BESCHWERDE

gegen Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland

[im Folgenden: Beschwerdegegnerin]

wegen Verstoßes gegen Art. 35 Absatz 1 in Verbindung mit Art. 34 Absatz 1 und 2 der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste)

Eingereicht durch die Gesellschaft für Freiheitsrechte e.V. in Kooperation mit dem Projekt „Ein Team gegen digitale Gewalt“

Vorbemerkung

Die Gesellschaft für Freiheitsrechte e.V. (GFF) verteidigt mit juristischen Mitteln die Grund- und Freiheitsrechte. Ein Themenschwerpunkt ist dem Thema Rechte im digitalen Zeitalter gewidmet. Um die Rechte im Netz effizienter durchzusetzen, hat die GFF das Center for User Rights gegründet, das Nutzer*innenrechte unter dem Digital Services Act (Gesetz über Digitale Dienste, Verordnung (EU) 2022/2065, DSA) durchsetzt. Das Projekt „Ein Team gegen digitale Gewalt“ schult seit 2023 Beratungsstellen und Frauenhäuser bundesweit zur technischen Sicherheit privater Kommunikationsmittel. Der Trägerverein Institut für Technik und Journalismus e.V. reagiert damit auf die seit Jahren bestehende Nachfrage nach Fortbildung im Unterstützungssystem.

Gegenstand der Beschwerde ist die Bewerbung von Stalking-Apps über Suchanzeigen der Beschwerdegegnerin. Suchanzeigen sind Anzeigen, welche die Beschwerdegegnerin durch das von ihr angebotene Online-Werbeprogramm „Google Ads“ im Rahmen der Google-Suchmaschine an Nutzer*innen der Google-Suche ausspielt. Durch das Ausspielen der Werbung verstößt die Beschwerdegegnerin gegen ihre Pflichten als sehr große Online-Suchmaschine (*very large online search engine*; im Folgenden VLOSE) nach dem Digital Services Act. Danach muss sie angemessene, verhältnismäßige und wirksame Maßnahmen treffen, um systemische Risiken zu mindern, die sich aus der Konzeption, dem Betrieb oder der Nutzung eines Dienstes ergeben (Art. 35 Abs. 1 i.V.m. Art. 34 DSA).

Mit Stalking-Apps können Einzelpersonen das Mobiltelefon einer anderen Person ohne deren Einwilligung heimlich überwachen und kontrollieren. So erlauben Stalking-Apps je nach Funktionalität das Mitlesen privater Kommunikation, das Aufzeichnen von Telefongesprächen und den Fernzugriff auf Kamera und Mikrofon. Nachweislich werden diese Apps dazu genutzt, geschlechtsspezifische Gewalt gegen Mädchen und Frauen auszuüben und zu erleichtern, insbesondere im Kontext von (Ex-)Partnerschaften, die von Missbrauch geprägt sind. Die Nutzung von Stalking-Apps ist in aller Regel rechtswidrig. Die Zahl der von Stalking-Apps Betroffenen steigt seit einiger Zeit. Auch wenn exakte Zahlen fehlen, dürften diese gleichwohl hoch sein. Darauf deuten Zahlen aus Daten-Leaks hin.

Im Rahmen unserer Recherchen sind wir auf zahlreiche ausgespielte Anzeigen einer Vielzahl verschiedener Anbieter*innen von Stalking-Apps gestoßen. Sie lassen sich sowohl im Ads Transparency Center der Beschwerdegegnerin als auch im Rahmen der Nutzung der Suchmaschine der Beschwerdegegnerin ohne Weiteres finden.

Die Beschwerdegegnerin erhöht über das Ausspielen der Werbung für Stalking-Apps an hervorgehobener Stellung entscheidend deren Auffindbarkeit und profitiert über die dafür erhobenen Gebühren unmittelbar davon. Sie veröffentlicht nicht nur rein passiv die von den Anbieter*innen erstellten Anzeigen, sondern trägt aktiv zur Erhöhung der Wirksamkeit und Reichweite der Anzeigen bei. So stellt sie KI-gestützte Produkte bereit und integriert sie sowohl in den Prozess des Erstellens als auch des Ausspielens von Suchanzeigen. Das begründet ein systemisches Risiko in Bezug auf geschlechtsspezifische Gewalt im Sinne des Art. 34 Abs. 1 UAbs. 2 Satz 2 lit. d DSA und hat darüber hinaus tatsächliche oder vorhersehbare nachteilige Auswirkungen auf die Ausübung der Grundrechte im Sinne des Art. 34 Abs. 1 UAbs. 2 Satz 2 lit. b DSA. Ihrer Risikominderungspflicht kommt die Beschwerdegegnerin nicht nach. Sie scheitert offenkundig bereits daran, die eigenen Werberichtlinien durchzusetzen, welche die Bewerbung der Stalking-Apps untersagen.

A. Sachverhalt

I. Funktionalität von Stalking-Apps

1 Die Beschwerde betrifft die Bewerbung sogenannter Stalking-Apps. Der Fachverband *Coalition against Stalkerware* definiert Stalkerware – die auch Stalking-Apps umfasst – als „Software, die für Privatpersonen frei oder käuflich verfügbar ist und mittels Remote-Steuerung eine Person in die Lage versetzt, Aktivitäten auf dem Gerät eines anderen Benutzers zu verfolgen, ohne dessen Zustimmung und ohne ausdrückliche, stete Benachrichtigung an diesen Benutzer zu senden.“[1]

2 Stalking-Apps umfassen typischerweise die folgenden Funktionen:

- SMS und Nachrichten mitlesen, die über Messenger-Dienste sowie Social Media-Dienste versendet werden;
- Telefonanrufe aufzeichnen;
- Kontaktlisten exportieren;
- Kalendereinträge überwachen;
- Fotos aufnehmen;
- Screenshots erstellen;
- Mobiltelefon orten;

[1] *Coalition against Stalkerware*, Informationen für Medien, https://stopstalkerware.org/de/informationen-fur-medien/ (abgerufen am 17.10.2024).

- Mikrofon aus der Ferne einschalten, um Gespräche abzuhören[2]

- Keylogging (Mitschneiden sämtlicher Tastatureingaben, also auch aller Passwörter).[3]

3 Die Kund*innen der Anbieter*innen von Stalking-Apps umgehen bei der Installation auf dem Zielgerät, meistens ein Mobiltelefon, in der Regel bewusst die Einwilligung der betroffenen Person. Da Stalking-Apps in der Regel nicht in der Liste installierter Applikationen angezeigt werden, können Betroffene sie in der Folge kaum erkennen.[4] Aber selbst wenn sie dort enthalten sind, werden sie durch „harmlose" Namen wie zum Beispiel „Sync Service" zwischen den anderen Applikationen versteckt.[5] Es handelt sich dabei um eine bewusst konzipierte Täuschungskomponente, die von vornherein bei der Entwicklung mitgedacht wird.

4 Nicht Gegenstand der Beschwerde ist die Bewerbung von so genannten Kinderschutz-Apps, auch wenn diese schwerwiegend in die Rechte der betroffenen Kinder und Jugendlichen eingreifen können. Eine Abgrenzung zu Stalking-Apps ist vor allem deshalb notwendig, weil Anbieter*innen von Stalking-Apps ihre Produkte auf Webseiten oft unter dem Deckmantel anbieten, dass die Apps (auch) zum Schutz von Kindern eingesetzt werden können. Kinderschutz-

---

2 *Kaspersky*, Stalkerware im Jahr 2023, Kaspersky Report, Februar 2024, S. 8, https://media.kasperskydaily.com/wp-content/uploads/sites/96/2024/03/08131849/The-State-of-Stalkerware-in-2023-DE.pdf?kaspr=stalkerware2023 (abgerufen am: 17.10.2024) (im Folgenden: Kaspersky Report 2023); *Huwiler/Oesch*, Ein Mann überwacht das Handy seiner Freundin mit einer iranischen Spyware. Dann knackt eine Schweizer Hackerin das System. Einblicke in einen lukrativen Markt, NZZ, 03.02.2024, https://www.nzz.ch/gesellschaft/wenn-der-schatz-auf-handy-mitliest-wie-eine-schweizerin-von-ihrem-partner-mit-iranischer-spyware-ausspioniert-wurde-ld.1775351 (abgerufen am 17.10.2024), (im Folgenden: NZZ Bericht zu Stalking-Apps 2024); *Coalition against Stalkerware*, What is stalkerware?, https://stopstalkerware.org/ (abgerufen am 17.10.2024).

3 Avira, Stalkerware verbreitet sich immer mehr. Schützen Sie sich davor, https://www.avira.com/de/blog/stalkerware-verbreitet-sich-immer-mehr-schuetzen-sie-sich-davor?srsltid=AfmBOoqQHj97qLP94Q8B83aX_RlJL3HOuoqogKDOnGyQSTZFr_VR4k6k (abgerufen am: 17.10.2024). S. beispielhaft MacTechNews, Spyware auf tausenden Geräten – auch Macs betroffen, https://www.mactechnews.de/news/article/Spyware-auf-tausenden-Geraeten-auch-Macs-betroffen-185337.html (abgerufen am: 17.10.2024).

4 Kaspersky Report 2023, S. 8.

5 Siehe beispielhaft PC Welt, So erkennen Sie Stalkerware auf dem Smartphone, https://www.pcwelt.de/article/1187394/so-erkennen-sie-stalkerware-auf-dem-smartphone.html (abgerufen am: 17.10.2024).

