunnen maken van de vele mogelijkheden die Android-stalkerware biedt, kan het gesloten systeem van iOS-toestellen omzeild worden door zulke toestellen te ***jailbreaken***. Hierdoor kan software en applicaties die niet ondersteund worden door Apple, dus ook stalkerware, toch op het toestel

---

[22] Norton Labs. (2021, 24 juni). *A year after lockdown: stalkerware on the rise.* Geraadpleegd van https://www.nortonlifelock.com/blogs/norton-labs/stalkerware-rise, Davidovic, I. (2021, 3 december). How to spot the software that could be spying on you. *BBC News.* Geraadpleegd van https://www.bbc.com/news/business-59390778; Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html; Kaspersky. (2022). *The state of stalkerware in 2022.* Geraadpleegd van https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/04/12075509/EN_The-State-of-Stalkerware-2021.pdf

[22] Norton Labs. (2021, 24 juni). *A year after lockdown: stalkerware on the rise.* Geraadpleegd van https://www.nortonlifelock.com/blogs/norton-labs/stalkerware-rise

[23] Khoo, C., Robertson, K., & Deibert, R. (2019). *Installing fear: A Canadian legal and policy analysis of using, developing, and selling smartphone spyware and stalkerware applications.* The Citizen Lab. Geraadpleegd van https://www.citizenlab.ca/docs/stalkerware-legal.pdf; Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The predator in your pocker: A multidisciplinary assessment of the stalkerware application industry.* The Citizen Lab. Geraadpleegd van https://citizenlab.ca/docs/stalkerware-holistic.pdf

[24] Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The predator in your pocker: A multidisciplinary assessment of the stalkerware application industry.* The Citizen Lab. Geraadpleegd van https://citizenlab.ca/docs/stalkerware-holistic.pdf

geïnstalleerd worden. Fysieke toegang is nog steeds noodzakelijk om een *jailbreak* uit te voeren en vergt meer inspanning en technologische kennis van de dader. Voldoende informatie is echter zonder problemen terug te vinden op het internet.[25]

2. Psychologische impact op het slachtoffer

Doordat het fenomeen stalkerware bij het grote publiek nog erg onbekend is en de moeizame detectie ervan, zijn **slachtoffers** zich er **vaak niet van bewust** dat ze via hun smartphone, tablet of computer door een (ex-)partner in de gaten worden gehouden. Toch kan het voorkomen dat slachtoffers een **vermoeden** hebben. Zo ondervindt het slachtoffer bijvoorbeeld dat de (ex-)partner op ieder moment weet heeft van de locatie van het slachtoffer, met wie het slachtoffer een interactie heeft gehad of over informatie beschikt uit berichten die naar een andere persoon dan de dader verzonden zijn.[26]

Net zoals fysieke stalking heeft **stalking gefaciliteerd door stalkerware** een enorme psychologische impact op het slachtoffer. Door *gaslighting* en de dwingende controle die de dader uitoefent, leven slachtoffers in een **constante staat van angst**. Het voelt alsof ze niet kunnen ontsnappen aan de dader. Dit heeft **een isolerende werking** op hen. Doordat ze zichzelf en hun eigen waarnemingen niet meer vertrouwen, **vermijden** slachtoffers het **contact met hun sociaal netwerk.**[27] Ook de vrees om hun familie en vrienden te betrekken bij de situatie van (ex-)partnergeweld, kan ervoor zorgen dat slachtoffers contact met hen zullen vermijden. Daarnaast zullen slachtoffers ook een **hoge drempel** ervaren om **contact** te zoeken met **hulporganisaties**, vaak uit vrees dat de dader op de hoogte zou zijn en de situatie verder zou escaleren.[28]

Meer specifiek in het kader van stalkerware, zullen slachtoffers **smartphone-, tablet- of computergebruik beperken of** zelfs helemaal **vermijden**. Hierdoor zijn slachtoffers niet alleen minder bereikbaar voor hun sociaal netwerk, maar ook hulp inschakelen bij eventueel gevaar kan dan minder snel gebeuren.[29]

3. Slachtofferschap: cijfers

3.1. Prevalentie algemeen slachtofferschap stalkerware[30]

In België worden er geen officiële cijfers bijgehouden over het aantal slachtoffers van stalkerware. Voor cijfergegevens moet daarom te rade worden gegaan bij antivirusbedrijven. Aangezien deze cijfers afhankelijk zijn van het klantenbestand van de bedrijven, de gehanteerde definitie van stalkerware en

