Recommandation

de l'Institut pour l'égalité des femmes et des hommes n° 2022/R/002

relatif à l'utilisation de stalkerwares dans le cadre de violences entre (ex)partenaires.

INSTITUT
POUR L'ÉGALITÉ
DES FEMMES
ET DES HOMMES

I. Compétence de l'Institut pour l'égalité des femmes et des hommes

Créé par la loi du 16 décembre 2002, l'Institut pour l'égalité des femmes et des hommes a entre autres pour mission de veiller au respect de la législation en matière d'égalité entre les femmes et les hommes et de combattre toute forme de discrimination et d'inégalité fondées sur le sexe.

II. Contexte de la recommandation

Le développement rapide de technologies de l'information et de la communication offre des possibilités nouvelles et supplémentaires aux auteur-e-s. Selon le GREVIO, cette dimension numérique de la violence est toutefois insuffisamment prise en compte. Il en va de même pour le **stalkerware**, une forme extrêmement inquiétante de violence entre (ex-)partenaires qui reste néanmoins encore relativement méconnue en Belgique.[1]

Le GREVIO stipule notamment dans sa *General Recommendation Nr 1 on the digital dimension of violence against women* que *« 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. »*[2]

1. Qu'est-ce qu'un stalkerware ?

Les stalkerwares (logiciels de harcèlement) comprennent tous les **logiciels disponibles dans le commerce**, souvent sous la forme d'une **application**, permettant à un tiers de surveiller/utiliser **à distance** l'appareil (**smartphone, tablette ou ordinateur**) **et l'activité** d'une personne sans le **consentement** de la personne en question. De plus, l'espionnage des appareils d'autres personnes se fait **à leur insu**. Une fois le logiciel installé sur l'appareil, l'utilisateur-rice ne reçoit aucune notification indiquant que son activité est surveillée ou manipulée par quelqu'un d'autre. Outre le terme « stalkerware », les termes « **creepware** » ou « **spouseware** » sont également utilisés pour décrire ces logiciels.[3]

1.1. Aspects technologiques

Contrairement au phénomène général des « spywares », il est nécessaire d'**accéder physiquement** à l'appareil pour installer un stalkerware. Dans le cas des appareils iOS, il est également possible d'accéder à l'appareil par le biais du compte iCloud de la personne ciblée.[4] Si l'accès physique n'est pas

[1] L'Institut a participé le 10 mars 2022 à la conférence en ligne sur la violence numérique à l'égard des femmes. Cette conférence a été organisée par les « Fund Operators of the EEA Grants Active Citizens Fund in Greece and Cyprus », en coopération avec le Conseil de l'Europe et le ministre norvégien de la Justice. Au cours de la conférence, le Conseil de l'Europe a notamment expliqué la violence sexuelle numérique à l'égard des femmes et le GREVIO a commenté sa nouvelle recommandation sur la violence numérique. Cette conférence a également donné lieu à une présentation relative au stalkerware.

[2] GREVIO General Recommendation Nr 1 on the digital dimension of violence against women. 20 octobre 2021. Consulté sur https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147.

[3] Coalition Against Stalkerware. (s.d). *Information for tech companies.* Consulté sur https://stopstalkerware.org/information-for-tech-companies

[4] Clerix, K. (2022, 2 février). *Je partner bespioneren via de gsm ? Kinderlijk eenvoudig (en illegaal).* Knack. Consulté sur le site https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

possible, l'auteur-e peut choisir de donner un appareil en cadeau à la victime sur lequel un stalkerware a déjà été installé.[5] Il existe même des entreprises spécialisées dans ce domaine. Elles installent le stalkerware sur un nouvel appareil au choix et, si souhaité, le livrent même directement à la victime. Une attention particulière est également accordée à l'emballage. Étant donné que le même emballage est utilisé que celui d'origine, rien n'indique que l'emballage a déjà été ouvert et qu'un tel logiciel a été installé sur l'appareil.[6]

Les stalkerwares sont **facilement disponibles dans le commerce**. En quelques clics, on trouve sur Internet (ordinaire) un large éventail de logiciels et d'applications faciles à installer sans connaissances technologiques spécifiques.[7] On peut même les retrouver dans le Google Play Store (Android) et l'Apple App Store (iOS). Certains sont gratuits, d'autres font l'objet d'un abonnement payant. Pour environ 20 à 30 euros par mois, il est possible de surveiller, sans problèmes, les activités numériques de quelqu'un.[8]

Afin d'échapper aux contrôles, les entreprises proposant des stalkerwares ont recours à l'**astuce de marketing** suivante : elles présentent leurs produits comme étant des **applications de sécurité ou antivol**. Elles ciblent également spécifiquement les parents qui veulent tenir leurs enfants à l'œil ou les employeur-se-s qui désirent surveiller leurs travailleur-se-s.[9] Les « app stores » tentent toutefois d'exclure les stalkerwares de leur offre. Dans le Google Play Store, par exemple, les applications qui traquent les utilisateur-rice-s et envoient des données à un autre appareil ne sont autorisées que si elles affichent constamment un message indiquant que la géolocalisation est en cours.[10] Certaines de ces applications passent néanmoins encore entre les mailles du filet.