Apps lassen sich von Stalking-Apps über den beschränkten Kreis der Funktionalitäten abgrenzen. Laut einer Studie überwachen Eltern in erster Linie den Standort ihrer Kinder sowie den Schulweg und/oder die Bildschirmzeit.[6] 95 Prozent der befragten Eltern gaben an, dass ihre Kinder von der Überwachung wüssten.[7] Bei 41 Prozent der Befragten ist die Standortüberwachung gegenseitig, sodass auch die Kinder den Standort der Eltern nachverfolgen können.[8] Apps, die Eltern einsetzen, weisen somit deutlich weniger Funktionen auf und sind damit weniger invasiv. Zudem lassen sich genuine Kinderschutz-Apps auch darüber abgrenzen, dass die Installation in der Regel mit dem Wissen des betroffenen Kindes erfolgt und gegebenenfalls auf Gegenseitigkeit basiert. Eine App, deren Vorhandensein auf dem Zielgerät verschleiert wird, indem sie unter einem Tarnnamen in der Liste der Apps erscheint, steht dem deutlich entgegen. Anbieter*innen, die mit der *heimlichen* Überwachung der gesamten Online-Aktivitäten anderer Personen werben, richten sich de facto nicht an Eltern und fallen somit in den von der Beschwerde erfassten Bereich der Stalking-Apps.

II. Geschlechtsspezifische Dimension

5 Die Nutzung von Stalking-Apps hat eine geschlechtsspezifische Dimension. Das ergibt sich im Wesentlichen daraus, dass die überwiegende Zahl der Opfer von (Cyber-)Stalking **Frauen und Mädchen** sind, die überwiegende Zahl der Täter Männer (**1.**).

6 Die Mehrzahl der (Cyber-)Stalking-Fälle findet zudem in **Beziehungskontexten** statt: Entweder innerhalb einer noch bestehenden Beziehung oder begangen durch Ex-Partner*innen. Stalking-Apps erleichtern die Kontrolle der Partner*innen zum Zweck der Aufrechterhaltung einer von Missbrauch geprägten Beziehung

---

6 *Mavoa et al.*, "It's About Safety Not Snooping": Parental Attitudes to Child Tracking Technologies and Geolocation Data, 2023, Surveillance & Society, Ausgabe 21 Heft 1, S. 45 (49), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/15719/10611 (abgerufen am: 17.10.2024); *Mols et al.*, Family Surveillance: Understanding Parental Monitoring, Reciprocal Practices, and Digital Resilience, 2023, Surveillance & Society, Ausgabe 21 Heft 4, S. 469 (475 f.), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/15645/11067 (abgerufen am: 17.10.2024).

7 *Mavoa et al.*, "It's About Safety Not Snooping": Parental Attitudes to Child Tracking Technologies and Geolocation Data, 2023, Surveillance & Society, Ausgabe 21 Heft 1, S. 45 (50), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/15719/10611 (abgerufen am: 17.10.2024).

8 Ebd.

und ermöglichen weitere physische oder psychische Bedrohungen und Gewalttaten. Sie stellen damit ein maßgebliches Instrument zur Ausübung psychischer und physischer Gewalt gegen Frauen dar (**2.**).

1. Gender Gap im (Cyber-)stalking

7 Die Nutzung von Stalking-Apps lässt sich in den auch strafrechtlich relevanten Phänomenbereich des Cyberstalkings einordnen. In der EU-Richtlinie zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt wird Cyberstalking als eine moderne Form der Gewalt definiert, die sich häufig gegen Familienangehörige oder im selben Haushalt wie der Täter lebende Personen richtet, aber auch von früheren Partnern oder Bekannten verübt wird. Üblicherweise missbraucht der Täter dafür Technologien, um das Zwangs- und Kontrollverhalten, die Manipulation und die Überwachung zu intensivieren und so die Angst des Opfers zu verstärken und es allmählich von Freund*innen, Familienangehörigen und dem beruflichen Umfeld zu isolieren.[9]

8 Aus den für den Bereich des (Cyber-)Stalking erhobenen Zahlen ergibt sich eindeutig eine geschlechtsspezifische Dimension. Die Opfer von Stalking sind weit überwiegend weiblich, die Täter weit überwiegend männlich. Die Polizeiliche Kriminalstatistik für Deutschland weist etwa für das Jahr 2023 insgesamt 23.156 Fälle der strafbaren Nachstellung (§ 238 StGB) aus. Von den insgesamt 18.724 Tatverdächtigen waren 15.206 Männer.[10] In Deutschland wurden im Jahr 2021 wegen Nachstellung (§ 238 StGB) 778 Personen verurteilt, davon waren 689 männlich.[11] Die Zahlen decken sich mit einer Studie im Auftrag der „Weisser Ring Stiftung“. Danach liegt die Lebenszeitprävalenz (bezogen auf die Studienteilnehmer*innen), mindestens einmal im Leben von Stalking betroffen zu sein, bei weiblichen Personen bei 14,4 Prozent, während sie bei männlichen

---

9 Erwägungsgrund 21 der Richtlinie (EU) 2024/1385 des Europäischen Parlaments und des Rates vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt.

10 Polizeiliche Kriminalstatistik Bund 2023, Tabelle 01, Zeile 207, Spalte P bis R, (Anlage 1).

11 Statistisches Bundesamt, Strafverfolgung 2021, 29. November 2022, Fachserie 10, Reihe 3, S. 34, https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Strafverfolgung-Strafvollzug/strafverfolgung-2100300217004.pdf?__blob=publicationFile (abgerufen am: 17.10.2024).

Personen nur bei 5,1 Prozent liegt.[12] In 83,3 Prozent der Fälle waren weibliche Personen von Stalking betroffen.[13] In 93,6 Prozent der Fälle war den Opfern der Täter bekannt, wobei 45 Prozent der betroffenen weiblichen Personen von ihrem Ex-Partner gestalkt wurden.[14]

9 Das Europäische Institut für Gleichstellungsfragen hat im Jahr 2022 eine Studie über Cybergewalt gegen Frauen und Mädchen in der Europäischen Union veröffentlicht. [15] Darin wird die bisherige Studienlage zum Cyberstalking ausgewertet. Rund 80 Prozent der Stalking-Opfer sind Frauen, während 86 Prozent der Täter Männer sind.[16] Ganze 5 Prozent der Frauen in der EU haben seit ihrem 15. Lebensjahr Cyberstalking erlebt.[17] Cyberstalking tritt tendenziell am häufigsten im Kontext von Ex-Partnerbeziehungen auf.[18]

10 Dieser Gender Gap spiegelt sich im Rahmen der Verwendung von Stalking-Apps wider. Umfragewerte des Cybersicherheitsunternehmens *Norton* zeigen, dass deutlich mehr Männer Stalking-Apps einsetzen als Frauen. Dazu wurden in zehn Staaten Menschen befragt. In Deutschland wie auch in Frankreich gaben Männer

---

12 *Dreßing/Gass/Kühner* (Zentralinstitut für Seelische Gesundheit, Mannheim), Ergebnisse der Stalking-Studie 2018, Abschlussbericht, August 2019, S. 5, https://weisser-ring-stiftung.de/system/files/domains/weisser_ring_stiftung/downloads/praevalenzvonstalkingergebnisse2018.pdf (abgerufen am: 17.10.2024).

13 Ebd., S. 6.

14 Ebd., S. 9, 12.

15 European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (abgerufen am: 17.10.2024).

16 European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, S. 41, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (abgerufen am: 17.10.2024) unter Verweis auf *Logan*, Examining stalking experiences and outcomes for men and women stalked by (ex)partners and non-partners, Journal of Family Violence, 2020, Vol. 35, No 3, S. 729–739.

17 European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, S. 40, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (abgerufen am: 17.10.2024) unter Verweis auf European Union Agency for Fundamental Rights (FAR), Violence against Women: An EU-wide survey – Main results report, 2014, abrufbar unter https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf (abgerufen am 17.10.2024).

18 European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, S. 41, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (abgerufen am: 17.10.2024). unter Verweis auf *Dreßing et al.*: Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims, Cyberpsychology, Behavior, and Social Networking, 2014, Vol. 17, No 2, pp. 61–67.

doppelt so häufig wie Frauen an, invasive Apps wie Stalkerware zu verwenden, um Partner*innen auszuspionieren.[19] In den USA liegt die Wahrscheinlichkeit, dass Männer Stalking-Apps nutzen, dreimal so hoch wie bei Frauen.[20] Aus geleakten Datensätzen des Anbieters Flexispy ergibt sich, dass mindestens 80 Prozent der Kund*innen Männer sind.[21]

2. Stalking-Apps als Instrument physischer und psychischer Gewalt gegen Frauen

11 Stalking-Apps stellen ein maßgebliches Instrument zur Ausübung psychischer und physischer Gewalt gegen Frauen dar. Cyberstalking und insbesondere die Nutzung von Stalking-Apps sind in der Regel eingebunden in Beziehungskontexte, die von Belästigung, Missbrauch und anderen Formen physischer und psychischer Gewalt geprägt sind. Frauen sind von Gewalt durch (Ex-)Beziehungspartner überdurchschnittlich stark betroffen (**2.1**). Cyberstalking und andere Formen von Gewalt stehen in engem Zusammenhang (**2.2**). Vor diesem Hintergrund begünstigt die Nutzung von Stalking-Apps Gewalt gegen Frauen (**2.3**). Das Problem potenziert sich angesichts steigender Nutzer*innenzahlen (**2.4**).

2.1 Gewalt in (Ex-)Partnerschaften betrifft weit überwiegend Frauen

12 Gewalt in Beziehungskonstellationen stellt ein strukturelles Problem dar. In der deutlichen Mehrzahl der Fälle richtet sich die Gewalt gegen Frauen. So waren laut dem Bundeslagebild des Bundeskriminalamts zu sogenannter „häuslicher Gewalt“ in Deutschland im Jahr 2023 70,5 Prozent der Opfer weiblich und 75,6 Prozent der Tatverdächtigen männlich.[22] In der Unterkategorie der

---

[19] Norton Cyber Safety Insights Report, Special Release – Online Creeping, Resources, Germany, (Gender breakout), France (Gender breakout), 2021, https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report-special-release-online-creeping/ (abgerufen am 17.10.2024).