---

[25] Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). *The predator in your pocker: A multidisciplinary assessment of the stalkerware application industry.* The Citizen Lab. Geraadpleegd van https://citizenlab.ca/docs/stalkerware-holistic.pdf; SecureMac. (2021, 13 oktober). *How to check for stalkerware on an iPhone.* Geraadpleegd van https://www.securemac.com/news/how-to-check-for-stalkerware-on-an-iphone

[26] Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

[27] York Morris, S., & Raypole, C. (2022, 24 november). *How to recognize gaslighting and get help. https://www.healthline.com/health/gaslighting#:~:text=Gaslighting%20is%20a%20form%20of,they%20question%20their%20own%20sanity)*

[28] Woodlock, D., Bentley, K., Schulze, D., Mahoney, N., Chung, D., & Pracillio, A. (2020). *Second National Survey of Technology Abuse and Domestic Violence in Australia.* WESNET. Geraadpleegd op 22 februari 2022, van https://wesnet.org.au/wp-content/uploads/sites/3/2020/11/Wesnet-2020-2nd-National-Survey-Report-72pp-A4-FINAL.pdf

[29] Woodlock, D., Bentley, K., Schulze, D., Mahoney, N., Chung, D., & Pracillio, A. (2020). *Second National Survey of Technology Abuse and Domestic Violence in Australia.* WESNET. Geraadpleegd op 22 februari 2022, van https://wesnet.org.au/wp-content/uploads/sites/3/2020/11/Wesnet-2020-2nd-National-Survey-Report-72pp-A4-FINAL.pdf

[30] Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

de al dan niet rapportering ervan door klanten, variëren ze sterk. ESET noteert 'honderden gevallen per jaar' en ook Kaspersky zag 180 stalkerware-infecties op Belgische smartphones in 2020. België stond daarmee zelf op plaats 9 in Kaspersky's top 10 Europese landen meest getroffen door stalkerware in 2020.[31] Ook in 2021 staat België nog steeds op plaats 9, al is het aantal wel gedaald naar 94 stalkerware-infecties.[32] Bij Bitdefender liggen de cijfers wat hoger, met 551 gevallen van stalkerware-infecties in 2021 in België. Norton zag een nog hoger cijfer dan Bitdefender: tussen 19 mei 2021 en 21 januari 2022 waren er 12.472 stalkerwaredetecties op 8.168 Belgische toestellen. Een mogelijke verklaring voor deze aanzienlijk hogere cijfers van Norton is te wijten aan de definitie die ze gebruiken. Ook legitieme software en apps die kunnen gebruikt worden om iemand in de gaten te houden zonder diens toestemming, worden meegerekend. Toch zijn deze cijfers pas het topje van de ijsberg en zullen de werkelijke cijfers in de praktijk nog veel hoger liggen. Heel wat Belgen hebben dan wel een antivirussoftware op hun computer geïnstalleerd, op smartphones en tablets is dit helemaal niet ingeburgerd.[33] The Coalition Against Stalkerware schat dan ook dat er wereldwijd bijna 1 miljoen personen per jaar slachtoffer worden van stalkerware.[34]

3.2. Prevalentie slachtoffers van stalkerware in het kader van (ex-)partnergeweld

Om een indicatie te krijgen van de omvang van de problematiek omtrent stalkerware in situaties van (ex-)partnergeweld moet beroep worden gedaan op buitenlandse studies.

In de tweede **National Survey on Technology Abuse and Domestic Violence in Australia** van **2020** rapporteerden 99,3% van de ondervraagde professionals dat zij cliënten hebben die al geconfronteerd werden met technologie-gefaciliteerde stalking, waaronder ook het gebruik van stalkerware. Bij de vraag naar het gebruik van GPS-tracking apps door de dader, gaf 16,2% van de professionals aan dit 'altijd' te zien en 45,6% 'vaak'. Monitoring via iCloud zagen 42,2% van de professionals 'vaak' door een dader van (ex-)partnergeweld gebruikt worden.[35]

Ook in **Frankrijk** werd al onderzoek gedaan naar cybergeweld tussen (ex-)partners. In een onderzoek van het **Centrum Hubertine Auclert** van **2018** gaf 64% van de respondenten, vrouwelijke slachtoffers van (ex-)partnergeweld, aan dat ze al een vorm van digitale monitoring hebben meegemaakt. 21% van de respondenten werd al in de gaten gehouden in het bijzonder door stalkerware. Door de al eerder aangehaalde moeilijke detectie van stalkerware, werd in het onderzoek ook gevraagd naar het 'vermoeden van toezicht door de dader' bij de respondenten. 64% van de respondenten gaf aan te denken dat hun (ex-)partner van op afstand toegang had gehad tot hun telefoon, accounts of mail, terwijl 19% denkt al gevolgd geweest te zijn via GPS. Bij 44% van de respondenten gaf het slachtoffer aan dat hun (ex-)partner wist waar ze zich bevonden, zonder daarover met hem eerst gesproken te hebben.[36]

