Der Feind in der eigenen Tasche

Stalkerware und digitale Überwachung im Kontext von Partnerschaftsgewalt

Chris Köver

Es gibt Branchen, die erfordern eine gewisse moralische Flexibilität, hierzu gehören die Branchen, die Überwachungssoftware vertreiben, die dazu dient, die eigenen Kinder oder Partner*innen auszuspähen. In wenigen Minuten lässt sich so ein Programm auf dem Telefon der Zielperson – auch heimlich – installieren. Besondere technische Fähigkeiten sind dazu nicht notwendig. Die entsprechende App läuft danach unbemerkt im Hintergrund und schneidet dort Telefonate, Chat-Nachrichten, Fotos, Videos und den Standort mit. Die Kund*innen –also diejenigen, die die App installiert haben – bekommen all diese Informationen in einem Browserfenster angezeigt und können sich dort durch das gesamte Telefon der überwachten Person scrollen. Ein tieferer Einblick in die Privatsphäre eines anderen Menschen ist kaum vorstellbar.

Die Firmen vermarkten ihre Apps öffentlich vor allem als Trackingsoftware für besorgte Eltern, die immer wissen wollen, wo ihre Kinder sind und was sie auf dem Smartphone tun (vgl. Parsons u.a. 2019: 67). Diese Verkaufsstrategie ist klug gewählt, denn das Abhören einer anderen Person ohne deren Wissen und Einverständnis ist in Deutschland und vielen anderen Ländern eine Straftat. Ein Produkt zu diesem Zweck dürfte gar nicht auf dem Markt sein. Wie viele Menschen Stalkerware einsetzen und wie viele von der illegalen Spionage betroffen sind, ist nicht erfasst. Aus bisherigen Recherchen (siehe z.B. Locker/Hoppenstedt 2017), Studien (siehe z.B. Chatterjee u.a. 2018) und den regelmäßig auftretenden Datenlecks der Apps, bei denen massenweise sensible Daten ins Internet gelangen, lässt sich jedoch einiges ableiten. Hierdurch ist zum Beispiel erkennbar, dass die meisten Nutzer dieser Apps männlich sind und dass sie die Apps vor allem nutzen, um (Ex-)Beziehungspartner*innen auszuspionieren.

Oft richten Männer die Geräte ein

Viele Beratungsstellen für Partnerschaftsgewalt kennen die Apps inzwischen durch ihre tägliche Arbeit. Frauen, die beispielsweise von einem Partner oder Ex-Partner bedroht und verfolgt werden, berichten dort regelmäßig, dass der Gewalttäter auch Spionagesoftware auf ihren Geräten installiert hat – oder dass sie dies zumindest vermuten. Nur so ist oft zu erklären, wie der Gewalttäter immer über Informationen darüber verfügt, wo sich die (Ex)-Partnerin befindet, mit wem sie spricht, was sie tut, um nur einiges zu nennen. Eine solche Form der Überwachung stellt eine Verletzung der Privatsphäre dar, die in Deutschland auch von der Verfassung geschützt wird. Diese Verletzung kann auch physische Gewalt als Folge haben, so z.B. wenn der Gewalttäter über das Ausspähen des Telefons von Trennungsabsichten der Partnerin erfährt – eine bekannte Hochrisikosituation – oder eine bereits geflohene Frau mit Hilfe der Geräteortung im Frauenhaus aufspürt, um ihr gegenüber gewalttätig zu sein. Expert*innen aus Beratungsstellen berichten, dass solche verdeckt arbeitenden Apps in den vergangenen Jahren zu einer massiven Bedrohung für die Sicherheit ihrer Klient*innen geworden sind. »Bei acht von zehn Fällen haben wir inzwischen eine digitale Komponente dabei« (bff 2019: o.S.), sagt Beate Köhler vom Anti-Stalking Projekt, einer Beratungsstelle in Berlin. Die Frauen kämen häufig bereits aus gewalttätigen Beziehungen, den Partnern gehe es vor allem um Kontrolle. Diese weiten sie über die Geräte aus – bis die Frauen selbst an ihrer geistigen Gesundheit zweifelten.