Les logiciels ou applications stalkerware demeurent **cachés** pour l'utilisateur-rice. Ils fonctionnent en **stealth modus** (mode furtif), c'est-à-dire qu'il n'y a pas d'icônes, par exemple, pour indiquer à l'utilisateur-rice que ce logiciel est présent sur l'appareil, et encore moins qu'il fonctionne en arrière-plan et surveille ses activités.[11] S'ils ne sont pas cachés, **ils se font passer pour des applications légitimes**. Avec des noms comme « battery saver » (économiseur de batterie) ou « system services (services de système), ils n'éveillent souvent pas les soupçons.[12] En tant qu'utilisateur-rice, il est donc déjà nécessaire de savoir ce qu'est un stalkerware et quels sont les signaux qui indiquent la présence d'un stalkerware, pour pouvoir le détecter.

---

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

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

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

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

[9] Clerix, K. (2022, 2 février). *« In België zijn er duizenden mensen die met stalkerware bespioneerd worden »/Intervieweuse S. Lemaire.* De wereld van Sofie. Consulté sur le site https://radio1.be/luister/select/nieuwe-feiten/in-belgie-zijn-er-duizenden-mensen-die-met-stalkerware-bespioneerd-worden

[10] Google. (2020, 16 septembre). *Developer program policy: September 16, 2020 announcement.* Consulté sur https://support.google.com/googleplay/android-developer/answer/10065487

[11] Kaspersky. (2021). *The state of stalkerware in 2020.* Consulté le 22 février 2022 sur https://securelist.com/the-state-of-stalkerware-in-2020/100875/

[12] Davidovic, I. (2021, 3 décembre). 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 février). *Je partner bespioneren via de gsm ? Kinderlijk eenvoudig (en illegaal).* Knack. Consulté sur le site https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

1.2. Pourquoi les auteur-e-s de violences entre (ex-)partenaire utilisent-ils-elles des stalkerwares ?

Les smartphones, les tablettes et les ordinateurs sont tellement ancrés dans la société actuelle qu'il est impossible d'imaginer nos vies personnelles, sociales et professionnelles sans eux. Cette intégration est si complète que « *full access to a person's phone, is the next best thing to full access to a person's mind ».*[13] Il n'y a donc rien de surprenant au fait que les auteur-e-s de violences entre (ex)partenaire en fassent usage. Les stalkerwares ne fournissent pas seulement à ces auteur-e-s une mine d'informations sur les allées et venues de leur victime, mais leur permettent également **d'utiliser ces informations pour exercer un contrôle coercitif** (« coercive control ») sur leur victime ou pour l'intensifier.[14]

En dehors de cela, les informations obtenues peuvent aussi être utilisées à des fins de **gaslighting,** une technique de manipulation très subtile qui consiste à faire douter la victime de la véracité de ses propres paroles, pensées et souvenirs. Comme nous le verrons plus loin (infra 1.3), certains stalkerwares offrent la possibilité d'envoyer des textos au nom de la victime. Aucune trace n'est alors laissée sur l'appareil de la victime lui permettant de savoir qu'un texto a été envoyé. La victime peut alors commencer à douter d'elle-même : *« Ai-je peut-être quand même envoyé ce message ? »*. À long terme, cela induit une insécurité extrême et une perte de confiance en soi. [15]

Les auteur-e-s utilisent des stalkerwares aussi bien **pendant une relation qu'après une rupture ou un divorce**.[16] En outre, le-la (ex-)partenaire n'est pas le-la seul-e à être surveillé-e. Les multiples fonctionnalités de ces stalkerwares permettent également d'obtenir de nombreuses informations sur le-la (ex-)partenaire par le biais d'un appareil d'un **enfant** commun. [17]

Il est important de noter que dans le cas de violences entre (ex-)partenaires, il faut toujours tenir compte de l'ensemble du contexte dans lequel les violences ont lieu. Les formes numériques de violence ne sont pas isolées, mais **s'accompagnent souvent de** manifestations de violence dans le monde « physique », comme **la violence émotionnelle, verbale, psychologique, physique ou sexuelle**.[18] Des données de l'enquête européenne de la FRA (2014) sur les violences à l'égard des femmes font ainsi apparaître que 7 femmes sur 10 ayant subi une forme de cyberharcèlement ont également subi au moins une forme de violence physique et/ou sexuelle de la part d'un-e partenaire.[19]

---

[13] Gasperin, E. (2019, décembre). *What you need to know about stalkerware* [Vidéo]. Conférences Ted Consulté sur https://www.ted.com/talks/eva_galperin_what_you_need_to_know_about_stalkerware

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

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

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

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

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

[19] FRA (2014). *Violence against women : an EU-wide survey.* Rapport des résultats à consulter sur 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.* Consulté sur file:///C:/Users/ellen/Downloads/ti_pubpdf_mh0417543nln_pdfweb_20171026164003%20(2).pdf

1.3. Comment les stalkerwares sont-ils utilisés par les auteur-e-s de violences entre (ex)partenaires ?

Ce qu'un-e agresseur-e peut surveiller précisément dépend du type de logiciel et du système d'exploitation (Android ou iOS) pour lequel le stalkerware est développé. En général, les stalkerwares peuvent faire usage de **tous les capteurs** (son, caméra, *écran tactile*, etc.) d'un appareil. [20]

Les stalkerwares développés spécifiquement pour les **appareils Android** offrent aux auteur-e-s davantage de possibilités de surveiller leurs (ex-)partenaires. Les éléments suivants peuvent, entre autres, être contrôlés par les auteur-e-s[21] :

- Lieu
- Appels vocaux (écoute en situation réelle et enregistrements)
- Photos
- Recherches sur Internet par le biais de la saisie de frappe (*keystroke logging*)
- Messages sms
- Caméra (permet également de prendre des photos à distance)
- Son
- Activités sur d'autres applications telles que les « social media apps » (p. ex., Whatsapp) ou les « email apps ».