---

[31] Kaspersky. (2021). *The state of stalkerware in 2020.* Geraadpleegd op 22 februari 2022, van https://securelist.com/the-state-of-stalkerware-in-2020/100875/

[32] Kaspersky. (2022). *The state of stalkerware in 2021.* Geraadpleegd van https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/04/12075509/EN_The-State-of-Stalkerware-2021.pdf

[33] Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

[34] Kaspersky. (2022). *The state of stalkerware in 2021.* Geraadpleegd van https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/04/12075509/EN_The-State-of-Stalkerware-2021.pdf

[35]Woodlock, D., Bentley, K., Schulze, D., Mahoney, N., Chung, D., & Pracillio, A. (2020). *Second National Survey of Technology Abuse and Domestic Violence in Australia.* WESNET. Geraadpleegd van https://wesnet.org.au/wp-content/uploads/sites/3/2020/11/Wesnet-2020-2nd-National-Survey-Report-72pp-A4-FINAL.pdf

[36] Centre Hubertine Auclert. (2018). *Cyberviolences conjugales: recherche-action menée auprès de femmes victimes de violences conjugales et des professionnel-le-s les accompagnant* [Rapport]. Geraadpleegd van https://www.centre-hubertine-auclert.fr/sites/default/files/documents/rapport_cyberviolences_conjugales_web.pdf

4. Technische mogelijkheden tot preventie, herkennen en verwijderen van stalkerware

4.1. Preventie van stalkerware

Zoals al eerder vermeld, is fysieke toegang een noodzakelijke voorwaarde bij de installatie van stalkerware. Je **toestel niet onbewaakt achterlaten of door iemand laten gebruiken en een goede beveiliging** vormen al een eerste drempel voor potentiële daders. Maak daarbij bijvoorbeeld geen gebruik van face-ID of vingerafdruk voor het ontgrendelen van een toestel, maar wel van een **sterk wachtwoord**.[38] De dader kan het ontgrendelen van het toestel via face-ID of vingerafdruk bijvoorbeeld omzeilen wanneer het slachtoffer slaapt. Volgens SafeOnWeb wordt best gekozen voor een lang wachtwoord dat minstens 13 karakters bevat en waarbij gebruik wordt gemaakt van cijfers, hoofdletters en symbolen. Aangezien wordt aangeraden om niet steeds hetzelfde wachtwoord te gebruiken voor verschillende accounts en het onthouden van meerdere sterke wachtwoorden niet vanzelfsprekend is, raadt SafeOnWeb ook het gebruik van **wachtwoordkluizen** aan. Omdat zo'n wachtwoordkluis alle wachtwoorden veilig bijhoudt, is het enkel nodig om het sterke wachtwoord dat toegang geeft tot de kluis te onthouden.[39]

Maar een sterk wachtwoord alleen is niet voldoende indien iemand kennis heeft van dat wachtwoord. Er wordt dan ook aangeraden om **wachtwoorden niet door te geven aan derden**[40]. In de praktijk worden wachtwoorden echter vaak gedeeld met partners. Uit een onderzoek van Kaspersky naar cyberstalking in relaties, met 21.055 deelnemers uit 21 landen, gaf 57% van de respondenten aan het wachtwoord van hun gsm gedeeld te hebben met hun partner. Een gelijkaardig percentage (56%) gaf aan weet te hebben van het wachtwoord van hun partners gsm. Bovendien vond ook 2 op 5 respondenten het normaal om de inloggegevens van hun iCloud- of Google-account te delen met hun familie.[41] En indien wachtwoorden niet vrijwillig gedeeld worden, kan in situaties van (ex-)partnergeweld een slachtoffer (subtiel) gedwongen worden om ze te delen.

Niet enkel de toegang tot het toestel kan bemoeilijkt worden, ook de installatie van stalkerware zelf. **Android** toestellen kunnen via de instellingen de **installatie van third-party apps blokkeren**.[42] Dit zal dus enkel doeltreffend zijn tegen stalkerware wanneer de software of app niet via de Google Play Store verkregen en gedownload is. Ook is het mogelijk dat een dader die kennis heeft van deze mogelijkheid, de optie gewoon terug deblokkeert.