Teil des Problems ist die Wahrnehmung von Technologie als ›Männersache‹. In cis-/heterosexuellen Partnerschaften sind Männer häufig diejenigen, die Geräte einrichten, Computer installieren, Passwörter verwalten und damit diesen ganzen Bereich in der Regel kontrollieren. Anette von Schröder von der Hamburger Beratungsstelle Patchwork bestätigt diese Erfahrung und kommt zum dem Schluss, dass die Unsicherheit vieler Frauen im Umgang mit Technologie das Problem verschärft. Die Folge dieser einseitigen Arbeitsteilung ist, dass in einer Trennungs- oder Gewaltsituation Frauen dann teils gar nicht wissen, wie sie die Kontrolle über ihre Geräte oder Accounts zurück erlangen können.

Täter*innen fassen: Rechtlich möglich, praktisch schwierig

In Deutschland ist der Einsatz eines solchen Programms ohne die Zustimmung der überwachten Person – im Regelfall – eine Straftat. Das Strafgesetzbuch verbietet das Abhören von Gesprächen und das unerlaubte Fotografieren, auch das Ausspähen von Daten ist untersagt. Auch wenn diese Bestimmungen aus einer Zeit stammen lange bevor jede*r Spionage-Apps für wenige Euro im Internet kaufen konnte, so gelten sie auch für diese Form des unerlaubten Abhörens. Theoretisch ist die Rechtslage für Betroffene in Deutschland also gut. Zu Anklagen kommt es jedoch trotzdem so gut wie nie. Einzelne Fälle stellen eine Ausnahme dar, so wie die Verurteilung eines jungen Mannes in Stuttgart, der Spyware auf dem Handy seiner Ex-Partnerin installiert hatte und sich deshalb wegen »Abfangens von Daten« vor Gericht verantworten musste (vgl. o.A. 2015: o.S.). Dass es so wenig Verurteilungen gibt, ist erstaunlich, da aus Datenlecks der einschlägigen Firmen bekannt ist, dass solche Apps in Deutschland – konservativ gerechnet – tausendfach genutzt werden (Locker/Hoppenstedt 2017: o.S.). Warum ist es also so schwer Täter*innen juristisch zur Verantwortung zu ziehen, die andere mit solchen Methoden überwachen und terrorisieren? Praktisch scheitern Konsequenzen häufig schon daran, dass die meisten Betroffenen nie erfahren, dass sie überwacht werden. Selbst wenn ein konkreter Verdacht besteht, etwa weil eine Person merkt, dass ihr*e Partner*in Dinge weiß, die er nur durch eine heimliche Überwachung erfahren haben kann, ist es für Betroffene kaum möglich Stalkerware auf ihrem Telefon nachzuweisen: Den Fachberatungsstellen fehlt häufig das Personal und das technologische Wissen, um forensische Analysen der Geräte durchzuführen.

Die Polizei hätte zwar die technischen Möglichkeiten (vgl. Meister 2018: o.S.). Sie untersucht aber in der Regel keine Geräte zur Beweissicherung in Fällen von Partnerschaftsgewalt. An vielen Stellen fehlt den Beamt*innen auch schlicht das Verständnis, so berichten Betroffene, die versuchten Anzeige zu stellen. Und selbst wenn der Beweis erbracht werden kann, dass Stalkerware auf dem Telefon installiert ist, muss noch eine Verbindung zu der Person nachgewiesen werden, die die Daten abfängt. Ohne eine Rechnung, die den Kauf der App bestätigt, eine*n Zeug*in oder ein Geständnis haben Betroffene kaum etwas in der Hand, um ein Gericht zu überzeugen. Stalkerware-Fälle gelten den Staatsanwaltschaften somit als schwierig und sind entsprechend unbeliebt (vgl. ebd.).