[20] Norton Cyber Safety Insights Report, Special Release – Online Creeping, Resources, US, Gender breakout, 2021, https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report-special-release-online-creeping/ (abgerufen am 17.10.2024).

[21] *Locker/Hoppenstedt*, Mehr als tausend Deutsche nutzen Spionage-App: "100 Prozent Erfolg - übermorgen ist meine Scheidung“, Vice, 04.05.2017, https://www.vice.com/de/article/ezjdbj/mehr-als-tausend-deutsche-nutzen-spionage-app-100-prozent-erfolg-uebermorgen-ist-meine-scheidung (abgerufen am 17.10.2024).

[22] Bundeskriminalamt, Bundeslagebild Häusliche Gewalt, 2023, V. 1.0, S. 4, (Anlage 2).

Partnerschaftsgewalt waren 79,2 Prozent der Opfer weiblich und 77,6 Prozent der Tatverdächtigen männlich. Die dabei verübten Delikte umfassten vor allem vorsätzliche Körperverletzungen mit 59,1 Prozent sowie Bedrohung, Stalking und Nötigung mit insgesamt 24,6 Prozent.[23] Diese geschlechterspezifische Aufteilung deckt sich mit den Ergebnissen US-amerikanischer Studien.[24]

2.2 Cyberstalking und andere Formen der Gewalt stehen in engem Zusammenhang

13 Die vom Europäischen Institut für Gleichstellungsfragen ausgewerteten Studien zeigen, dass sich Cyberstalking und physisches Stalking nicht trennen lassen, sondern häufig ineinander übergehen und ein Kontinuum bilden. Physisches Stalking ist ein Risikofaktor für Cyberstalking und umgekehrt kann Stalking, das online beginnt, in physische Handlungen münden oder zu anderen Formen von Cyber-Gewalt führen.[25] In über der Hälfte der Fälle des Cyberstalking (54 Prozent) soll nach einer britischen Studie die erste Begegnung mit dem Stalker offline stattgefunden haben.[26] In vielen Fällen ist Cyberstalking ein elementarer Faktor von Gewalt in Paarbeziehungen.[27] Daten aus einer Umfrage von 2014

---

[23] Ebd., S. 5.

[24] Vgl. US-Justizministerium (Statistikabteilung), Special Report: Intimate Partner Violence, 1993 - 2010, November 2012, überarbeitet am 29.9.2012, S. 1, https://bjs.ojp.gov/content/pub/pdf/ipv9310.pdf (abgerufen am: 17.10.2024); Office for Victims of Crime, Intimate Partner Violence, kein Veröffentlichungsdatum, S. 1, (Anlage 3); *Black, M.C. et al.*, The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, 2011, S. 2, 9, https://www.nsvrc.org/sites/default/files/2021-04/NISVS_Report2010-a.pdf (abgerufen am: 17.10.2024).

[25] European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, S. 40, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (abgerufen am: 17.10.2024) unter Verweis auf *Reyns/Fisher*, The Relationship between offline and online stalking victimisation: a gender-specific analysis, Violence and Victims, 2018, Vol. 33, No 4, pp. 769-786.

[26] European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, S. 40, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (abgerufen am: 17.10.2024) unter Verweis auf *Maple/Short/Brown,* Cyber Stalking in the United Kingdom: An analysis of the ECHO pilot survey, 2011, S. 14, https://uobrep.openrepository.com/bitstream/handle/10547/270578/ECHO_Pilot_Final.pdf?sequence=1&isAllowed=y (abgerufen am: 17.10.2024).

[27] European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, S. 40, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (abgerufen am: 17.10.2024) unter Verweis auf *Al-Alosi*, Cyber-violence: digital abuse in the context of domestic violence, University Of New South Wales Law Journal, Vol. 40, No 4, pp. 1573-1603.

zeigen, dass 7 von 10 Frauen, die Cyberstalking erlebt haben, auch mindestens eine Form von körperlicher und/oder sexualisierte Gewalt durch einen intimen Partner erlebt haben.[28]

14 Im Rahmen einer Untersuchung des Cybersicherheitsunternehmens *Kaspersky*[29] gaben 23 Prozent von insgesamt 21.000 Befragten aus 21 Ländern an, dass sie in irgendeiner Form Cyberstalking durch eine Person erlebt haben, mit der sie kürzlich zusammen waren. Mehr als ein Drittel (39 Prozent) der Befragten berichtete über Erfahrungen mit Gewalt oder Missbrauch durch eine*n aktuelle*n oder frühere*n Partner*in. Zehn Prozent der Umfrageteilnehmer*innen gaben an, dass ihr Standort verfolgt wurde, weitere zehn Prozent stellten bereits unbefugten Zugriff auf ihre Social-Media-Konten oder E-Mails fest, und bei sieben Prozent der Befragten wurde schon Stalker-Software ohne ihr Wissen auf ihrem Gerät installiert.

2.3 Stalking-Apps als wesentlicher Teil von Gewalt gegen Frauen

15 Stalking-Apps spielen in diesem Zusammenhang eine entscheidende Rolle. Die Nutzung von Stalking-Apps begünstigt die Überwachung der Beziehungspartner*innen, deren Belästigung, Missbrauch sowie Stalking in anderen Formen und/oder Gewalt.[30]

16 Stalking-Apps stellen weltweit ein seit mehreren Jahren bekanntes Phänomen im Rahmen der Ausübung von Gewalt gegen Frauen dar. In Deutschland waren nach dem Bundesverband Frauen gegen Gewalt e.V. von 176 Frauenberatungsstellen und Frauennotrufen bereits im Jahr 2016 nahezu alle mit dem Problem von Stalking-Apps konfrontiert.[31] Expert*innen aus Beratungsstellen berichten, dass

---

[28] European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, S. 40, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (abgerufen am: 17.10.2024) unter Verweis auf European Union Agency for Fundamental Rights (FAR), Violence against Women: An EU-wide survey – Main results report, 2014, abrufbar unter https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf (abgerufen am 17.10.2024).

[29] Kaspersky Report 2023, S. 9.

[30] *Coalition against Stalkerware*, Informationen für Technologieunternehmen, https://stopstalkerware.org/de/informationen-fur-technologieunternehmen/ (abgerufen am: 17.10.2024).

[31] *Locker/Hoppenstedt*, Mehr als tausend Deutsche nutzen Spionage-App: "100 Prozent Erfolg - übermorgen ist meine Scheidung“, Vice, 04.05.2017, https://www.vice.com/de/article/ezjdbj/mehr-als-tausend-deutsche-nutzen-spionage-app-100-prozent-erfolg-uebermorgen-ist-meine-scheidung (abgerufen am 17.10.2024).

solche verdeckt arbeitenden Apps in den vergangenen Jahren zu einer massiven Bedrohung für die Sicherheit ihrer Klient*innen geworden seien.[32]

17 Zahlen aus anderen Ländern stützen den Befund. Laut dem in den USA ansässigen *National Network to End Domestic Violence* überwachen 71 Prozent der „häuslichen Gewalttäter*innen“ die Computeraktivitäten ihrer Opfer und 54 Prozent die Mobiltelefone mittels Stalking-Apps. [33] Eine Umfrage des australischen *Domestic Violence Resources Centre Victoria* aus dem Jahr 2013 ergab, dass 82 Prozent der Missbrauchsopfer auch von Missbrauch unter Nutzung von Smartphones berichteten, während 74 Prozent der befragten Praktiker*innen berichteten, dass die Verfolgung über Apps bei ihrer Klientel häufig vorkommt.[34]

18 In Kanada ergab eine Befragung unter Anti-Gewalt-Helfer*innen für das Jahr 2012, dass 98 Prozent der Täter*innen Technologie nutzen, um ihre Opfer einzuschüchtern oder zu bedrohen, 72 Prozent der Täter*innen die E-Mail- und Social-Media-Konten der betroffenen Frauen und Mädchen gehackt hatten, dass weitere 61 Prozent Computer gehackt hatten, um Online-Aktivitäten zu überwachen und Informationen zu extrahieren und weitere 31 Prozent Computerüberwachungssoftware installiert hatten.[35]

19 Cyberstalking und damit auch die Nutzung von Stalking-Apps stellt daher kein isoliertes Problem dar, das nur Auswirkungen in der „virtuellen“ Welt hat. Vielmehr kann die damit verbundene Überwachung auch zu physischer Gewalt führen. Allein etwa dadurch, dass Täter*innen der genaue Standort des Opfers bekannt ist und aus beispielsweise Textnachrichten ersichtlich ist, ob sich Frauen allein an einem bestimmten Ort aufhalten, werden physische Übergriffe ermöglicht und

---

[32] *Köver*, Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung, 2021, S. 227 (228), https://www.transcript-verlag.de/shopMedia/openaccess/pdf/oa9783839452813.pdf (abgerufen am: 17.10.2024).

[33] *Citizen Lab*, The Predator in your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry, Research Report Nr. 119, Juni 2019 (im Folgenden: Citizen Lab Stalkerware Studie 2019), S.1, https://citizenlab.ca/docs/stalkerware-holistic.pdf (abgerufen am: 17.10.2024) unter Verweis auf *Citron*, Spying Inc., 2015, Washington and Lee Law Review, Vol. 72, No 3, pp. 1243-1282.

[34] *Citizen Lab* Stalkerware Studie 2019, S.1 unter Verweis auf *Woodlock*, Technology-facilitated Stalking: Findings and Recommendations from the SmartSafe Project, SmartSafe, 2014.

[35] *Citizen Lab* Stalkerware Studie 2019, S.1 unter Verweis auf *Safety Net Canada,* Assessing Technology in the Context of Violence Against Women & Children: Examining Benefits & Risks, British Columbia Society of Transition Houses, 2013, S. 6, 71.

begünstigt. Dazu kommen ebenso reale Auswirkungen auf die Psyche der Betroffenen wie Angstzustände oder Depressionen.[36]

2.4 Steigende Zahlen von Stalking-Apps Betroffener

20 Die Nutzer*innenzahlen von Stalking-Apps steigen und dementsprechend die Gefahr, mit einer Stalking-App überwacht zu werden.