Tenslotte wordt ook aangeraden om een **antivirusprogramma** te installeren en dit op ieder toestel. Een antivirusprogramma kan namelijk stalkerware-programma's herkennen en indien nodig ook verwijderen.[43]

4.2. Herkennen van stalkerware

Aangezien stalkerware developers er alles aan doen om hun software te verbergen op een geïnfecteerd toestel, is het niet gemakkelijk om de signalen van een stalkerware infectie te herkennen. Al zeker niet wanneer je als gebruiker niet weet waar je precies naar op zoek moet. Er zijn echter wel enkele signalen

---

[38] Coalition Against Stalkerware. (2022, 20 mei). *What is stalkerware?* [Video]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0;

[39] SafeOnWeb.be. (z.d.). Gebruik lange wachtwoorden. Geraadpleegd van https://www.safeonweb.be/nl/gebruik-lange-wachtwoorden

[40] Coalition Against Stalkerware. (2022, 20 mei). *What is stalkerware?* [Video]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0

[41] Kaspersky. (2021). *Digital stalking in relationships.* Geraadpleegd van https://media.kasperskydaily.com/wp-content/uploads/sites/86/2021/11/17164103/Kaspersky_Digital-stalking-in-relationships_Report_FINAL.pdf

[42] Coalition Against Stalkerware. (2022, 20 mei). *What is stalkerware ?* [Video]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0

[43] Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

die kunnen duiden op een mogelijke stalkerware-infectie. Ten eerste kan, zoals al eerder aangehaald, de **dader** zelf een eerste indicatie geven door **kennis** te hebben **van informatie** die hij of zij **onmogelijk zou kunnen weten**.[44] Ten tweede wordt niet alle stalkerware rechtstreeks vanuit app stores geïnstalleerd. De dader zal dan ook naar bepaalde sites moeten surfen voor informatie over stalkerware en hoe dit te installeren op een toestel. Het is daarom ook nuttig om bij vermoedens de **internetgeschiedenis van het toestel na te kijken**. Het is belangrijk in het achterhoofd te houden dat de afwezigheid van dergelijke sites in de internetgeschiedenis niet wil zeggen dat stalkerware niet aanwezig is op het toestel. Het is namelijk heel makkelijk om de internetgeschiedenis te wissen. Tenslotte zijn er ook signalen die op het besmette toestel zelf van toepassing zijn. Zo zal de gebruiker ervaren dat het **toestel 'vreemd doet'**. De batterij loopt bijvoorbeeld heel snel leeg, het toestel voelt heel warm aan op momenten dat het niet intensief gebruikt wordt of het toestel start zichzelf ad random opnieuw op.[45] Daarom wordt aanbevolen om frequent de **geïnstalleerde software of apps en diens machtigingen na te kijken** op het toestel. Vooral apps waarvan de gebruiker weet dat hij of zij die niet geïnstalleerd heeft en die zij of hij niet herkent, maar die toch toegang hebben tot verschillende sensoren van het toestel[46], zijn een signaal voor een potentieel met stalkerware geïnfecteerd toestel.[47]

Specifiek voor iOS-toestellen zijn de aanwezigheid van de **apps Cydia of Sileo** een indicatie. Beide apps worden namelijk het meeste gebruikt om een iOS-toestellen te *jailbreaken*.[48]

4.3. Verwijderen van stalkerware

Niet alle stalkerware laat zich even gemakkelijk verwijderen. Veelal wordt aangeraden om met een **antivirusprogramma** een scan uit te voeren op het toestel om stalkerware te detecteren en zo te verwijderen. Daarna kan het toestel opnieuw gescand worden om te controleren of de stalkerware weldegelijk is weggehaald. Indien dit niet het geval is, kan men nog steeds terugvallen op een harde reset, namelijk de **fabrieksinstellingen** van het toestel **herstellen**.[49]

Veel online adviezen raden aan om zo snel mogelijk stalkerware van het toestel te verwijderen. In situaties van (ex-)partnergeweld is enige voorzichtigheid echter aangewezen. Sommige stalkerware sturen een notificatie naar de dader dat de app opgemerkt of verwijderd is. Dit kan zorgen voor een **escalatie** van de situatie van partnergeweld.[50] Bovendien resulteert het verwijderen van de betreffende software of app ook in het **verwijderen van het bewijsmateriaal**.[51]