Outre la surveillance passive, l'auteur-e peut également utiliser des stalkerwares pour restreindre les fonctions de l'appareil infecté. Un-e auteur-e peut, entre autres[22] :

- Rejeter à distance les appels entrants
- Bloquer certains sites web
- Envoyer des messages au nom de la victime (SMS-spoofing), les messages envoyés étant cachés à la victime et ne pouvant être retrouvés dans l'historique des messages.

Les **stalkerwares iOS** ont généralement des capacités plus limitées. Le système plus « fermé » des appareils iOS rend également plus difficile l'installation de stalkerwares sur les iPhones. Les stalkerwares ciblant les appareils iOS utilisent donc principalement le compte iCloud de la victime pour collecter des données. Après avoir saisi les informations de connexion et le mot de passe du compte iCloud de la victime dans l'application stalkerware, **toutes les données d'iCloud sont mises à la disposition** de l'auteur-e. Ces données comprennent, entre autres[23] :

- Coordonnées

---

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

[21] Norton Labs. (2021, 24 juin). *A year after lockdown : stalkerware on the rise.* Consulté sur https://www.nortonlifelock.com/blogs/norton-labs/stalkerware-rise, Davidovic, I. (2021, 3 décembre). How to spot the software that could be spying on you. *BBC News.* Consulté sur https://www.bbc.com/news/business-59390778; Clerix, K. (2022, 2 février). *Je partner bespioneren via de gsm ? Kinderlijk eenvoudig (en illegaal).* Knack. Consulté sur 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.* Consulté sur https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/04/12075509/EN_The-State-of-Stalkerware-2021.pdf

[21] Norton Labs. (2021, 24 juin). *A year after lockdown : stalkerware on the rise.* Consulté sur https://www.nortonlifelock.com/blogs/norton-labs/stalkerware-rise

[22] 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. Consulté sur 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. Consulté sur https://citizenlab.ca/docs/stalkerware-holistic.pdf

[23] 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. Consulté sur https://citizenlab.ca/docs/stalkerware-holistic.pdf

- Photos
- Calendrier
- Notes
- Géolocalisation
- Documents stockés dans l'iCloud

Pour pouvoir continuer à utiliser les multiples fonctionnalités des stalkerwares sur Android, le système fermé des appareils iOS peut être contourné par un ***jailbreak*** de ces appareils. Cela permet d'installer sur l'appareil des logiciels et des applications qui ne sont pas soutenus par Apple, donc aussi des stalkerwares. L'accès physique est toujours nécessaire pour effectuer un *jailbreak* et exige plus d'efforts et de connaissances technologiques de la part de l'agresseur-e. On peut toutefois trouver sans problème suffisamment d'informations sur Internet.[24]

2. Impact psychologique sur la victime

Comme le phénomène du stalkerware est encore très peu connu du grand public et qu'il est difficile à détecter, les **victimes ignorent souvent** qu'elles sont surveillées par un-e (ex-)partenaire par le biais de leur smartphone, leur tablette ou leur ordinateur. Néanmoins, les victimes peuvent avoir des **soupçons**. Par exemple, la victime a le sentiment que son (ex-)partenaire sait à tout moment où elle se trouve, avec qui elle a eu une interaction ou qu'il-elle dispose d'informations provenant de messages envoyés à une autre personne que l'auteur-e.[25]

Tout comme le harcèlement physique, le **harcèlement facilité par les stalkerwares** a un impact psychologique considérable sur la victime. En raison du *gaslighting* et du contrôle coercitif exercé par l'auteur-e, les victimes vivent dans un **état d'anxiété perpétuel**. Elles ont l'impression de ne pas pouvoir échapper à leur auteur-e et se sentent **de plus en plus isolées**. Parce qu'elles n'ont plus confiance en elles-mêmes et en leurs propres perceptions, les victimes **évitent tout contact avec leur réseau social**.[26] La crainte d'impliquer leur famille et leurs ami-e-s dans la situation de violence créée par leur (ex-)partenaire peut également amener les victimes à éviter tout contact avec eux-elles. En outre, si les victimes **hésitent** bien souvent à **contacter** les **organisations d'aide**, c'est généralement par crainte que l'auteur-e ne soit au courant et que la situation ne s'aggrave ultérieurement.[27]

Plus spécifiquement dans le contexte des stalkerwares, les victimes, **limiteront, voire éviteront** complètement l'**utilisation de leurs smartphone**, **tablette ou ordinateur**. Par conséquent, les victimes sont non seulement moins accessibles pour leur réseau social, mais il est également plus difficile pour elles d'obtenir de l'aide en cas de danger.[28]

---

[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. Consulté sur https://citizenlab.ca/docs/stalkerware-holistic.pdf ; SecureMac. (13 octobre 2021). *How to check for stalkerware on an iPhone.* Consulté sur https://www.securemac.com/news/how-to-check-for-stalkerware-on-an-iphone

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

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

[27] 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. Consulté le 22 février 2022 sur https://wesnet.org.au/wp-content/uploads/sites/3/2020/11/Wesnet-2020-2nd-National-Survey-Report-72pp-A4-FINAL.pdf.

[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. Consulté le 22 février 2022 sur https://wesnet.org.au/wp-content/uploads/sites/3/2020/11/Wesnet-2020-2nd-National-Survey-Report-72pp-A4-FINAL.pdf.