21 Exakte Zahlen etwa zu Downloads aus den großen App-Stores fehlen zwar. Die Anbieter*innen von Stalking-Apps wählen in der Regel nicht diesen Vertriebsweg bzw. können ihn (im Vergleich zu weniger invasiven Kindersicherungen) nicht wählen (siehe dazu **A.III.**). Zudem bleibt die Nutzung der Apps entsprechend ihres Anwendungszwecks häufig unbemerkt. Selbst wenn die betroffene Person die Nutzung bemerkt, stellt sie nicht in allen Fällen eine Strafanzeige. Die Anzahl der von der heimlichen Nutzung von Stalking-Apps betroffenen Personen als auch die Anzahl der Täter*innen dürfte gleichwohl hoch sein. Darauf deuten im Rahmen von Daten-Hacks und -Leaks der Anbieter*innen von Stalking-Apps bekannt gewordene Daten hin. Von dem Anbieter *mSpy* waren beispielsweise über 2 Millionen Datensätze öffentlich zugänglich. Die Datensätze enthielten unter anderem iCloud-Benutzernamen und -Passwörter der Betroffenen, SMS, Standortdaten und Daten der Anrufer*innen.[37] Insgesamt wurden im Jahr 2023 von einem Cybersicherheitsunternehmen 195 verschiedene Stalking-Apps entdeckt.[38]

22 Die Gefahr, mittels einer Stalking-App überwacht zu werden, ist in den letzten Jahren weltweit wie auch in Deutschland stark gestiegen. Das legen Zahlen nahe, die Cybersicherheitsunternehmen veröffentlicht haben. Demnach waren 2023 weltweit insgesamt 31.031 einzelne Nutzer*innen von Stalking-Apps betroffen.

---

[36] *Short/Linford/Wheatcroft/Maple*, The Impact of Cyberstalking: The Lived Experience – A Thematic Analysis, 2014, Studies in Health Technology and Informatics, Vol. 199, pp. 133-137; *Logan*, Examining Stalking Experiences and Outcomes for Men and Women Stalked by (Ex)partners and Non-partners, 2019, Journal of Family Violence, Vol. 35, pp. 729-739.

[37] *Krebs*, Krebs on Security: For 2nd Time in 3 Years, Mobile Spyware Maker mSpy Leaks Millions of Sensitive Records, 04.09.2018, https://krebsonsecurity.com/2018/09/for-2nd-time-in-3-years-mobile-spyware-maker-mspy-leaks-millions-of-sensitive-records/ (abgerufen am: 17.10.2024); Techcrunch: Mobile spyware maker leaks 2 million records, 05.09.2018, https://techcrunch.com/2018/09/05/mobile-spyware-maker-leaks-2-million-records/ (abgerufen am: 17.10.2024).

[38] Kaspersky Report 2023, S. 8.

Das entspricht einem Anstieg gegenüber 2022 von 5,86 Prozent. Spitzenreiter in Europa ist Deutschland.[39] Der Trend steigender Nutzer*innenzahlen besteht schon länger: Die Zahl hat sich nach Angaben von Cybersicherheitsunternehmen bereits im Zeitraum von Januar 2020 bis Dezember 2022 drastisch erhöht, weltweit um 239 Prozent und speziell in Deutschland um 575 Prozent.[40]

III. Verbot der Bewerbung von Stalking-Apps durch die Beschwerdegegnerin

23 Im August 2020 hat die Beschwerdegegnerin ihre Werberichtlinien zur „Ermöglichung von unlauterem Verhalten“ angepasst.[41] Seitdem verbietet die Beschwerdegegnerin in ihren Werberichtlinien ausdrücklich das Bewerben von „Produkte[n] oder Dienstleistungen, mit denen andere Personen oder ihre Aktivitäten ohne deren Einwilligung beobachtet bzw. überwacht werden können“. Insbesondere umfasst das Verbot „Spyware und Technologien zur Kontrolle von Beziehungspartnern, insbesondere Spyware oder Malware, mit der Nutzer Textnachrichten, Telefonanrufe oder Browserverläufe überwachen können“.[42]

24 Überwachungs-Apps, die sich auf dem Smartphone verstecken, verstoßen außerdem gegen die Richtlinien des Google Play Stores, der Vertriebsplattform für Anwendungssoftware.[43] Auch Apple, der maßgebliche Wettbewerber der Beschwerdegegnerin in Bezug auf den Betrieb von App-Stores, lässt solche Apps

---

39 Kaspersky Report 2023, S. 3, 6.

40 *Avast*, Stalkerware wächst deutschlandweit um 575 Prozent in den letzten drei Jahren, 14.03.2023, https://press.avast.com/de-de/stalkerware-wachst-deutschlandweit-um-575-prozent-in-den-letzten-drei-jahren (abgerufen am: 17.10.2024); *Avast*, Stalkerware Grows 239% Worldwide Over the Past Three Years, 14.03.2023, https://investor.gendigital.com/news/news-details/2023/Stalkerware-Grows-239-Worldwide-Over-the-Past-Three-Years/default.aspx (abgerufen am: 17.10.2024).

41 *Google*, Aktualisierung der Richtlinie zur Ermöglichung von unlauterem Verhalten, August 2020, https://support.google.com/adspolicy/answer/9726908?hl=de&sjid=4462208304556098119-EU (abgerufen am: 17.10.2024).

42 Google Ads Werberichtlinien: Ermöglichung unlauteren Verhaltens, 2024, https://support.google.com/adspolicy/answer/6016086?hl=de&sjid=5524670563677541947-EU, (abgerufen am: 17.10.2024).

43 Vgl. Google Play-Richtlinie zu Malware, https://support.google.com/googleplay/android-developer/answer/9888380?#stalkerware (abgerufen am 31.10.2024).

– mit Ausnahme von Überwachungsapps, die sich an Eltern richten – nicht in seinem App Store zu.[44]

IV. Die Bewerbung von Stalking-Apps über das Werbeprogramm der Beschwerdegegnerin

25 Trotz des Verbots in den Werberichtlinien der Beschwerdegegnerin finden sich Anzeigen der Anbieter*innen von Stalking-Apps und ihre Produkte ohne Aufwand über die Suchmaschine der Beschwerdegegnerin bei Eingabe der einschlägigen Suchbegriffe. Die Beschwerdegegnerin unterstützt die werbenden Anbieter*innen von Stalking-Apps im Rahmen ihrer allgemeinen Angebote an Werbetreibende bei der Buchung und Gestaltung der Werbeanzeigen (dazu **1.**). Die Werbung über bei der Beschwerdegegnerin gebuchte Anzeigen ist maßgeblich für die Auffindbarkeit von Apps und Stalking-Apps im Speziellen (dazu **2.**). Tatsächlich buchen Anbieter*innen von Stalking-Apps Werbeanzeigen bei der Beschwerdegegnerin im erheblichen Ausmaß. Davon hat die Beschwerdegegnerin Kenntnis (dazu **3.**).

1. Ablauf der Bewerbung über das Werbeprogramm der Beschwerdegegnerin

26 Die Bewerbung über das Werbeprogramm der Beschwerdegegnerin funktioniert wie folgt: Mittels eines Google Ads-Kontos legen die Werbenden unter anderem Text und Beschreibung der Anzeige, die Zielgruppe sowie die Suchbegriffe („Keywords“) fest, bei denen die Auslieferung der Anzeige erfolgen soll. Typische Suchbegriffe, die zu einschlägigen Treffern führen, sind etwa „Partner Handy überwachen“ oder „freundin handy überwachen“. Geben Nutzer*innen der Suchmaschine Suchbegriffe in die Suchleiste ein, die mit den von den Werbetreibenden festgelegten Keywords übereinstimmen, zeigt die Beschwerdegegnerin die Anzeigen gesondert gekennzeichnet vor und zwischen den organischen Suchergebnissen an. Dabei können die Werbenden sowohl bei der Anzeigenerstellung als auch bei der Anzeigenauslieferung auf automatisiert arbeitende KI-Programme der Beschwerdegegnerin zurückgreifen. Diese Programme schlagen unter anderem geeignete Anzeigentexte und -titel sowie

---

[44] *Apple*, App-Prüfungsrichtlinien: 5.1.1 Datenerfassung und -speicherung, lit. viii., April 2024, S. 33, https://developer.apple.com/support/downloads/terms/app-review-guidelines/App-Review-Guidelines-20240913-German.pdf (abgerufen am: 17.10.2024).

Suchbegriffe vor und erstellen bei der Eingabe der Suchbegriffe automatisiert auf die jeweilige Suchanfrage abgestimmte personalisierte Anzeigen. Hierdurch steigert die Beschwerdegegnerin selbst durch ihr eigenes zusätzliches Angebot die Effektivität und Reichweite der Anzeigen erheblich.