---

[44] Clerix, K. (2022, 2 februari). *"In België zijn er duizenden mensen die met stalkerware bespioneerd worden"/Interviewer S. Lemaire.* De wereld van Sofie. Geraadpleegd op18 februari 2022, van https://radio1.be/luister/select/nieuwe-feiten/in-belgie-zijn-er-duizenden-mensen-die-met-stalkerware-bespioneerd-worden

[45] Clerix, K. (2022, 2 februari). *"In België zijn er duizenden mensen die met stalkerware bespioneerd worden"/Interviewer S. Lemaire.* De wereld van Sofie. Geraadpleegd op18 februari 2022, van https://radio1.be/luister/select/nieuwe-feiten/in-belgie-zijn-er-duizenden-mensen-die-met-stalkerware-bespioneerd-worden; Coalition Against Stalkerware. (2022, 20 mei). *What is stalkerware?* [Video]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0

[46] Voorbeelden van dergelijke sensoren zijn de camera, geluid, *touch screen* enz.

[47] Coalition Against Stalkerware. (2022, 20 mei). *What is stalkerware ?* [Video]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0

[48] SecureMac. (2021). *How to check for stalkerware on an iPhone.* Geraadpleegd van https://www.securemac.com/news/how-to-check-for-stalkerware-on-an-iphone

[49] Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

[50] Coalition Against Stalkerware. (2022, 20 mei). *What is stalkerware ?* [Video]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0

[51] Clerix, K. (2022, 2 februari). *Je partner bespioneren via de gsm? Kinderlijk eenvoudig (en illegaal).* Knack. Geraadpleegd van https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html; Coalition Against Stalkerware. (2022, 20 mei). *What is stalkerware ?* [Video]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0

5. Good practices uit het Buitenland

5.1. Wetgevende initiatieven

Met de wet nr. 2020-936 van 30 juli 2020 geeft **Frankrijk** een duidelijk signaal dat het heimelijk en zonder toestemming in de gaten houden van een persoon via geolocatie niet getolereerd wordt. *"Het vastleggen, opnemen of doorgeven, op welke manier dan ook, van de werkelijke of vertraagde plaats in de tijd van een persoon zonder diens toestemming"* is strafbaar. Bovendien wordt er extra aandacht besteed aan de kwetsbare situatie van slachtoffers van (ex-)partnergeweld waarbij een (ex-)partner hun locatie in de gaten houdt. In dergelijke gevallen zijn er hogere gevangenisstraffen van toepassing.[52]

Ook **Duitsland** heeft stappen ondernomen in het kader van cyberstalking in het algemeen en cybersurveillance in het bijzonder. Sinds 1 oktober 2021 staat stalking via een computerprogramma met als doel een andere te bespioneren in de Duitse strafwet als onderdeel van de rubriek 'stalking'.[53]

5.2. Association de lutte contre l'utilisation de la technologie dans les violences faites aux femmes (ECHAP) & Clinic to End Tech Abuse (CETA) – Handleidingen

ECHAP is een feministisch hackerscollectief uit Frankrijk dat zich inzet in de strijd tegen technologisch geweld tegen vrouwen. Ze geven workshops aan professionals die werken met vrouwelijke slachtoffers van geweld en bieden aan de slachtoffers zelf technische ondersteuning indien gewenst. Ook schrijven ze **handleidingen voor slachtoffers van (ex-)partnergeweld** waarbij de dader misbruik maakt van technologie.[54] Zo stellen ze op hun site algemene gidsen ter beschikking over wachtwoordstrategieën en hoe een slachtoffer na een relatie zich digitaal kan loskoppelen van een ex-partner. Daarnaast hebben ze ook specifiekere gidsen die betrekking hebben op online accountbeveiliging of IT-apparaatbeveiliging, waaronder het herkennen van de signalen van stalkerware op een smartphone. [55]

Ook **CETA** (VS) beschikt over stap-voor-stap handleidingen voor slachtoffers van (ex-)partnergeweld. Net zoals ECHAP zijn er zowel algemene als meer specifieke gidsen. Daarnaast zijn er ook gidsen die specifiek voor verschillende (sociale media) accounts oplijsten hoe een slachtoffer de instellingen van een account kan aanpassen om voor extra beveiliging te zorgen.[56]

Wat de handleidingen van beide organisaties een *good practice* maakt is dat ze **gemakkelijk te gebruiken** zijn, **ongeacht iemands technologische kennis**. Bovendien hebben beide organisaties in hun handleidingen **specifiek aandacht voor de bijzondere situatie** waarin slachtoffers van **(ex-)partnergeweld** gefaciliteerd door technologie zich bevinden. Zo wordt meermaals in de handleidingen de lezer op het hart gedrukt dat het veranderen van bijvoorbeeld wachtwoorden of het ontzeggen van de toegang tot een bepaald account kan resulteren in een gedragsverandering bij de dader en zelfs kan leiden tot escalatie van de situatie. Bovendien wordt slachtoffers aangeraden om een **veiligheidsplan op te stellen, alvorens** over te gaan tot het **verwijderen van stalkerware of het veranderen van wachtwoorden**.