3. Victimisation : chiffres

3.1. Prévalence de la victimisation générale due aux stalkerwares[29]

En Belgique, il n'existe pas de chiffres officiels sur le nombre de victimes des stalkerwares. Il convient donc de consulter les sociétés antivirus pour obtenir des chiffres. Comme ces chiffres dépendent de la clientèle des entreprises, de la définition du stalkerware utilisée et du fait que les client-e-s le signalent ou non, ils varient considérablement. L'ESET note « des centaines de cas par an » et Kaspersky a également constaté 180 infections par stalkerware sur des smartphones belges en 2020. La Belgique occupe ainsi la 9e place dans le top 10 des pays européens les plus touchés par les stalkerwares en 2020, selon Kaspersky.[30] En 2021, la Belgique est toujours en 9e position, bien que le nombre soit tombé à 94 infections par stalkerware[31] Les chiffres de Bitdefender sont un peu plus élevés, avec 551 cas d'infections par stalkerware en Belgique en 2021. Norton a enregistré un chiffre encore plus élevé que Bitdefender : entre le 19 mai 2021 et le 21 janvier 2022, 12 472 détections de stalkerware ont été effectuées sur 8 168 appareils belges. Une explication possible de ces chiffres nettement plus élevés de Norton est due à la définition qu'ils utilisent. Les logiciels et applications légitimes qui peuvent être utilisés pour surveiller une personne sans son consentement sont également inclus. Ces chiffres ne représentent toutefois que la partie émergée de l'iceberg et dans la pratique, les chiffres réels seront bien plus élevés. Si de nombreux Belges ont installé un logiciel antivirus sur leur ordinateur, ce n'est pas du tout le cas sur les smartphones et les tablettes.[32] La Coalition Against Stalkerware estime ainsi que près de 1 million de personnes dans le monde sont victimes de ces logiciels chaque année.[33]

3.2. Prévalence des victimes de stalkerwares dans le contexte de violences entre (ex)partenaire

Il est nécessaire de s'appuyer sur des études étrangères pour se faire une idée de l'ampleur du problème lié aux stalkerwares dans les situations de violences entre (ex-)partenaires.

Lors de la deuxième **National Survey on Technology Abuse and Domestic Violence in Australia** de **2020**, 99,3 % des professionnel-le-s interrogé-e-s ont déclaré avoir des client-e-s qui avaient déjà été victimes de harcèlement facilité par la technologie, y compris par l'utilisation de stalkerwares. Interrogé-e-s sur l'utilisation d'applications de repérage GPS par l'auteur-e, 16,2 % des professionnel-le-s ont répondu qu'ils/elles le voyaient « toujours » et 45,6 % « souvent ». 42,2 % des professionnel-le-s considèrent que Monitoring via iCloud est « fréquemment » utilisé par un-e auteur-e de violences envers son (ex-)partenaire.[34]

En **France** également, des recherches ont déjà été menées sur les cyberviolences entre (ex)partenaires. Selon une enquête réalisée en **2018** par le **Centre Hubertine Auclert**, 64 % des personnes interrogées, des femmes victimes de violences de la part de leur (ex-)partenaire, ont indiqué avoir déjà fait l'expérience d'une forme de surveillance numérique. 21 % des personnes interrogées ont

---

[29] Clerix, K. (2 février 2022). *Je partner bespioneren via de gsm ? Kinderlijk eenvoudig (en illegaal).* Knack. Consulté sur le site https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

[30] Kaspersky. (2021). *The state of stalkerware in 2020.* Consulté le 22 février 2022 sur https://securelist.com/the-state-of-stalkerware-in-2020/100875/

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

[32] Clerix, K. (2 février 2022). *Je partner bespioneren via de gsm ? Kinderlijk eenvoudig (en illegaal).* Knack. Consulté sur le site https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

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

[34] 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. Consulté sur https://wesnet.org.au/wp-content/uploads/sites/3/2020/11/Wesnet-2020-2nd-National-Survey-Report-72pp-A4-FINAL.pdf

déjà été surveillées en particulier par des stalkerwares. En raison de la difficulté de détection des stalkerwares mentionnée précédemment, il a également été demandé aux répondant-e-s, dans le cadre de l'enquête, s'ils/elles « soupçonnaient l'auteur-e de les surveiller ». 64 % des personnes interrogées ont déclaré qu'elles pensaient que leur (ex-)partenaire avait eu accès à distance à leur téléphone, leurs comptes ou leur courrier, tandis que 19 % pensaient avoir été suivies par GPS. Chez 44 % des personnes interrogées, la victime a indiqué que son (ex-)partenaire savait où elle se trouvait, sans lui en avoir parlé au préalable.[35]

4. Possibilités techniques de prévention, de reconnaissance et d'élimination des stalkerwares

4.1. Prévention des stalkerwares

Comme nous l'avons déjà mentionné, l'accès physique est une condition préalable à l'installation d'un stalkerware. **Ne pas laisser son appareil sans surveillance ou ne pas laisser quelqu'un l'utiliser, et une bonne protection** constituent déjà une première barrière pour les agresseur-e-s potentiel-le-s. Par exemple, n'utilisez pas l'identification faciale ou l'empreinte digitale pour déverrouiller un appareil, mais utilisez un **mot de passe fort**.[36] L'agresseur-e peut, par exemple, contourner le déverrouillage de l'appareil par l'identification faciale ou l'empreinte digitale lorsque la victime est endormie. Selon SafeOnWeb, il est préférable de choisir un mot de passe long, contenant au moins 13 caractères et utilisant des chiffres, des majuscules et des symboles. Comme il est recommandé de ne pas utiliser le même mot de passe pour différents comptes et que se souvenir de plusieurs mots de passe forts n'est pas évident, SafeOnWeb recommande également l'utilisation de **coffres-forts électroniques**. Étant donné qu'un tel coffre-fort électronique conserve de manière sûre tous les mots de passe, il convient uniquement de se souvenir du mot de passe fort qui donne accès au coffre-fort.[37]