Was das kanadische Citizen Lab[1] 2019 für Kanada forderte, gilt auch für Deutschland: Beamt*innen, Staatsanwaltschaften und Gerichte müssen besser geschult werden und brauchen mehr Personal, um solchen Fällen nachgehen zu können. Sonst können Täter*innen weiterhin in Ruhe illegal überwachen, ohne Konsequenzen fürchten zu müssen (vgl. Köver 2019a: o.S.).

Verantwortung von Hersteller*innen

Die meisten Stalkerware-Firmen verkaufen ihre Produkte vordergründig als Software zur Überwachung der eigenen Kinder – ein Szenario, das tatsächlich legal, wenn auch nicht legitim ist. In ihren Nutzungsbedingungen weisen sie darauf hin, dass die App nur mit ausdrücklicher Zustimmung der zu überwachenden Person installiert werden darf. Das macht es schwer, rechtlich gegen solche so genannten »Dual-Use«[2]-Produkte vorzugehen. Die Firmen berufen sich darauf, dass sie nichts Illegales täten. Für Straftaten, die mit ihren Apps begangen werden, seien allein die Täter*innen verantwortlich.

Auch die deutschen Datenschutzbehörden kommen an die Firmen kaum ran. Zwar gilt in Deutschland seit 2018 die Datenschutzgrundverordnung (DSGVO). Wer dagegen verstößt, begeht eine Ordnungswidrigkeit und kann mit Strafen von bis zu 20 Millionen Euro oder 4 % des Jahresumsatzes belegt werden. Dies gilt selbst dann, wenn die Firmen außerhalb der EU sitzen.[3] Allerdings kennt die DSGVO keine Herstellerhaftung für Datenschutzverstöße. »Verantwortlicher im datenschutzrechtlichen Sinne ist grundsätzlich die Person, die die Software einsetzt« schreibt Johannes Pepping von der Landesdatenschutzbehörde Niedersachsen (vgl. Köver 2019b: o.S.). Und die Person begeht weit mehr als eine Ordnungswidrigkeit, denn das illegale Ausspähen ist eine Straftat. Selbst wenn den Firmen nachgewiesen werden kann, dass sie selbst Daten erheben, etwa weil sie diese auf ihren Servern speichern, stehen die Chancen, eine Firma mit Sitz außerhalb der EU tatsächlich zu

1 Das Citizen Lab in Kanada ist ein interdisziplinärer Forschungs-Zusammenschluss, der sich mit Fragen an den Schnittstellen von Kommunikationstechnologie, Menschenrechten und globaler Sicherheit befasst, siehe dazu https://citizenlab.ca/about/.

2 Der Begriff Dual-Use steht sinngemäß für den doppelten Verwendungszweck eines Produktes und wird vorrangig benutzt, um Waren zu beschreiben, die für zivile Zwecke verwendet werden, sich aber auch für militärische Zwecke eignen und hierfür missbraucht werden.

3 Siehe hierzu Art. 3 DSGVO »Räumlicher Anwendungsbereich«.

fassen zu bekommen, sehr schlecht. Realistisch – so Pepping – sei das nur in Ländern, in denen es überhaupt Datenschutzbehörden gebe, wie etwa Kanada. Sonst bräuchte es Rechtshilfeabkommen mit dem jeweiligen Land (vgl. ebd.).