27 Dazu im Einzelnen:

1.1 Die Festlegung von Suchbegriffen

28 Um Produkte wie etwa Stalking-Apps über Google Ads zu bewerben, müssen die jeweiligen Anbieter*innen in einem für diesen Zweck erstellten Google Ads-Konto unter anderem neben dem Text der Anzeige, der geografischen Eingrenzung der Kampagne, der Zielgruppe und dem Budget bestimmte Suchbegriffe festlegen, bei denen die Auslieferung der Anzeige erfolgen soll. Dabei können die Werbenden nicht nur selbst erdachte Suchbegriffe festlegen, sondern sich entsprechende Suchbegriffe auch von einem KI-gestützten Programm der Beschwerdegegnerin vorschlagen lassen, dem sogenannten „Keyword-Planer“. Das Programm generiert auf Basis entweder der Inhalte der vom Werbenden angegebenen Webseite oder der manuell durch den Werbenden bereits eingegebenen Suchbegriffe automatisiert neue passende Suchbegriffe, bei denen die Werbung für die Nutzer*innen der Suchmaschine der Beschwerdegegnerin angezeigt werden sollen. Die so generierten Suchbegriffe kann der Werbende dann zu seiner Werbekampagne hinzufügen.[45]

29 Auch unabhängig von der gesonderten Nutzung des Tools *Keyword-Planer* nutzt die Beschwerdegegnerin bereits im regulären Erstellungsprozess der Anzeige die vom Werbenden angegebenen Informationen zur Zielgruppe der Werbekampagne als Basis dafür, weitere Suchbegriffe zu empfehlen, um die Reichweite der Anzeige zu erhöhen.[46]

---

[45] *Google*, Google Ads Hilfe: Keyword-Planer, 2024, https://support.google.com/google-ads/answer/7337243?hl=de&sjid=16595194781768165231-EU#zippy=%2Ca-ideen-f%C3%BCr-neue-keywords-abrufen (abgerufen am: 17.10.2024).

[46] *Google*, Ihre erste Google Ads-Kampagne einrichten, kein Veröffentlichungsdatum, https://ads.google.com/intl/de_de/home/how-it-works/, (abgerufen am: 17.10.2024).

1.2 Die Festlegung von Anzeigentexten

30 Nach Festlegung der Suchbegriffe müssen die Werbenden die Anzeige selbst erstellen. Die Beschwerdegegnerin unterstützt die Werbenden dabei, eine möglichst zielgerichtete Anzeige über ihre Oberfläche zu schalten. Aktiviert der Werbende die Funktion „Responsive Search Ads“, schlägt ein KI-basiertes Programm der Beschwerdegegnerin nach Angabe der URL des Werbenden auch Anzeigenüberschriften und Anzeigenbeschreibungstexte automatisiert vor, die potenziell zum Inhalt der unter der URL abrufbaren Inhalte passen. Dabei greift das Programm auf Inhalte zurück, die nach der Erfahrung der KI besonders gut bei den Nutzer*innen der Suchmaschine Anklang finden. Werbende können diese für die Erstellung der Anzeige auswählen. In der Regel werden hier mehrere verschiedene Anzeigenüberschriften und Beschreibungstextzeilen von den Werbenden angegeben.[47]

1.3 Die Auswahl der effektivsten Text- und Titelkombination im Verlauf der jeweiligen Suche mittels „Responsive Search Ads“

31 Die Anzeige der so gebuchten Werbung ist für die jeweiligen Nutzer*innen der Suchmaschine nicht statisch. Die Anzeigen stehen mit Beendigung des Erstellungsprozesses noch nicht fest, sondern werden erst mit der Eingabe des Suchbegriffs neu für jede suchende Person generiert. So kombiniert die Beschwerdegegnerin die von den Werbenden ausgewählten Überschriften und Beschreibungen zu einer individuellen Anzeige zeitgleich während der Suche. Mit der KI-basierten Funktion „Responsive Search Ads“ wählt das Programm der Beschwerdegegnerin basierend auf der Analyse des bisherigen Verhaltens der suchenden Person automatisiert diejenige Anzeigenüberschrift und -beschreibung aus, welche dem Interesse der suchenden Nutzer*innen am nächsten kommt. Nur diese individuell angepasste Suchanzeige zeigt sie den Nutzer*innen an. Dadurch erhöht die Beschwerdegegnerin die Wahrscheinlichkeit, dass ihre Nutzer*innen auf die Anzeige klicken. Sucht ein*e Nutzer*in der Suchmaschine etwa nach „Laufschuhen“ soll nach einem erläuternden Beispiel der Beschwerdegegnerin ihr KI-Programm nun aus den von den Werbenden angegebenen Optionen für Überschriften die zum vorherigen

---

[47] *Google,* Google Ads: Responsive Search Ads. A Guide to Writing Ads that Perform, Kein Veröffentlichungsdatum, S. 6, https://services.google.com/fh/files/misc/responsive_search_ads_a_guide_to_writing_ads_that_perform_2023.pdf (abgerufen am: 17.10.2024).

Suchverhalten passende Überschrift angezeigt werden (etwa „Marathon Schuhe“ statt „Schuhe zum Sprinten“, wenn zuvor nach „Beste Orte für einen Marathonlauf“ gesucht wurde).[48]

2. Maßgeblichkeit der Bewerbung für die Auffindbarkeit von Stalking-Apps

32 Die Bewerbung über die Suchmaschine der Beschwerdegegnerin ist entscheidend für die Auffindbarkeit der Stalking-Apps für ihre Nutzer*innen. Das folgt aus dem Zusammenspiel mehrerer Faktoren:

- Da Stalking-Apps sowohl aus Apples App Store als auch dem Google Play Store der Beschwerdegegnerin und damit den zentralen Vertriebswegen für Smartphone-Apps verbannt sind (siehe oben unter **A.III.**), wirken sich Online-Werbung und Suchanzeigen maßgeblich auf App-Installationen aus (**2.1**).

- Die Marktmacht der Beschwerdegegnerin führt dazu, dass Stalking-Apps durch die Bewerbung über ihre Suchmaschine einem sehr großen Kreis von Personen zugänglich gemacht werden, die diese Apps ansonsten nicht oder nur schwer aufgefunden hätten (**2.2**).

- Stalking-Apps wären ohne die Ausspielung von Werbeanzeigen durch die Beschwerdegegnerin über organische Suchergebnisse nicht in gleichem Ausmaß auffindbar (**2.3**).

2.1 Wirkung von Online-Werbung und Suchanzeigen auf App-Installationen

33 Einer Studie zufolge finden 40 Prozent der Nutzer*innen neue Apps über Suchmaschinen. Damit stehen Suchmaschinen an zweiter Stelle direkt hinter der Nutzung von App Stores (46 Prozent).[49] In dieselbe Richtung weist eine Umfrage

---

[48] Vgl. *Google*, Google Ads: Unlock the Power of Search. Inside Google AI-powered ads, kein Veröffentlichungsdatum, S. 8 und 24 https://services.google.com/fh/files/misc/unlock_the_power_of_search_2022.pdf (abgerufen am: 17.10.2024).

[49] *Marketing Charts*, Here’s How US Adults Discover Apps, and Why They Keep Using Them, 13.06.2024, https://www.marketingcharts.com/digital/mobile-phone-229739 (abgerufen am: 17.10.2024).

der Beschwerdegegnerin: Sie kommt zu dem Ergebnis, dass 31 Prozent der Nutzer*innen über Online-Werbeanzeigen während des Surfens im Internet auf neue Apps aufmerksam werden und 21 Prozent über Suchmaschinen.[50]

34 Für Unternehmen spielt Online-Werbung eine entscheidende Rolle. Im Jahr 2023 hatte Onlinewerbung in Deutschland einen Anteil von 49,7 Prozent am Gesamtnettoumsatz aller Werbeträger (umfassend unter anderem Print, Fernsehen etc.). [51] Sie wirkt sich auf Unternehmensumsätze und den Unternehmenswert deutlich positiver aus als Offline-Werbung.[52] Dabei bestehen Unterschiede auch zwischen den verschiedenen Formen der Online-Werbung. So führt das hier interessierende *paid search advertising*, also bezahlte Werbeanzeigen, die bei bestimmten Suchbegriffen parallel zu organischen Ergebnissen einer Suchmaschine angezeigt werden (Search-Ads), gegenüber *online display advertising* zu weit höheren Umsatzsteigerungen. Letzteres bezeichnet Werbung durch Werbebanner, mit Texten, Medieninhalten oder durch Werbevideos (Display-Ads). [53] Das spiegelt sich in der wirtschaftlichen Entwicklung des Werbemarkts insgesamt wider: Die Nettowerbeeinnahmen über Search-Ads stiegen im Jahr 2023 um 11,8 Prozent, während Display-Ads ein Wachstum von lediglich 6,4 Prozent aufwiesen.[54] Die Beschwerdegegnerin soll laut einem Bericht im ersten Quartal 2024 circa 46 Millionen US-Dollar mit „Google search & other“ eingenommen haben.[55] Es ist davon auszugehen, dass ein Großteil aus Werbeeinnahmen stammt.

---

[50] *Google*, How people discover, use, and stay engaged with apps, Oktober 2016, S. 5, https://www.thinkwithgoogle.com/_qs/documents/331/how-users-discover-use-apps-google-research.pdf (abgerufen am: 17.10.2024).

[51] *ZAW*, Werbemarkt nach Medien, kein Veröffentlichungsdatum, https://zaw.de/branchendaten/werbemarkt-nach-medien/ (abgerufen am: 17.10.2024).

[52] *Bayer, E. et al*.: The impact of online display advertising and paid search advertising relative to offline advertising on firm performance and firm value, In: International Journal of Research in Marketing, Dezember 2020, Ausgabe 37, Heft 4, S. 789 (S. 790, 801) (Anlage 4).

[53] Ebd., S. 801.

[54] Vgl. *ZAW*, Werbemarkt nach Medien, kein Veröffentlichungsdatum, https://zaw.de/branchendaten/werbemarkt-nach-medien/ (abgerufen am: 17.10.2024), (11,8 Prozent gegenüber 6,4 Prozent-Wachstum bei “Display Ads” inkl. Video-Streaming).

[55] Alphabet Investor Relations, Alphabet Announces First Quarter 2024 Results, S. 2, https://abc.xyz/assets/91/b3/3f9213d14ce3ae27e1038e01a0e0/2024q1-alphabet-earnings-release-pdf.pdf (abgerufen am 17.10.2024).