---

[52] LOI n° 2020-936 du 30 julliet 2020 visant à protéger les victimes de violences conjugales (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042176652)

[53] Gezets zur Änderung des Strafgesetsbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings sowie Verbesserung des strafrechtlichen Schutzes gegen Zwangsprostitution. Geraadpleegd van https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Bgbl_Cyberstalking.pdf;jsessionid=876E15DAD59AA3AE0027036B966708EC.2_cid324?__blob=publicationFile&v=2

[54] ECHAP. (z.d.). *Association de lutte contre l'utilisation de la technologie dans les violences faites aux femmes.* Geraadpleegd van https://echap.eu.org/

[55] ECHAP. (z.d.). *Nos guides*. Geraadpleegd van https://echap.eu.org/ressources/

[56] CETA. (z.d.). *Resources.* Geraadpleegd van https://www.ceta.tech.cornell.edu/resources

III. Aanbevelingen

Op basis van bovenstaande informatie, wetenschappelijk onderzoek en de aanbevelingen van GREVIO[57] en de Europese Commissie[58], worden in dit advies een aantal concrete aanbevelingen geformuleerd.

1. Nood aan prevalentieonderzoek

Zoals in dit advies wordt geïllustreerd, is er een tekort aan Belgische cijfers omtrent slachtoffers van stalkerware in het algemeen en in het bijzonder over slachtoffers van (ex-)partnergeweld die geconfronteerd worden met stalkerware. Momenteel tast men in het duister over de omvang van deze problematiek in ~~de~~ België.

2. Nood aan sensibilisering

2.1. Algemene sensibilisering

Aangezien stalkerware een relatief 'recent' fenomeen betreft, is er nood aan sensibilisering van de **algemene bevolking**.

2.2. Sensibilisering van slachtoffers

Daarnaast moeten ook **(potentiële) slachtoffers van (ex-)partnergeweld** gesensibiliseerd worden. Doordat stalkerware software en apps vaak verborgen zijn en er alles aan doen om dit zo te houden, is het noodzakelijk dat (potentiële) slachtoffers weet hebben van het bestaan van stalkerware en weten wat de signalen zijn die kunnen wijzen op een met stalkerware geïnfecteerd toestel. Het is bovendien ook belangrijk dat (potentiële) slachtoffers weten waar ze terecht kunnen voor hulp.

Slachtoffers van (ex-)partnergeweld dienen concrete informatie ter beschikking te krijgen over wat stalkerware is, wat de mogelijke signalen van een geïnfecteerd toestel zijn en welke stappen een slachtoffer zelf kan ondernemen om hun leven, zowel offline als online, terug in handen te nemen en eventueel klacht in te dienen. Deze aanbeveling kan bijvoorbeeld gerealiseerd worden door de ontwikkeling van een handleiding waarin stap-voor-stap wordt uitgelegd wat een slachtoffer kan doen indien hij of zij vermoeden of kennis heeft van stalkerware die op zijn of haar toestel werd geïnstalleerd. Ook hier moet de veiligheid van het slachtoffer centraal staan. Alle risico's omtrent het detecteren of verwijderen van stalkerware moeten opgelijst worden alsook de aanbeveling om eerst een veiligheidsplan op te stellen alvorens over te gaan tot handelen. Verder moet ook duidelijk gemaakt worden dat het verwijderen van stalkerware tot gevolg heeft dat het bewijsmateriaal verloren gaat.