Viel effektiver könnte hier die Bundesnetzagentur eingreifen: Sie kann, anders als die Datenschützer, Produkte tatsächlich verbieten. In der Vergangenheit ist das etwa bei der vernetzen Puppe Cayla[4] passiert, die von der Agentur als verbotene »Abhöranlage« eingestuft wurde (vgl. Kühl 2017: o.S.). Die Bundesnetzagentur hat allerdings keine Rechtsgrundlage um gegen Apps vorzugehen. Ihre Verbote basieren auf dem § 90 Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen des Telekommunikationsgesetzes (TKG), der den Missbrauch von »Sende- oder sonstigen Telekommunikationsanlagen« regelt. Der Paragraf richtet sich damit ausschließlich gegen Hardware. Stalkerware-Apps auf einem Telefon fallen nicht darunter – obwohl sie der Funktion nach das gleiche und noch viel mehr erlauben. Zu überlegen wäre, ob im Kampf gegen Stalkerware nicht eine Erweiterung des Mandats dieser Behörde hilfreich sein könnte, oder ob analog zu der Behörde nicht eine Institution den Auftrag haben sollte Apps verbieten zu dürfen, sofern diese zumindest mehrheitlich missbräuchlich genutzt werden.

Auf der Suche nach Lösungen

Das Citizen Lab, ein Forschungsinstitut an der University of Toronto, hat die Branche in zwei ausführlichen Berichten untersucht (siehe Parsons u.a. 2019; Khoo u.a. 2019). Auf mehr als 300 Seiten analysierte ein Team aus Jurist*innen, Politikwissenschaftler*innen und Tech-Expert*innen, wie diese Programme funktionieren, wie sie vermarktet werden und vor allem: wie ihnen mit einem Netz aus Maßnahmen beigekommen werden kann. Die Autor*innen des Berichts betonen: Selbst wenn Herstellende ihre Software als

4 Cayla ist eine Spielzeugpuppe aus den USA, die mit Netzwerkzugang, Mikrofon und Spracherkennungs-Software ausgestattet ist. Da der Zugriff auf das Mikrofon über eine ungesicherte Bluetooth-Verbindung erfolgt, wurde sie 2017 in Deutschland nach § 90 Telekommunikationsgesetz als »verbotene Sendeanlage« eingestuft. In Österreich wurde die Puppe dagegen nicht verboten, da es keine entsprechende gesetzliche Grundlage gab. Siehe hierzu: https://futurezone.at/digital-life/spionage-im-kinderzimmer-puppe-cayla-wird-verboten/247.055.266 [Zugriff: 29.6.2020].

legale Dual-Use-Produkte anbieten, könnten diese zur Verantwortung gezogen werden. So könnten die Firmen zum Beispiel vom Gesetzgeber gezwungen werden den »Tarn-Modus« zu entfernen, also die Möglichkeit, eine App unsichtbar im Hintergrund auf einem Telefon laufen zu lassen, ohne dass die überwachte Person dies mitbekommt. Schließlich gibt es keinen legalen Anwendungsfall, für den so eine Funktion nötig wäre. Wenn eine Person der Überwachung zugestimmt hat, muss die Software nicht vor ihr versteckt werden. Wenn es um das eigene Kind geht, kann auch dieses über die App informiert werden. Zusätzlich könnten die Programme regelmäßig auf ihre Aktivität hinweisen, etwa mit Push-Mitteilungen auf dem Telefon oder einem »Zustimmungsdialog«, in dem die überwachte Person regelmäßig explizit ihr Einverständnis erteilt. Beides würde eine heimliche Überwachung verhindern.

Hersteller*innen müssten außerdem dafür sorgen, dass Betroffene auf ihren Seiten Anleitungen finden, wie sie das entsprechende Programm auf ihrem Telefon erkennen und deinstallieren können. Derzeit finden sich auf keiner der Firmen-Websites solche Hinweise. Sie richten sich ausschließlich an die potentiellen Kund*innen, also Überwacher*innen oder jene, die es werden wollen. Firmen sollen Betroffene zudem benachrichtigen müssen, wenn deren Daten im Zuge eines Sicherheitslecks öffentlich werden. Diese Lecks treten regelmäßig auf (vgl. Franceschi-Bicchierai 2019: o.S.). Nach der europäischen Datenschutzgrundverordnung und auch der kanadischen Entsprechung sind Firmen dazu verpflichtet, Nutzer*innen auf solche Verstöße gegen den Datenschutz hinzuweisen. Die Firmen beschränken sich allerdings bisher darauf, ihre Kund*innen und damit die Täter*innen zu informieren.