2.2 Erhöhte Zugangsmöglichkeiten aufgrund der Marktmacht der Beschwerdegegnerin

35 In diesem Kontext kommt der Beschwerdegegnerin eine enorme Marktmacht zu. Im Zeitraum vom 1. Januar 2024 bis zum 30. Juli 2024 hatte die Online-Suchmaschine der Beschwerdegegnerin basierend auf den mit ihrem Google-Account eingeloggten Nutzer*innen monatlich durchschnittlich 377.400.000 Nutzer*innen. Basierend auf unterscheidbaren Sitzungen von nicht eingeloggten Nutzer*innen hatte sie eine durchschnittliche monatliche Anzahl von 448.000.000 Nutzer*innen.[56]

36 Weltweit kommt die Online-Suchmaschine der Beschwerdegegnerin auf einen Marktanteil von 79,62 Prozent hinsichtlich der Nutzung von Suchmaschinen auf dem Desktop, auf Mobilgeräten sogar auf einen weltweiten Marktanteil von 94,08 Prozent.[57] Erst kürzlich hat dementsprechend etwa ein US-amerikanisches Gericht in einem kartellrechtlichen Streit geurteilt, dass die Beschwerdegegnerin mit ihrer Suchmaschine eine Monopolstellung aufrechterhalte.[58]

2.3 Keine gleichwertige Auffindbarkeit ohne das Ausspielen der Werbeanzeigen durch die Beschwerdegegnerin

37 Stalking-Apps wären ohne die Werbeanzeigen der Beschwerdegegnerin als organische Suchergebnisse zu einschlägigen Suchbegriffen nicht in gleichem Ausmaß auffindbar, wie sie es derzeit sind. Organische Suchergebnisse zu einschlägigen Suchbegriffen verweisen überwiegend auf vertrauenswürdige Quellen, die Nutzer*innen über die Gefahren von Stalking-Apps aufklären.

38 Denn bislang existiert nicht die eine etablierte und damit auch ohne Bewerbung ausreichend bekannte App. Darüber hinaus wechselt ein Teil der Anbieter*innen

---

[56] *Google*, Information about Monthly Active Recipients under the Digital Services Act (EU), 16.08.2024, S. 2, https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-24_2024-1-1_2024-6-30_en_v1.pdf (abgerufen am: 17.10.2024).

[57] *Statista Research Department*: Marktanteile der Suchmaschinen weltweit nach mobiler und stationärer Nutzung im September 2024, 02.10.2024 https://de.statista.com/statistik/daten/studie/222849/umfrage/marktanteile-der-suchmaschinen-weltweit/ (abgerufen am: 17.10.2024).

[58] The New York Times, 05.08.2024, https://www.nytimes.com/interactive/2024/08/05/technology/google-antitrust-ruling.html (abgerufen am: 17.10.2024).

regelmäßig die Namen – etwa von „SpyHide“ zu „oospy“.[59] Hinzu kommt, dass die Namen der Stalking-Apps selbst häufig generisch sind und ohne größere Alleinstellungsmerkmale („uMobix“, „mektabyt“). Das erschwert eine Auffindbarkeit der Webseiten der Anbieter*innen. Somit werden Stalking-Apps regelmäßig nicht über die Suche nach einem bestimmten Namen der App gefunden. Vielmehr suchen Nutzer*innen mit allgemeineren oder kontextualisierten Begriffen, wie beispielsweise „handy freundin überwachen“. Bei Eingabe dieser und entsprechender Suchbegriffe werden priorisiert und noch vor den organischen Suchergebnissen Werbeanzeigen ausgespielt. Das führt dazu, dass Stalking-Apps sofort gefunden werden, während die Webseiten der Anbieter*innen – wenn überhaupt – erst in nachrangigen Suchergebnissen auftauchen.

3. Von der Suchmaschine der Beschwerdegegnerin angezeigte Werbeanzeigen für Stalking-Apps

39 Die der Beschwerde zugrunde liegende Recherche hat ergeben, dass die Beschwerdegegnerin über ihre Suchmaschine eine Vielzahl von Werbeanzeigen für Stalking-Apps ausspielt. Sie hat seit vielen Jahren aktive Kenntnis von der Schaltung der Werbeanzeigen von Betreiber*innen von Stalking-Apps. Trotzdem kann festgestellt werden, dass die Beschwerdegegnerin nach wie vor eine Bewerbung dieser Apps entgegen den eigenen Richtlinien ermöglicht.[60]

40 Für die Recherche wurden zwei methodische Anknüpfungspunkte gewählt. Zum einen lässt sich über die Suchmaschine der Beschwerdegegnerin mit kontextualisierten Begriffen suchen. Zum anderen lässt sich über das Werbearchiv der Beschwerdegegnerin nachvollziehen, welche Anzeigen die Beschwerdegegnerin in einem bestimmten Zeitfenster ausgespielt hat.

---

[59] NZZ Bericht zu Stalking-Apps 2024; vgl. *Köver*, Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung, 2021, S. 227 (234 f.), https://www.transcript-verlag.de/shopMedia/openaccess/pdf/oa9783839452813.pdf (abgerufen am: 17.10.2024).

[60] Siehe auch *Williams,* in: MIT Technology Review, Google is failing to enforce its own ban on ads for stalkerware, 12.05.2022, https://www.technologyreview.com/2022/05/12/1052125/google-failing-stalkerware-apps-ads-ban/ (abgerufen am: 17.10.2024).

41 Mit der Einrichtung des Werbarchivs[61], dem *Ads Transparency Center*, kommt die Beschwerdegegnerin ihrer entsprechenden Pflicht aus dem Digital Services Act nach. Art. 39 DSA verpflichtet sie als VLOSE ein Werbearchiv einzurichten. Art. 39 Abs. 2 DSA benennt die Angaben, die mindestens enthalten sein müssen. Darunter befindet sich die Gesamtzahl der erreichten Nutzer*innen. In den Einträgen des Werbearchivs der Beschwerdegegnerin können je ausgespielter Anzeige die jeweiligen Zielgruppen der Werbung sowie das Ausmaß der Sichtbarkeit nachvollzogen werden. Dort wird insbesondere dokumentiert, wie oft eine Anzeige insgesamt auf den Plattformen der Beschwerdegegnerin ausgespielt wurde, aufgeschlüsselt nach Auslieferungsort der Anzeige. Allerdings setzt eine Recherche im Werbearchiv voraus, dass der Name der Werbetreibenden bekannt ist. Da es eine Vielzahl von Stalking-App Anbieter*innen gibt, ist eine abschließende Recherche über das Werbearchiv kaum möglich. Folglich sind auch die nachfolgenden Ergebnisse keinesfalls abschließend. Allein dieser Ausschnitt verdeutlicht aber, dass und in welchem Umfang diese Anzeigen ausgespielt werden.

42 Hinzu kommt, dass nach den Recherche-Ergebnissen Anzeigen tatsächlich ausgespielt wurden, die sich nicht im Werbearchiv finden lassen. Laut Angaben der Beschwerdegegnerin[62] kann dies daran liegen, dass es bis zu 72 Stunden dauert, bis Informationen über die Anzeige verfügbar sind. Weitere Gründe für das Fehlen der Anzeige im Werbearchiv können sein, dass die Anzeige wegen eines Richtlinienverstoßes bereits entfernt, in den letzten 365 Tagen nicht ausgespielt wurde oder nur eine von vielen Varianten der Werbeanzeige sei. Dennoch zeigte etwa das Auffinden der Anzeige vom Stalking-App-Anbieter „mekatbyt.com“ im Laufe der Recherche Gegenteiliges. Auch drei Tage später war die Anzeige nach erneuter Suche nicht im Werbearchiv aufzufinden. Fraglich ist, ob dies an technischen Einschränkungen der Anzeige liegt, allerdings ist das mit Blick auf die Art der Anzeige eher fernliegend (vgl. **Anlage 23.1**).

43 Im Rahmen der Recherche konnte für folgende Stalking-Apps nachgewiesen werden, dass die Beschwerdegegnerin Anzeigen ausgespielt hat: uMobix, mSpy, Spynger, ClevGuard, SpyX, Haqerra, spyera, Spytech SpyAgent, GuardW,

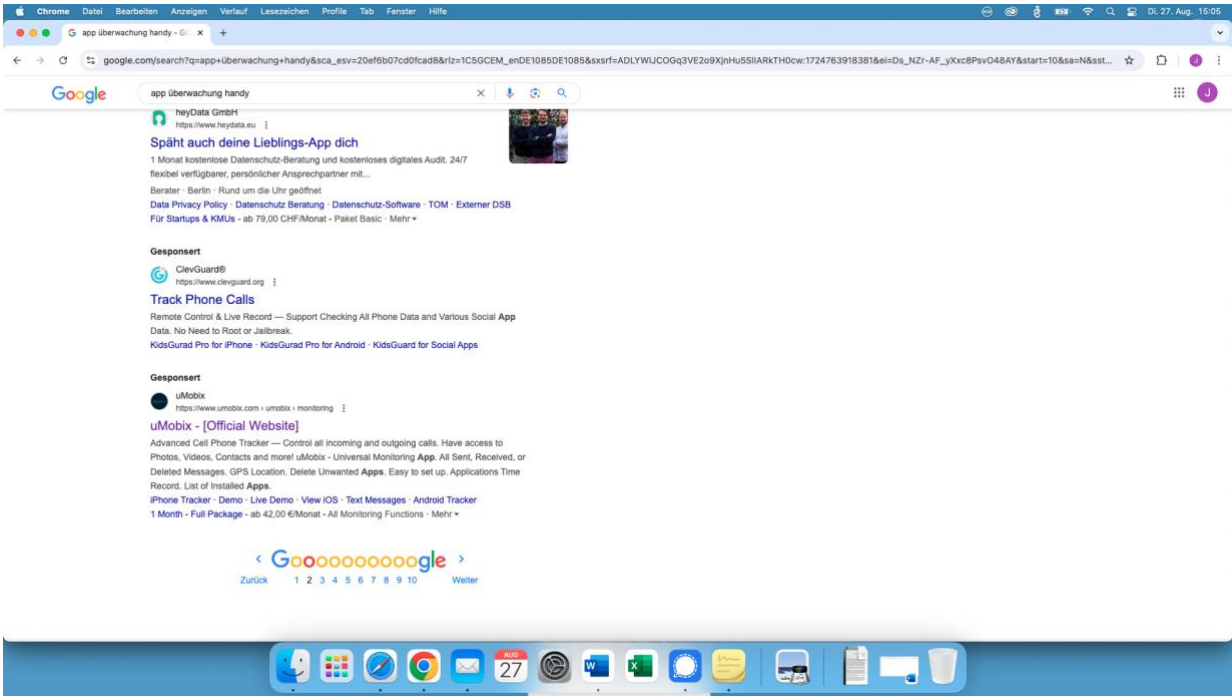
---

61 *Google*, Ads Transparency Center, https://adstransparency.google.com/?region=DE (abgerufen am: 17.10.2024).