2.3. Sensibilisering van professionals

Ook bij **politie en justitie** ontbreekt nog vaak kennis van stalkerware. Dit komt niet alleen door de relatieve onbekendheid van het fenomeen maar ook door de gespecialiseerde materie. Daarom dient de sensibilisering van de relevante praktijkactoren niet alleen duidelijk te maken wat stalkerware precies is, maar ook dat het een vorm van (ex-)partnergeweld betreft en dus als bewijs in zaken van (ex-)partnergeweld dient beschouwd te worden. Vanaf de aanmelding van dossiers omtrent (ex-)partnergeweld moet dus aandacht besteed worden aan digitale vormen van geweld, zoals de installatie van stalkerware, ongeacht of het slachtoffer daar zelf bij aanmelding een indicatie van geeft. Ook moet

[57] GREVIO. (2021). *General recommendation no. 1: On the digital dimension of violence against women.* Adopted on October 20, 2021). Geraadpleegd van https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

[58] European Commission. (2022). *Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence* [2022/0066 (COD)]. Geraadpleegd van https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/com_2022_105_1_en.pdf

rekening gehouden worden met het feit dat niet alleen een toestel van het slachtoffer stalkerware kan bevatten, maar ook die van het gezamenlijk kind, zeker bij echtscheidingen. Bovendien mogen digitale vormen van geweld niet geminimaliseerd worden. Wetenschappelijk onderzoek, zoals eerder ook aangegeven in dit advies, illustreert duidelijk dat het een mythe is dat digitaal geweld een minder zware impact heeft op het slachtoffer.

Doorheen het hele proces dat bij politie en justitie doorlopen wordt, moet de veiligheid van het slachtoffer centraal staan. Dit houdt voornamelijk in dat het slachtoffer geïnformeerd wordt over de gevaren die de detectie van stalkerware in het kader van de bewijsverzameling met zich mee kan brengen. Sommige types van stalkerware sturen namelijk een notificatie naar de dader met de boodschap dat de app opgemerkt of verwijderd is. Dit kan resulteren in een escalatie van het geweld.

Een **aanpassing van de COL 4/2006** met specifieke aandacht voor digitale vormen van (ex-)partnergeweld dringt zich dan ook op.

Net zoals bij politie en justitie moet ook in de **hulpverleningssector** aandacht besteed worden aan digitale vormen van (ex-)partnergeweld, waar de installatie van stalkerware één voorbeeld van is. Al vanaf de aanmelding van het slachtoffer bij een hulporganisatie dient er gepolst te worden naar digitale veiligheid. Is er sprake van gedeelde accounts? Heeft de dader toegang gehad tot een toestel dat nu 'vreemd' doet? Ook hier moet de veiligheid van het slachtoffer centraal staan. Hulpverleners moeten geïnformeerd worden over hoe precies een veiligheidsplan moet opgesteld worden waarbij rekening wordt gehouden met de digitale dimensie van (ex-)partnergeweld. Vervolgens kunnen hulpverleners ook slachtoffers tips en tools aanreiken omtrent veiligheid online.

Naast politie, justitie en de hulpverleningssector kan ook de **IT-sector** baat hebben bij informatie over het gebruik van stalkerware in het kader van (ex-)partnergeweld. Er bestaat namelijk een reële kans dat slachtoffers van partnergeweld bij hen aankloppen in verband met een toestel dat 'vreemd doet' of met het vermoeden dat een (ex-)partner hen via het toestel in de gaten houdt.

Een praktische uitwerking omtrent de sensibilisering gericht op de IT-sector is bijvoorbeeld een brochure waarin uitgelegd wordt wat (ex-)partnergeweld is, hoe technologie zoals stalkerware door een dader gebruikt kan worden om het slachtoffer in de gaten en onder controle te houden en hoe dergelijke slachtoffers het beste ondersteund kunnen worden. De veiligheid van het slachtoffer dient in de brochure centraal te staan. Er dient bijvoorbeeld uitdrukkelijk vermeld te worden dat niet tot acties mag overgegaan worden, zoals het verwijderen van de stalkerware, zonder kennisgeving van de risico's die daaraan verbonden zijn en zonder de uitdrukkelijke toestemming van het slachtoffer. Tenslotte bevat de brochure idealiter ook een lijst van organisaties waarnaar slachtoffers doorverwijzen kunnen worden voor verdere hulp of eventuele aangifte.

3. Bijzondere aandacht voor vluchthuizen en stalkerware

Wanneer een slachtoffer van (ex-)partnergeweld zich niet meer veilig voelt thuis of niet langer thuis kan verblijven, kan zij of hij terecht bij een vluchthuis. Het is uitermate belangrijk voor de werking van het vluchthuis en voor de veiligheid van het slachtoffer dat het adres geheim blijft voor de dader. Een door de dader van (ex-)partnergeweld met stalkerware geïnfecteerd toestel brengt dit echter in gevaar. Het is dan ook belangrijk dat een samenwerking wordt gerealiseerd tussen IT-experten en vluchthuizen om het gevaar verbonden aan stalkerware in de context van (ex-)partnergeweld zoveel mogelijk te beperken. Zo zou bij iedere aanmelding, ongeacht of er een vermoeden is dat een toestel van het slachtoffer stalkerware bevat, elk toestel van het slachtoffer nagekeken moeten worden door een IT-expert om de geheime locatie van het vluchthuis te vrijwaren. Om logische redenen gebeurt dit nazicht best alvorens het slachtoffer aankomt in het vluchthuis. Zoals al eerder aangehaald is de samenwerking tussen IT-experten en vluchthuizen ook nuttig in het kader van potentiële bewijsverzameling.