Technologische Lösungen haben allerdings ihre Grenzen. In vielen Fällen von häuslicher Gewalt übt der Partner ganz offen Kontrolle aus und zwingt entweder die Partnerin dazu, sich überwachen zu lassen oder erklärt dies zu einem ›Liebesbeweis‹ aus ›Sorge‹, dem die Partnerin zustimmt. In solchen Fällen hilft auch keine Push-Mitteilung. Solche verpflichtenden Designauflagen könnten laut dem Citizen Lab deswegen nur ein Faden in einem »Netz von Einschränkungen« sein, die um die Branche gelegt werden, um Betroffene vor Stalkerware zu schützen.

»Träumst du davon, das Telefon deiner Gattin auszuspionieren?«

Die Forscher*innen des Citizen Lab haben auch das Marketing der Produkte untersucht, also die Frage, wie Stalkerware-Firmen potentielle Kund*innen per Suchmaschinenoptimierung und bezahlten Anzeigen auf ihre Webseiten lotsen. Die Firma »mSpy« zum Beispiel geht dabei besonders dreist vor. Sie hat im HTML-Code ihrer Seite mehrere Textblöcke versteckt, die nicht auf der Website angezeigt werden. Dennoch werden sie von Suchmaschinen wahrgenommen und bei der Suche nach Stalkerware in den Suchergebnissen beachtet. Für Betrachter*innen werden sie nur sichtbar, wenn sie sich den Quelltext der Seite anschauen würden. Dort steht zum Beispiel: »Obwohl dieser Tracker für Eltern entwickelt wurde, die ihren rebellischen Teenager kontrollieren wollen, kann er auch von Partnern genutzt werden, um ihre bessere Hälfte auszuspionieren […].« (Parsons u.a. 2019: 67, Übersetzung C.K.) Auf einer anderen Blogseite versteckt sich der Text: »Träumst du davon, heimlich das Telefon deines Gatten/deiner Gattin auszuspionieren, um zu erfahren, ob er/sie dich betrügt?« (ebd.)

Um die Firmen zu entlarven, war es in vielen Fällen jedoch gar nicht nötig nach versteckten Texten und Schlagworten zu suchen. Sechs der neun im Bericht untersuchten Firmen bewarben ihre Produkte ganz offen als Hilfsmittel für Partnerschaftsgewalt. In diesen Fällen kann kaum von Dual-Use gesprochen werden, schreiben die Autor*innen plakativ (vgl. ebd.: 76), so müssten die Szenarien umgedreht werden: Diese Software sei in erster Linie ein Werkzeug für Stalking und Partnerschaftsgewalt – und könne nur zweitrangig für legale Zwecke genutzt werden.

Erkenntnisse des Citizen Lab für Deutschland

Das Citizen Lab sitzt in Kanada und schaut vor allem auf die dortige Rechtslage. Die Erkenntnisse sind jedoch auch aus deutscher Perspektive interessant. Erstens, weil einige der untersuchten Programme wie »FlexiSpy« und »mSpy« auch in Deutschland rege vermarktet und genutzt werden (vgl. Locker/Hoppenstedt 2017: o.S.). Dies ist bekannt aufgrund der zahlreichen Datenlecks der vergangenen Jahre, bei denen auch Nutzer*innendaten öffentlich wurden (vgl. ebd.). Und zweitens, weil viele der Beobachtungen sich fast eins zu eins auf Deutschland übertragen lassen. So kommen die Jurist*innen des Citizen Lab ebenfalls zu dem Schluss, dass Kanada theoretisch über eine ausreichen-

de Gesetzesgrundlage verfügt, um der Gewalt und dem Missbrauch durch Stalkerware zu begegnen. In der Realität führe dies aber nicht dazu, dass Betroffenen tatsächlich geholfen wird. Die Autor*innen führen dies zurück auf einen »Mangel an sozio-kulturellem und/oder technologischem Bewusstsein« (Khoo/Robertson/Deibert 2019: 150) für technologie-gestützte, geschlechtsspezifische Gewalt. Dies gelte entlang der gesamten Kette, angefangen bei den Polizeibeamt*innen, die Fälle aufnehmen, bis hin zu den Anwält*innen, Gerichten und den Gesetzgeber*innen, die die Fälle verhandeln.