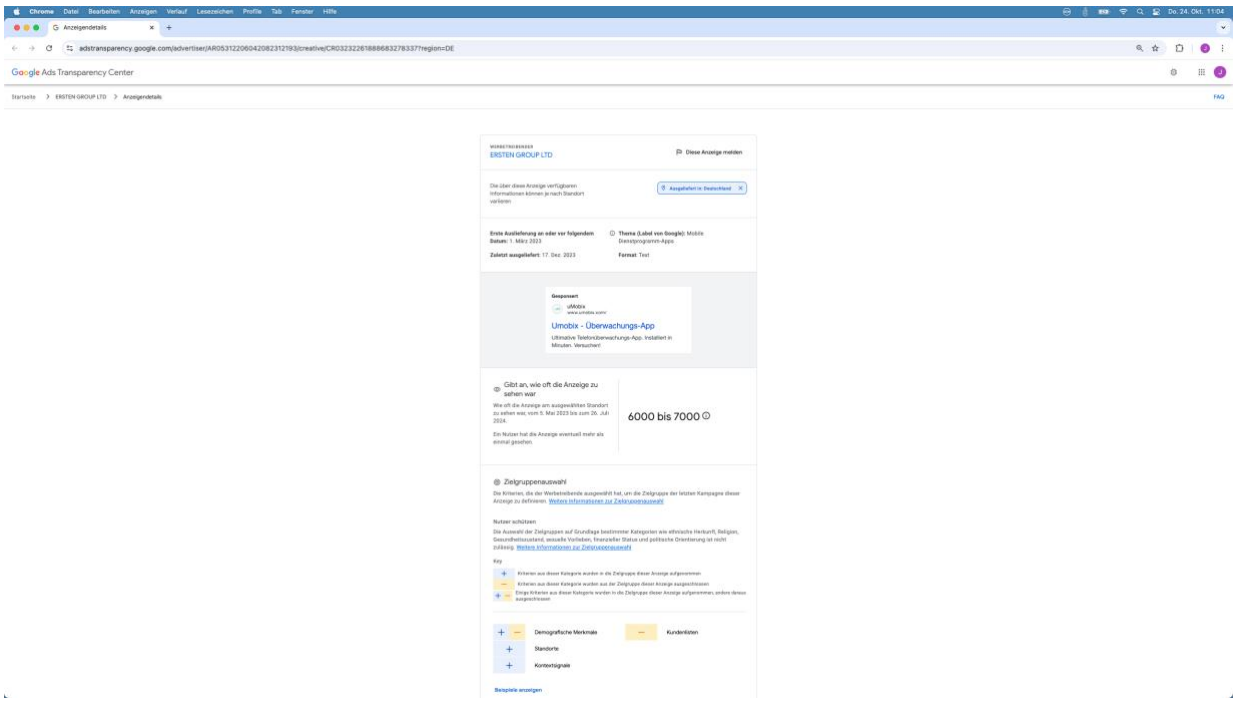
62 *Google,* Ads Transparency Center FAQ, https://adstransparency.google.com/faq (abgerufen am: 17.10.2024).

SpyBubble, Msafely, TiSpy, Spylix, Cicispy, FamiSpy, Spy366 PRO, phonemonitor, geistertrupp, zyslen und mektabyt.

1) uMobix[63]



63 https://umobix.com (abgerufen am 14.10.2024).



- **Suchbegriff**: „App Überwachung Handy“, 27. August 2024
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 6000 bis 7000 Mal in Deutschland ausgespielt wurden
- **Funktionalitäten der App**: verborgene Überwachung von
    - Social-Media-Anwendungen
    - der eingehenden und ausgehenden Anrufe und Nachrichten
    - der Kontaktliste, der Videos, Fotos und Audioaufnahmen
    - Keylogging
    - GPS-Ortung
    - Fernzugriff auf das Gerät

2) mSpy[64]

- **Suchbegriff**: „WhatsApp heimlich mitlesen“, 27. August 2024. (**Anlage 5.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 3000 bis 4000 Mal in Deutschland ausgespielt wurden (**Anlage 5.2**)
- **Funktionalitäten** der App: verborgene Überwachung der
  - gängigen Social-Media-Anwendungen
  - der eingehenden und ausgehenden Anrufe und Nachrichten
  - der Kontaktliste
  - der Browserchronik
  - des Kalenders
  - der Videos, Fotos und Audioaufnahmen
  - Keylogging
  - GPS-Ortung des Geräts

3) Spynger[65]

- **Suchbegriff**: „Spynger App“, 29. August 2024. (**Anlage 6.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 25000 bis 30000 Mal in Deutschland ausgespielt wurden (**Anlage 6.2**)
- **Funktionalitäten** der App: verborgene Überwachung der

---

64 https://mspy.mobi (abgerufen am 14.10.2024).
65 https://spynger.net/de (abgerufen am 14.10.2024).

- genutzten Social-Media-Anwendungen
- Abhören der ein- und ausgehenden Telefonate
- Einsicht in Fotos und Videos
- GPS-Ortung
- Keylogging

4) ClevGuard[66]

- **Suchbegriff**: „Freundin Handy ausspionieren“, 27. August 2024. (**Anlage 7.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 40000 bis 45000 Mal in Deutschland ausgespielt wurden (**Anlagen 7.2, 7.3, 7.4**)
- **Funktionalitäten** der App: verborgene Überwachung der
  - gängigen Social-Media-Anwendungen
  - der eingehenden und ausgehenden Anrufe und Nachrichten
  - der Kontaktliste
  - der Browserchronik
  - des Kalenders
  - der Videos, Fotos und Audioaufnahmen
  - GPS-Ortung des Geräts

[66] https://www.clevguard.de (abgerufen am 14.10.2024).

5) SpyX[67]

- **Suchbegriff**: „Freundin Handy ausspionieren“, 27. August 2024. (**Anlage 8.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 250000 bis 300000 Mal in Deutschland ausgespielt wurden (**Anlage 8.2**)
- **Funktionalitäten** der App: verborgene Überwachung der
  - gängigen Social-Media-Anwendungen
  - der eingehenden und ausgehenden Anrufe und Nachrichten
  - der Kontaktliste
  - der Browserchronik,
  - des Kalenders
  - der Videos, Fotos und Audioaufnahmen
  - Keylogging
  - GPS-Ortung des Geräts

6) Haqerra[68]

- **Suchbegriff**: “Handy Spion kostenlos”, 27. August 2024. (**Anlage 9.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 25000 bis 30000 Mal in Deutschland ausgespielt wurden (**Anlage 9.2**)
- **Funktionalitäten** der App: verborgene Überwachung der

---

67 https://spyx.com/de (abgerufen am 14.10.2024).
68 https://haqerra.net (abgerufen am 14.10.2024).

- gängigen Social-Media-Anwendungen
- der eingehenden und ausgehenden Anrufe und Nachrichten
- der Kontaktliste
- der Browserchronik
- des Kalenders
- der Videos, Fotos und Audioaufnahmen
- Keylogging
- GPS-Ortung

7) Spyera[69]

- **Suchbegriff**: „Spyera“, 29. August 2024. (**Anlage 10.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 3000 bis 4000 Mal in Deutschland ausgespielt wurden (**Anlage 10.2**)
- **Funktionalitäten** der App: verborgene Überwachung der
  - gängigen Social-Media-Anwendungen
  - der eingehenden und ausgehenden Anrufe und Nachrichten
  - der Kontaktliste
  - der Browserchronik
  - des Kalenders

[69] https://spyera.com/de/ (abgerufen am 14.10.2024).

- der Videos, Fotos und Audioaufnahmen
- Keylogging
- GPS-Ortung/Geofencing
- Überwachung des Geräts mittels Screenshots
- Kontrolle über Mikrofon und Abhören der Umgebung

8) Spytech SpyAgent[70]

- Ausgespielt bei folgendem **Suchbegriff**: „Freundin Handy Überwachen Unsichtbar“, 27. August 2024 (**Anlage 11.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 15000 bis 20000 Mal in Deutschland ausgespielt wurden (**Anlagen 11.2, 11.3**)
- **Funktionalitäten** der App: verborgene Überwachung der
  - gängigen Social-Media-Anwendungen
  - der eingehenden und ausgehenden Anrufe und Nachrichten
  - der Kontaktliste
  - der E-Mails
  - der Browserchronik
  - des Kalenders
  - der Videos, Fotos und Audioaufnahmen
  - Key- und Mouselogging

[70] https://www.spytech-spyagent.com (abgerufen am 14.10.2024).