Mais un mot de passe fort ne suffit pas si quelqu'un d'autre en a connaissance. C'est pourquoi il est recommandé de ne **pas communiquer des mots de passe à des tiers**[38]. Dans la pratique, cependant, les mots de passe sont souvent partagés entre partenaires. Lors d'une étude de Kaspersky sur le cyberharcèlement dans les relations, menée auprès de 21 055 participant-e-s de 21 pays, 57 % des personnes interrogées ont déclaré avoir partagé le mot de passe de leur téléphone portable avec leur partenaire. Un pourcentage similaire (56 %) a déclaré connaître le mot de passe du téléphone portable de son/sa partenaire. Par ailleurs, 2 répondant-e-s sur 5 considèrent qu'il est normal de partager les informations de connexion de leur compte iCloud ou Google avec leur famille.[39] Et si les mots de passe ne sont pas partagés volontairement, dans les situations de violences entre (ex-)partenaires, une victime peut être (subtilement) forcée à les partager.

Non seulement l'accès à l'appareil peut être rendu plus difficile, mais aussi l'installation du stalkerware lui-même. Les appareils **Android** permettent de configurer les paramètres pour bloquer l'**installation**

---

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

[36] Coalition Against Stalkerware. (20 mai 2022). *What is stalkerware ?* [Vidéo]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0;

[37] SafeOnWeb.be. (s.d.). Utilisez des mots de passe longs. Consulté sur https://www.safeonweb.be/fr/utilisez-des-mots-de-passe-longs

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

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

d'applications tierces.[40] Cette mesure ne sera donc efficace contre les stalkerwares que si le logiciel ou l'application n'a pas été obtenu et téléchargé à partir du Google Play Store. Il est également possible qu'un-e agresseur-e ayant connaissance de cette possibilité débloque simplement l'option.

Et enfin, il est également recommandé d'installer un **programme antivirus** sur chaque appareil. Un programme antivirus peut en effet détecter les programmes de harcèlement et même les supprimer si nécessaire.[41]

4.2. Détecter les stalkerwares

Étant donné que les développeurs de stalkerware font tout leur possible pour dissimuler leur logiciel sur un appareil infecté, il n'est pas facile de détecter les signes d'une infection par un stalkerware. Certainement pas lorsque, en tant qu'utilisateur, vous ne savez pas exactement ce qu'il faut rechercher. Il existe toutefois certains signes qui peuvent indiquer une possible infection par un stalkerware. Premièrement, comme cela a déjà été évoqué, l'**auteur-e** peut lui/elle-même donner une première indication en ayant **connaissance d'informations** qu'il/elle **ne pourrait normalement pas connaître**.[42] Deuxièmement, tous les stalkerwares ne sont pas installés directement à partir d'app stores. L'auteur-e devra donc naviguer sur certains sites pour obtenir des informations relatives aux stalkerwares et à la manière de les installer sur un appareil. C'est pourquoi il est également utile de **vérifier l'historique Internet de l'appareil** en cas de suspicion. Il est important de garder à l'esprit que l'absence de tels sites dans l'historique Internet ne signifie pas pour autant que le stalkerware n'est pas présent sur l'appareil. Il est en effet très facile de supprimer l'historique Internet. Et enfin, il existe également des signaux qui s'appliquent à l'appareil infecté lui-même. Ainsi, l'utilisateur-rice aura l'impression que l'**appareil se comporte de façon « étrange »**. Par exemple, la batterie se vide très rapidement, l'appareil est très chaud lorsqu'il n'est pas utilisé de manière intensive ou l'appareil redémarre de manière aléatoire.[43] Il est donc recommandé de **vérifier** fréquemment les **logiciels ou applications installés sur l'appareil, ainsi que leurs autorisations**. En particulier, les applications dont l'utilisateur-rice sait qu'il/elle ne les a pas installées et qu'il/elle ne reconnaît pas, mais qui accèdent néanmoins à divers capteurs de l'appareil[44], peuvent indiquer que l'appareil est potentiellement infecté par un stalkerware.[45]

Spécifiquement pour les appareils iOS, la présence des **applications Cydia ou Sileo** constitue une indication. Ces deux applications sont les plus utilisées pour *jailbreaker* les appareils iOS.[46]

4.3. Supprimer les stalkerwares

---

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

[41] Clerix, K. (2 février 2022). *Je partner bespioneren via de gsm ? Kinderlijk eenvoudig (en illegaal).* Knack. Consulté sur le site https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

[42] Clerix, K. (2 février 2022). *« In België zijn er duizenden mensen die met stalkerware bespioneerd worden »/Intervieweuse S. Lemaire.* De wereld van Sofie. Consulté le 18 février 2022 sur https://radio1.be/luister/select/nieuwe-feiten/in-belgie-zijn-er-duizenden-mensen-die-met-stalkerware-bespioneerd-worden

[43] Clerix, K. (2 février 2022). *« In België zijn er duizenden mensen die met stalkerware bespioneerd worden »/Intervieweuse S. Lemaire.* De wereld van Sofie. Consulté le 18 février 2022 sur https://radio1.be/luister/select/nieuwe-feiten/in-belgie-zijn-er-duizenden-mensen-die-met-stalkerware-bespioneerd-worden ; Coalition Against Stalkerware. (20 mai 2022). *What is stalkerware ?* [Vidéo]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0

[44] Des exemples de tels capteurs sont la caméra, le son, l'*écran tactile*, etc.