Vergleichbares berichten Expert*innen für geschlechtsspezifische Gewalt in Deutschland, etwa der Bundesverband der Frauenberatungsstellen und Frauennotrufe (bff)[5] oder die Anti-Stalkingberatung des Frieda Frauenzentrums in Berlin[6].

Für Kanada wie für Deutschland gilt daher: Polizei und Staatsanwaltschaft müssen anfangen, den Einsatz von Stalkerware konsequent strafrechtlich zu verfolgen.

Die Rolle von PayPal

Ein weiterer Akteur im Geflecht von Stalkerware ist PayPal. Die Branche gedeiht auch deswegen so prächtig, weil sie von der einfachen Zahlung mit wenigen Klicks profitiert (vgl. Köver 2019a: o.S.). Wer Stalkerware verkauft, verstößt damit eigentlich gegen die Nutzungsbedingungen der Plattform. Immer wieder sperrt PayPal daher die Konten von Stalkerware-Firmen, zuletzt etwa von »Hellospy«. Die Firma bewirbt ihr Produkt offen als Lösung, um vermeintlich untreue Partner*innen auszuspionieren. Illustriert wird das auf der Website mit dem Foto eines Mannes, der eine Frau am Handgelenk packt – ihr Gesicht voller Blutergüsse. Eine Sperrung des PayPal-Kontos passierte allerdings erst in Folge von journalistischen Recherchen und Berichterstattung. In diesem Fall hatte die Tech-Nachrichtenseite »Motherboard« über den Fall berichtet (vgl. Cox,/Franceschi-Bicchierai 2019: o.S.). Und ebenso schnell wie die Firmen gesperrt werden, sind sie meist wieder da. Sie melden sich dafür

5 bff im Podcast siehe: https://netzpolitik.org/2019/npp-168-wenn-maenner-stalken-drohen-und-abhoeren/ [Zugriff: 29.6.2020].

6 Frieda Frauenzentrum Berlin zu Cyber-Stalking siehe: https://netzpolitik.org/2019/cyber-stalking-beraterinnen-fordern-staatliche-meldestelle/[Zugriff: 29.06.2020].

einfach unter einem neuen Firmennamen an. So wird das Melden von Anbietern zu einem Katz-und-Maus-Spiel, das sich endlos weiterspielen lässt.

Warum so ein offensichtlicher Täuschungsversuch eines bereits gesperrten Händlers nicht erkannt wird, will PayPal sich nicht äußern. Dabei kann es für Zahlungsdienstleister nicht so schwer sein zu erkennen, dass es sich um dasselbe Produkt handelt, dessen Verkauf auf der Plattform schon einmal verboten wurde. Offen bleibt auch, warum PayPal HelloSpy rauswirft, aber zahlreiche andere Spionage-Apps des gleichen Herstellers nach wie vor über die Plattform bezahlt werden können. Derzeit wickeln etwa ein Dutzend weitere Stalkerware-Firmen ihre Zahlungen über PayPal ab (vgl. Heasley 2019: o.S.).