4. Wijziging strafwetboek: uitbreiding van het begrip 'stalking' (art. 442bis Sw.)

Het gebruik van stalkerware kan momenteel onder twee strafbepalingen vallen. Vooreerst voorziet het misdrijf belaging in art. 442bis van het Strafwetboek een gevangenisstraf voor personen die de rust van een persoon ernstig verstoord hebben. Belaging vergt geen bijzonder opzet om te schaden. Er is ook geen vereiste dat de stalking fysiek van aard moet zijn en kan dus ook gebeuren via het gebruik van technologische middelen (zoals een smartphone) of het internet. Belaging veronderstelt wel een niet-aflatende of steeds terugkerende gedraging. Het Hof van Cassatie heeft echter ook aanvaard dat één enkele gedraging die voortdurende gevolgen teweegbrengt waardoor iemands persoonlijke levenssfeer wordt aangetast, het misdrijf belaging kan opleveren.[59] Deze rechtspraak werd met veel kritiek door de rechtsleer onthaald.[60] De discussie omtrent het bestaan van een vereiste van meerdere handelingen lijkt daarmee mogelijks nog niet finaal beslecht te zijn.

Belaging met gebruik van stalkerware zal in de meeste gevallen ook bestraft kunnen worden onder het misdrijf van elektronische belaging (art. 145 §3bis van de wet elektronische communicatie), namelijk het gebruik van een elektronisch communicatienetwerk of communicatiemiddel met als doel overlast te bezorgen aan de correspondent of schade te berokkenen. Hierbij volstaat een eenmalige gedraging voor de strafbaarheid. Helaas heeft dit misdrijf wel enkele limieten. Zo dient in hoofde van de belager sprake te zijn van een bijzonder opzet, namelijk de wil om overlast of schade te veroorzaken. Bovendien geldt in tegenstelling tot 'gewone' belaging, de strafverzwaring wegens haat-gerelateerde drijfveren (zoals art. 442ter Sw.) niet voor artikel 145, §3bis WEC.

Een recente richtlijn van de Europese Commissie ijvert voor een uitbreiding van het misdrijf 'stalking'. Zo zou het ook de continue monitoring van een derde, zonder diens toestemming of medeweten, door middel van technologie- en of communicatietechnologieën moeten omvatten. Voorbeelden hiervan zijn de monitoring van de geolocatie via de installatie van stalkerware of het in gaten houden van (sociale media) accounts van het slachtoffer door het stelen van hun wachtwoorden.

De twee voornoemde strafbepalingen hebben een onzekere invulling. Een wettelijke verduidelijking dat het gebruik van stalkerware neerkomt op (elektronische) belaging dringt zich dan ook op.

[59] Cass. 29 oktober 2013, P.13.1270.N, Arr.Cass. 2013, nr. 563.
[60] D. VOORHOOF, "Recente rechtspraak belaagt expressievrijheid op het internet", *Juristenkrant* 2013, 3, 278

! Belangrijke aandachtspunten omtrent stalkerware voor <u>alle</u> stakeholders !

- Stalkerware is een vorm van (ex-)partnergeweld.
- Vanaf de aanmelding van het slachtoffer aandacht hebben voor digitale vormen van geweld, ongeacht of het slachtoffer dit zelf aanbrengt.
- Bij het verzamelen van bewijs in het kader van stalkerware moeten niet alleen de toestellen van het slachtoffer onder de loep genomen worden, maar ook die van gezamenlijk(e) kind(eren), en dit zeker bij echtscheidingen.
- De veiligheid van het slachtoffer staat te allen tijde centraal; alvorens over te gaan tot actie dient een veiligheidsplan opgesteld te worden.
- Het slachtoffer dient steeds geïnformeerd te worden over de mogelijke gevaren die de detectie en verwijdering van stalkerware met zich meebrengen en het slachtoffer dient bijgestaan te worden bij de verdere stappen ten gevolge van het ontdekken van stalkerware.