[45] Coalition Against Stalkerware. (20 mai 2022). *What is stalkerware ?* [Vidéo]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0

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

Il n'est pas facile de supprimer tous les stalkerwares. Il est souvent recommandé d'effectuer un scan de l'appareil avec un **programme antivirus** pour détecter et supprimer les stalkerwares. L'appareil peut ensuite être à nouveau soumis à un scan afin de vérifier que le stalkerware a bien été supprimé. Si ce n'est pas le cas, il est possible de réinitialiser l'appareil (hard reset), c'est-à-dire **restaurer** les **paramètres d'usine**.[47]

De nombreux avis en ligne recommandent de supprimer le stalkerware de l'appareil dès que possible. Dans les situations de violences entre (ex-)partenaires, une certaine prudence est toutefois de mise. Certains stalkerwares envoient une notification à l'auteur-e l'informant que l'application a été détectée ou supprimée. Cela peut conduire à une **escalade** de la situation de violences entre partenaires.[48] En outre, la suppression du logiciel ou de l'application en question entraîne également l'**élimination de la preuve**.[49]

5. Bonnes pratiques à l'étranger

5.1. Initiatives législatives

Avec la loi n° 2020-936 du 30 juillet 2020, la **France** envoie un signal clair : toute surveillance en secret et non autorisée d'une personne par le biais de la géolocalisation ne sera pas tolérée. *« Fixer, enregistrer ou transmettre de quelque manière que ce soit la localisation réelle ou différée dans le temps d'une personne sans son consentement »* constitue un délit. En outre, une attention particulière est accordée à la situation de vulnérabilité des victimes de violences entre (ex-)partenaires lorsqu'un-e (ex-)partenaire surveille leur localisation. Dans de tels cas, des peines de prison plus élevées s'appliquent.[50]

L'**Allemagne** a également adopté des mesures dans le domaine du cyberharcèlement en général et de la cybersurveillance en particulier. Depuis le 1er octobre 2021, le harcèlement par le biais d'un programme informatique visant à espionner une autre personne est inclus dans le Code pénal allemand, comme un élément du volet « stalking ».[51]

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

ECHAP est un collectif de hackers féministe français engagé dans la lutte contre les violences technologiques faites aux femmes. Il organise des ateliers de travail pour les professionnel-le-s qui travaillent avec des victimes féminines de violences et offre un soutien technique aux victimes si elles le souhaitent. Il rédige également des **manuels pour les victimes de violences commises par un-e (ex-)partenaire** lorsque l'auteur-e fait un usage abusif de la technologie.[52] Sur son site, il met par exemple des guides généraux à disposition concernant les stratégies relatives aux mots de passe et la façon dont une victime peut, une fois la relation terminée, se déconnecter numériquement d'un-e (ex-

---

[47] Clerix, K. (2 février 2022). *Je partner bespioneren via de gsm ? Kinderlijk eenvoudig (en illegaal).* Knack. Consulté sur le site https://www.knack.be/nieuws/belgie/je-partner-bespioneren-via-de-gsm-kinderlijk-eenvoudig-en-illegaal/article-longread-1829437.html

[48] Coalition Against Stalkerware. (20 mai 2022). *What is stalkerware ?* [Vidéo]. Youtube. https://www.youtube.com/watch?v=zLtfoCw16Z0

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

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

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

[52] ECHAP. (s.d.). *Association de lutte contre l'utilisation de la technologie dans les violences faites aux femmes.* Consulté sur https://echap.eu.org/

)partenaire. Il dispose également de guides plus spécifiques sur la sécurité des comptes en ligne ou la sécurité des appareils informatiques, notamment sur la manière de détecter les signes de la présence d'un stalkerware sur un smartphone. [53]

CETA (États-Unis) dispose également de manuels « étape par étape » pour les victimes de violences entre (ex-)partenaire. Comme l'ECHAP, CETA dispose aussi bien de guides généraux que de guides plus spécifiques. En outre, il existe également des guides spécifiques pour différents comptes (de médias sociaux) qui indiquent comment une victime peut adapter la configuration des paramètres d'un compte pour assurer une sécurité supplémentaire.[54]

Les manuels des deux organisations constituent également de *bonnes pratiques* par le fait qu'ils sont **faciles à utiliser**, **quelles que soient les connaissances technologiques de chacun**. En outre, les deux organisations ont spécifiquement abordé dans leurs manuels la **situation particulière** des victimes de **violences facilitées par la technologie commises par un-e (ex)partenaire**. Les manuels rappellent ainsi à plusieurs reprises au/à la lecteur-rice que le fait de changer les mots de passe ou d'interdire l'accès à un certain compte, par exemple, peut amener l'auteur-e à modifier son comportement et peut même aggraver la situation. Il est de surcroît conseillé aux victimes d'**élaborer un plan de sécurité avant** de **supprimer les stalkerwares ou de modifier les mots de passe**.

III. Recommandations

Sur la base des informations ci-dessus, des recherches scientifiques et des recommandations du GREVIO[55] et de la Commission européenne[56], le présent avis formule un certain nombre de recommandations concrètes.