Antivirenprogramme als Werkzeuge zur digitalen Selbstverteidigung

Bei digitaler Gewalt spielen auch Antivirenprogramme eine wichtige Rolle. Die großen Hersteller*innen wie z.B. »Kaspersky«, »Norton«, »ESET« und »Avira« haben Stalkerware als Bedrohung lange Zeit nicht ernst genommen – wohl, weil diese Programme in der engeren Definition tatsächlich keine Viren sind. Dabei könnten diese Firmen entscheidend dazu beitragen, Stalkerware auf Geräten auszuspüren. Eine Studie der Cornell University aus dem Jahr 2018 hatte untersucht, wie zuverlässig die Programme Stalkerware auf Telefonen finden. Das ernüchternde Ergebnis: Unter den großen Anbietern war keiner, der Spionage-geeignete Apps zuverlässig erkannt hätte. »Vermutlich reflektiert [dieses Ergebnis] die Designziele«, resümieren die Autor*innen, »die das Aufspüren von Spyware für intime Partnerschaftsgewalt nicht unbedingt mit einschließen, geschweige denn von Dual-Use-Apps« (Chatterjee 2018: 12, Übersetzung C.K.).

Diese Haltung ändert sich derzeit durch eine Initiative der Sicherheitsforscherin Eva Galperin. Galperin arbeitet bei der digitalen Bürgerrechtsorganisation Electronic Frontier Foundation und beschäftigt sich dort auch mit Partnerschaftsgewalt und deren digitalen Werkzeugen. Sie hat es mit hartnäckiger Lobbyarbeit geschafft, eine internationale Kampagne loszutreten. Teil dieser Bewegung ist auch die Softwarefirma Kaspersky Lab. Sie warnt ihre Nutzer*innen mit einer besonderen Nachricht, wenn Spionage-Software auf ihrem Telefon entdeckt wurde: »Diese App könnte dazu genutzt werden, um ihre persönlichen Daten zu kompromittieren, etwa ihre Anrufe mit-

zuhören, ihre E-Mails und Textnachrichten zu lesen, ihren Standort festzustellen oder ihre Kommunikation auf sozialen Netzwerken mitzuschneiden.« (Köver 2019c: o.S.) Galperin kritisiert, dass Programme, die direkten Zugriff auf das Telefon erfordern, von vielen Expert*innen bislang nicht als echtes Hacking anerkannt wurden. Dass eine Bedrohung für die Sicherheit von Frauen häufig nicht von fremden Hacker*innen oder gar Regierungsbehörden ausgeht, sondern von Menschen aus ihrer eigenen Familie, das lag für viele Sicherheitsforscher*innen außerhalb ihrer Horizonts (vgl. Köver 2019c: o.S.). Dies ändert sich derzeit. Nach dem Vorstoß von Kaspersky sind inzwischen auch Avira und Norton Teil der von Galperin initiierten Coalition Against Stalkerware[7].

Es bleibt zu hoffen, dass die gemeinsame Arbeit der Koalition tatsächliche Verbesserungen für Betroffene von geschlechtsspezifischer Gewalt mit sich bringt und auch andere Vertreiber*innen von IT-Sicherheitsprodukten sowie Legislative und Judikative hier ihre Verantwortung erkennen und zukünftig dem Schutz vor geschlechtsspezifischer Gewalt einen höheren Stellenwert einräumen.

Literatur

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (2019): »Workshop zur Erstellung eines Leitfadens zum Umgang mit Spionage-Apps auf Smartphones und Tablets im Zusammenhang mit Stalking und häuslicher Gewalt«. 25.3.2019, Berlin.

Chatterjee, Rahul/Doerfler, Periwinkle/Orgad, Hadas/Havron, Sam/Palmer, Jackeline/Freed, Diana/Levy, Karen/Dell, Nicola/McCoy, Damon/Ristenpart, Thomas (2018): »The Spyware Used in Intimate Partner Violence«. 2018 IEEE Symposium on Security and Privacy (SP) (Hg.). San Francisco, CA, 2018, S. 441-458. https://doi:10.1109/SP.2018.00061 [Zugriff: 29.6.2020].

7 Neben IT-Firmen beteiligen sich mehrere Organisationen an der Koalition, die zu geschlechtsspezifischer Gewalt arbeitet und Betroffene unterstützt. Der bff: Bundesverband Frauenberatungsstellen und Frauennotrufe ist im Mai 2020 der Koalition beigetreten siehe: https://frauen-gegen-gewalt.de/de/aktuelles/nachrichten/nachricht/bff-unterstuetzt-koalition-gegen-spionagesoftware-coalition-against-stalkerware-40-cas-41.html [Zugriff: 29.6.2020].