1. Nécessité d'une étude de prévalence

Comme l'illustre le présent avis, il y a un manque de chiffres belges concernant les victimes de stalkerware en général, et plus particulièrement les victimes de violences commises par un-e (ex)partenaire qui sont confrontées aux stalkerwares. À l'heure actuelle, l'étendue de ce problème en Belgique n'est pas clairement déterminée.

2. Besoin de sensibilisation

2.1. Sensibilisation générale

Les stalkerwares étant un phénomène relativement « récent », il est nécessaire de sensibiliser le **grand public** à leur sujet.

2.2. Sensibilisation des victimes

De plus, les victimes **(potentielles)** de **violences commises par un-e (ex-)partenaire** doivent également être sensibilisées. Étant donné que les logiciels et les applications de harcèlement sont souvent cachés et qu'ils font tout pour le rester, il est impératif que les victimes (potentielles) aient connaissance de l'existence des stalkerware et sachent quels sont les signes pouvant indiquer qu'un

[53] ECHAP. (s.d.). *Nos guides*. Consulté sur https://echap.eu.org/ressources/

[54] CETA. (s.d.). *Resources.* Consulté sur https://www.ceta.tech.cornell.edu/resources

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

[56] 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)]. Consulté sur https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/com_2022_105_1_en.pdf

appareil est infecté par un stalkerware. Il est également important que les victimes (potentielles) sachent où trouver de l'aide.

Les victimes de violences entre (ex-)partenaires devraient recevoir des informations concrètes sur ce qu'est un stalkerware, sur les signes possibles indiquant un appareil infecté et sur les étapes à suivre pour reprendre le contrôle de sa vie, tant hors ligne qu'en ligne, et éventuellement porter plainte. Cette recommandation peut être mise en œuvre, par exemple, en élaborant un manuel expliquant, pas à pas, ce qu'une victime peut entreprendre si elle soupçonne ou a connaissance de l'installation d'un stalkerware sur son appareil. A nouveau, la sécurité de la victime est primordiale. Tous les risques liés à la détection ou à la suppression d'un stalkerware doivent être énumérés et l'élaboration d'un plan de sécurité avant d'agir doit être recommandé. Il convient également de préciser que la suppression d'un stalkerware entraînera la perte de preuves.

2.3. Sensibilisation des professionnels

La **police et la justice** manquent aussi souvent de connaissances sur les stalkerwares. Cela s'explique non seulement par la relative méconnaissance du phénomène, mais également par la spécialisation du sujet. Par conséquent, la sensibilisation des praticien-ne-s pertinent-e-s devrait non seulement consister à clarifier ce qu'est exactement un stalkerware, mais aussi à expliquer qu'il s'agit d'une forme de violence commise par l'(ex-)partenaire. Il devrait donc être considéré comme une preuve dans les cas de violences entre (ex-)partenaires. Dès le signalement des dossiers concernant des violences entre (ex)partenaires, il convient de prêter attention aux formes numériques de violence, telles que l'installation de stalkerwares, et ce, indépendamment du fait que la victime en ait ou non fait mention au moment de son signalement. Il faut également tenir compte du fait que non seulement l'appareil de la victime peut contenir un stalkerware, mais aussi celui de l'enfant commun, certainement en cas de divorce. Les formes numériques de violence ne peuvent de surcroît pas être minimisées. La recherche scientifique, comme indiqué précédemment dans le présent avis, montre clairement qu'affirmer que la violence numérique a un impact moindre sur la victime constitue un mythe.

Tout au long du processus policier et judiciaire, la sécurité de la victime doit être primordiale. Il s'agit principalement d'informer la victime des dangers que la détection de stalkerwares peut présenter dans le cadre de la collecte de preuves. Certains types de stalkerware envoient en effet une notification à l'auteur-e l'informant que l'application a été détectée ou supprimée. Cela peut entraîner une escalade de la violence.

Il est donc nécessaire d'**adapter la circulaire COL 4/2006** en accordant une attention particulière aux formes numériques de violences entre (ex-)partenaires.

Tout comme la police et la justice, le **secteur de l'aide** doit également prêter attention aux formes numériques de violences entre (ex-)partenaires, dont l'installation d'un stalkerware constitue un exemple. Dès le signalement de la victime auprès d'une organisation d'aide, sa sécurité numérique doit être examinée. Y a-t-il des comptes partagés ? L'auteur-e avait-il/elle accès à un appareil qui se comporte maintenant de façon « étrange » ? Ici aussi, la sécurité de la victime est primordiale. Les intervenant-e-s sociaux-ales doivent être informés de la façon exacte d'élaborer un plan de sécurité tenant compte de la dimension numérique des violences commises par l'(ex-)partenaire. Par la suite, les intervenant-e-s sociaux-ales peuvent également fournir aux victimes des conseils et des outils sur la sécurité en ligne.

Outre la police, la justice et le secteur de l'aide, le **secteur IT** pourrait également tirer avantage d'informations sur l'utilisation des stalkerwares dans le contexte des violences entre (ex-)partenaires. En effet, il est fort probable que les victimes de violences entre (ex-)partenaires s'adressent à eux avec un appareil qui « se comporte bizarrement » ou avec le soupçon qu'un-e partenaire ou un-e ex-partenaire les surveille par le biais de cet appareil.