Cox, Joseph/Franceschi-Bicchierai, Lorenzo (2019): »PayPal Processes Payments for ›Stalkerware‹ Software Sold to Abusive Partners«. https://vice.com/en_us/article/7xnwa9/paypal-payments-stalkerware-software-abusive-partners [Zugriff: 29.6.2020].

Franceschi-Bicchierai, Lorenzo (2019): »This Spyware Data Leak Is So Bad We Can't Even Tell You About It«. https://vice.com/en_us/article/j573k3/spyware-data-leak-pictures-audio-recordings [Zugriff: 30.6.2020].

Heasley, Cian (2019): »PayPal is Handling Stalkerware Blood Money«. https://medium.com/@nscrutables/paypal-is-handling-stalkerware-blood-money-dc75acfad12c [Zugriff: 29.6.2020].

Khoo, Cynthia/Robertson, Kate/Deibert, Ronald (2019): »Installing Fear. A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications«. Citizen Lab Research (Hg.). Report No. 120, Toronto. https://citizenlab.ca/docs/stalkerware-legal.pdf [Zugriff: 29.6.2020].

Köver, Chris (2019a): »Spionage-Apps sind in erster Linie ein Werkzeug für Partnergewalt«. https://netzpolitik.org/2019/spionage-apps-sind-in-erster-linie-ein-werkzeug-fuer-partnergewalt/ [Zugriff: 29.6.2020].

Köver, Chris (2019b): »Warum es so schwer ist, rechtlich gegen Spionage-Apps vorzugehen«. https://netzpolitik.org/2019/warum-es-so-schwer-ist-rechtlich-gegen-spionage-apps-vorzugehen/ [Zugriff: 29.6.2020].

Köver, Chris (2019c): »Werden Virenschutz-Programme zu Verbündeten im Kampf gegen Stalkerware?«. https://netzpolitik.org/2019/werden-virenschutz-programme-zu-verbuendeten-im-kampf-gegen-stalkerware/ [Zugriff: 29.6.2020].

Kühl, Eike (2017): »Vernichten Sie diese Puppe«. https://zeit.de/digital/datenschutz/2017-02/my-friend-cayla-puppe-spion-bundesnetzagentur [Zugriff: 29.6.2020].

Locker, Theresa/Hoppenstedt, Max (2017): »Mehr als tausend Deutsche nutzen Spionage-App: 100 Prozent Erfolg – übermorgen ist meine Scheidung«. https://vice.com/de/article/ezjdbj/mehr-als-tausend-deutsche-nutzen-spionage-app-100-prozent-erfolg-uebermorgen-ist-meine-scheidung [Zugriff: 3.5.2020].

Meister, Andre (2018): »Mit diesen sieben Programmen liest die Polizei Smartphone-Daten aus«. https://netzpolitik.org/2018/digitale-forensik-mit-diesen-sieben-programmen-liest-die-polizei-smartphone-daten-aus/ [Zugriff: 29.6.2020].

o.A. (2015): »Handy-Spionage: Misstrauen unter Partnern kann strafbar sein«. https://sueddeutsche.de/wissen/technik-handy-spionage-misstrauen-unter-partnern-kann-strafbar-sein-dpa.urn-newsml-dpa-com-20090101-151209-99-189070 [Zugriff: 29.6.2020].

Parsons, Christopher/Molnar, Adam/Dalek, Jakub/Knockel, Jeffrey/Kenyon, Miles/Haselton, Bennett/Khoo, Cynthia/Deibert, Ronald (2019): »The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry«. Citizen Lab Research (Hg.). Report No. 119, Toronto. https://citizenlab.ca/docs/stalkerware-holistic.pdf [Zugriff: 29.6.2020].