Un exemple pratique de la sensibilisation axée sur le secteur IT peut se traduire par une brochure expliquant en quoi consiste la violence entre (ex)partenaires, comment la technologie telle que les stalkerwares peut être utilisée par un-e auteur-e pour surveiller et contrôler la victime et comment ces victimes peuvent être soutenues au mieux. La sécurité de la victime doit occuper une place centrale dans la brochure. Il devrait, par exemple, être explicitement mentionné qu'aucune action, telle que la suppression du stalkerware, ne devrait être entreprise sans notification des risques y afférents et sans le consentement explicite de la victime. Et enfin, la brochure devrait idéalement contenir également une liste d'organisations vers lesquelles les victimes peuvent être dirigées pour y recevoir une aide supplémentaire ou éventuellement, pour y porter plainte.

3. Une attention particulière est accordée aux refuges et aux stalkerwares

Lorsqu'une victime de violences commises un-e (ex-)partenaire ne se sent plus en sécurité chez elle ou ne peut plus y rester, elle peut se rendre dans un refuge. Il est extrêmement important pour le fonctionnement du refuge et pour la sécurité de la victime que l'adresse reste secrète pour l'auteur-e. Un appareil infecté par un stalkerware installé par l'auteur-e des violences entre (ex-)partenaires peut compromettre la situation. C'est pourquoi il est important d'établir une coopération entre les expert-es IT et les refuges afin de minimiser le danger associé aux stalkerwares dans le contexte de violence entre (ex-)partenaires. Par exemple, qu'il y ait ou non une suspicion que l'appareil d'une victime contienne un stalkerware, chaque appareil de la victime devrait être vérifié par un expert-e IT afin de préserver l'emplacement secret du refuge. Pour des raisons évidentes, il est préférable d'effectuer ce contrôle avant l'arrivée de la victime au refuge. Comme mentionné précédemment, la coopération entre les expert-e-s IT et les refuges est également utile dans le cadre de la collecte potentielle de preuves.

4. Modification du Code pénal : extension de la notion de « harcèlement » (art. 442bis C. pén.)

L'utilisation des stalkerwares peut actuellement relever de deux dispositions pénales. Tout d'abord, le délit de harcèlement visé à l'art. 442bis du Code pénal est passible d'une peine de prison pour ceux/celles qui ont gravement affecté la tranquillité d'une personne. Le harcèlement ne nécessite pas une intention particulière de nuire. Il n'est pas non plus nécessaire que le harcèlement soit de nature physique et il peut donc également avoir lieu par l'utilisation de moyens technologiques (comme un smartphone) ou de Internet. Toutefois, le harcèlement présuppose un comportement continu ou récurrent. La Cour de cassation a également accepté qu'un comportement unique produisant des effets persistants qui affectent la vie privée d'une personne puisse constituer un délit de harcèlement.[57] Cette jurisprudence a été accueillie avec beaucoup de critiques par la doctrine juridique.[58] La discussion concernant l'existence d'une exigence d'actes multiples n'est donc peut-être pas encore définitivement tranchée.

Le harcèlement avec utilisation de stalkerware sera dans la plupart des cas également punissable au titre du délit de harcèlement électronique (art. 145 §3bis de la loi sur les communications électroniques), à savoir l'utilisation abusive d'un réseau de communication électronique ou d'un moyen de communication dans le but d'importuner ou de provoquer des dommages à la personne concernée. Dans ce contexte, un acte unique est suffisant pour être punissable. Malheureusement, cette infraction présente quelques limites. Par exemple, le-la harceleur-se doit avoir une intention particulière, à savoir la volonté de causer des nuisances ou des préjudices. En outre, contrairement au harcèlement « ordinaire », l'aggravation de la peine pour des motifs liés à la haine (comme l'art. 442ter du C. pén.) ne s'applique pas à l'article 145, §3bis de la LCE.

[57] Cass. 29 octobre 2013, P.13.1270.N, Arr.Cass. 2013, n° 563.
[58] D. VOORHOOF, « Recente rechtspraak belaagt expressievrijheid op het Internet », *Juristenkrant* 2013, 3, 278

Une récente directive de la Commission européenne vise à élargir la notion du délit de harcèlement. Elle devrait également inclure la surveillance continue d'un tiers, sans son consentement ni sa connaissance, au moyen de technologies et/ou de moyens de communication. Il peut s'agir, par exemple, de la surveillance de la géolocalisation par le biais de l'installation d'un stalkerware ou de la surveillance des comptes (de médias sociaux) des victimes par le vol de leurs mots de passe.

Les deux dispositions pénales susmentionnées laissent place à une interprétation incertaine. Une clarification juridique du fait que l'utilisation de stalkerwares équivaut à du harcèlement (électronique) s'avère donc nécessaire.

! Points d'attention importants pour toutes les parties prenantes concernant tous les stalkerwares !

- Le stalkerware est une forme de violence entre (ex)partenaires.
- Dès le signalement de la victime, il convient de prêter attention aux formes de violence numériques, et ce, indépendamment du fait que celles-ci soient ou non dénoncées par la victime.
- Lors de la collecte de preuves liées à l'utilisation d'un stalkerware, il convient d'examiner non seulement les appareils de la victime, mais également ceux de l'enfant ou des enfants communs, certainement en cas de divorce.
- La sécurité de la victime est primordiale à tout moment ; un plan de sécurité doit être établi avant d'agir.
- La victime doit toujours être informée des dangers possibles liés à la détection et à la suppression de stalkerwares, et elle doit bénéficier d'un accompagnement lors de toute démarche ultérieure consécutive à la découverte de ces stalkerwares.