- Überwachung des Geräts mittels Screenshots

9) GuardW[71]

- Ausgespielt bei folgendem **Suchbegriff**: “Handy Spion Kostenlos”, 27. August 2024 (**Anlage 12.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 3000 bis 4000 Mal in Deutschland ausgespielt wurden (**Anlagen 12.2, 12.3**)
- **Funktionalitäten** der App: verborgene Überwachung der
  - gängigen Social-Media-Anwendungen
  - der eingehenden und ausgehenden Anrufe und Nachrichten
  - der Kontaktliste
  - der Browserchronik
  - des Kalenders
  - der Videos, Fotos und Audioaufnahmen
  - GPS-Ortung

10) SpyBubble[72]

- Ausgespielt bei folgendem **Suchbegriff**: „Guard Spy App“, 29. August 2024 (**Anlage 13.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 10000 bis 15000 Mal in Deutschland ausgespielt wurden (**Anlage 13.2**)

---

71 https://www.guardw.net/de/ (abgerufen am 14.10.2024).
72 https://spybubblepro.com (abgerufen am 14.10.2024).

- **Funktionalitäten** der App: verborgene Überwachung der
    - gängigen Social-Media-Anwendungen
    - der eingehenden und ausgehenden Anrufe und Nachrichten
    - der Kontaktliste
    - der Browserchronik
    - der Videos, Fotos und Audioaufnahmen
    - Keylogging
    - GPS-Ortung

11) Msafely[73]

- Ausgespielt bei folgendem **Suchbegriff**: „Freundin Handy Ausspionieren“, 27. August 2024 (**Anlage 14.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 30000 bis 35000 Mal in Deutschland ausgespielt wurden (**Anlage 14.2**)
- **Funktionalitäten** der App: verborgene Überwachung der
    - gängigen Social-Media-Anwendungen
    - der eingehenden und ausgehenden Anrufe und Nachrichten
    - der Kontaktliste
    - der Browserchronik
    - der E-Mails

[73] https://msafely.com (abgerufen am 14.10.2024).

- der Videos, Fotos und Audioaufnahmen
- des Keyloggings
- der GPS-Ortung/Geofencing

12) TiSpy[74]

- Ausgespielt bei folgendem **Suchbegriff**: „Freundin Handy Ausspionieren“, 27. August 2024 (**Anlage 15.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 7000 bis 8000 Mal in Deutschland ausgespielt wurden (**Anlage 15.2**)
- **Funktionalitäten** der App: verborgene Überwachung
  - der gängigen Social-Media-Anwendungen
  - der eingehenden und ausgehenden Anrufe und Nachrichten
  - der Kontaktliste
  - der Browserchronik
  - des Kalenders
  - der Videos, Fotos und Audioaufnahmen
  - des Keyloggings
  - die GPS-Ortung
  - durch Bildschirmaufnahme

[74] https://tispy.net (abgerufen am 14.10.2024).

13) Spylix[75]

- Ausgespielt bei folgendem **Suchbegriff**: „Freundin Handy Ausspionieren“, 27. August 2024 (**Anlage 16.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 2000 bis 3000 Mal in Deutschland ausgespielt wurden (**Anlage 16.2**)
- **Funktionalitäten** der App: verborgene Überwachung
    - der gängigen Social-Media-Anwendungen
    - der eingehenden und ausgehenden Anrufe und Nachrichten
    - der Kontaktliste
    - der Browserchronik
    - der Videos, Fotos und Audioaufnahmen
    - des Keyloggings
    - der GPS-Ortung

14) CiciSpy[76]

- Ausgespielt bei folgendem **Suchbegriff**: „Handy klonen“, 27. August 2024 (**Anlage 17.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 4000 bis 5000 Mal in Deutschland ausgespielt wurden (**Anlagen 17.2, 17.3, 17.4**)
- **Funktionalitäten** der App: verborgene Überwachung

---

[75] https://www.spylix.com (abgerufen am 14.10.2024).
[76] https://www.cicispy.com (abgerufen am 14.10.2024).

- der gängigen Social-Media-Anwendungen
- der eingehenden und ausgehenden Anrufe und Nachrichten
- der Kontaktliste
- der Browserchronik
- der Kalender
- der Videos, Fotos und Audioaufnahmen
- des Keyloggings
- der GPS-Ortung

15) FamiSpy[77]

- Ausgespielt bei folgendem **Suchbegriff**: „Freundin Handy Ausspionieren“, 29. August 2024 (**Anlage 18.1**)
- **Werbearchiv**: erfasst sind ähnliche Anzeigen vom selben Anbieter, die 0 bis 1000 Mal in Deutschland ausgespielt wurde (**Anlage 18.2**)
- **Funktionalitäten** der App: verborgene Überwachung der
  - gängigen Social-Media-Anwendungen
  - der eingehenden und ausgehenden Anrufe und Nachrichten
  - der Kontaktliste
  - der E-Mails
  - der Browserchronik

[77] https://famispy.com/de/ (abgerufen am 14.10.2024).

- der Videos, Fotos und Audioaufnahmen
- Keylogging
- Überwachung des Geräts mittels Screenshots

16) Spy366PRO[78]

- Ausgespielt bei folgendem **Suchbegriff**: „Freundin Handy Ausspionieren“, 29. August 2024 (**Anlage 19.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 20000 bis 25000 Mal in Deutschland ausgespielt wurde (**Anlage 19.2**)
- **Funktionalitäten** der App: verborgene Überwachung der
  - gängigen Social-Media-Anwendungen
  - der eingehenden und ausgehenden Anrufe und Nachrichten
  - der Kontaktliste
  - der E-Mails
  - der Browserchronik
  - der Videos, Fotos und Audioaufnahmen
  - Keylogging
  - Überwachung des Geräts mittels Screenshots

17) PhoneMonitor[79]

---

78 https://spy366.pro (abgerufen am 14.10.2024).
79 https://phonemonitor.com (abgerufen am 14.10.2024).

- Ausgespielt bei folgendem **Suchbegriff**: „Überwachung Partnerin Handy“, 29. August 2024 (**Anlage 20.1**)

- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, bisher bis 1000 Mal in Deutschland ausgespielt wurden (**Anlagen 20.2, 20.3**)

- **Funktionalitäten** der App: verborgene Überwachung von

    - Social-Media-Anwendungen

    - Web-Aktivitäten

    - ein- und ausgehende Telefonate und Nachrichten

    - Fernzugriff auf das Smartphone

    - GPS-Ortung

18) Geistertrupp[80]

- Ausgespielt bei folgendem **Suchbegriff**: „Spy App“, 29. August 2024 (**Anlage 21.1**)

- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 4000 bis 5000 Mal in Deutschland ausgespielt wurde (**Anlage 21.2**)

- **Funktionalitäten** der App: “einhacken” in

    - diverse Social-Media-Anwendungen

    - Abhören der Anrufe

    - GPS-Ortung

    - Nachrichtenwiederherstellung

---

[80] https://www.geistertrupp.com (abgerufen am 14.10.2024).

19) Zyslen[81]

- Ausgespielt bei folgendem **Suchbegriff**: „Freundin Handy Ausspionieren“, 29. August 2024 (**Anlage 22.1**)
- **Werbearchiv**: erfasst ähnliche Anzeigen vom selben Anbieter, die 150000 bis 175000 Mal in Deutschland ausgespielt wurden (**Anlage 22.2**)
- **Funktionalitäten** der App: je nach gebuchtem Paket die Überwachung von
  - WhatsApp-Nachrichten
  - allen Anwendungen auf dem Smartphone
  - genereller Kommunikation
  - GPS-Ortung
  - Browserchronik
  - Fernzugriff

20) mektabyt[82]

- Ausgespielt bei folgendem **Suchbegriff**: „Überwachung Partnerin Sofort“, 29. August 2024 (**Anlage 23.1**)
- **Werbearchiv**: im Werbearchiv nicht erfasst, auch nach 72 Stunden nach der ersten Suche war keine Anzeige im Werbearchiv aufgeführt (**Anlage 23.2**)
- **Funktionalitäten** der App:

---

81 https://zyslen.com (abgerufen am 14.10.2024).
82 https://www.mektabyt.com (abgerufen am 14.10.2024).

- Abhören von Telefonaten
- die Einsicht von Fotos und Videos
- die Überwachung von Nachrichten und der Anrufliste

B. Rechtliche Würdigung: Verstoß gegen Art. 35 Abs. 1 Satz 1 i.V.m. Art. 34 DSA

44 Die Beschwerdegegnerin verstößt gegen ihre Pflicht zur Risikominderung gemäß Art. 35 Abs. 1 Satz 1 i.V.m. Art. 34 DSA.

45 Gemäß Art. 35 Abs. 1 Satz 1 DSA ergreifen die Anbieter*innen sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen angemessene, verhältnismäßige und wirksame Risikominderungsmaßnahmen, die auf die gemäß Artikel 34 ermittelten besonderen systemischen Risiken zugeschnitten sind. Dabei sind die Auswirkungen solcher Maßnahmen auf die Grundrechte besonders zu berücksichtigen. Gemäß Art. 35 Abs. 1 Satz 2 lit. e DSA können hierzu unter Umständen die Anpassung ihrer Werbesysteme und Annahme von gezielten Maßnahmen zur Beschränkung oder Anpassung der Anzeige von Werbung in Verbindung mit dem von ihnen erbrachten Dienst gehören.

46 Die Beschwerdegegnerin ist als VLOSE Adressatin der Risikominderungspflicht (**I.**). Obwohl sich aus der Bewerbung von Stalking-Apps systemische Risiken im Sinne des Art. 34 Abs. 1 DSA ergeben (**II.**), hat sie keine ausreichenden Risikominderungsmaßnahmen getroffen (**III.**).

I. Beschwerdegegnerin als Anbieterin einer sehr großen Online-Suchmaschine

47 Die Beschwerdegegnerin ist Adressatin der Risikominderungspflicht gemäß Art. 35 Abs. 1 Satz 1 DSA.

48 Die Norm richtet sich an Anbieter*innen sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen. Die Beschwerdegegnerin betreibt die Google-Suchmaschine. Die Europäische Kommission hat die Suchmaschine der Beschwerdegegnerin gemäß Art. 33 Abs. 4 DSA als VLOSE im Sinne des Art. 33 DSA benannt.[83]

---

[83] *Europäische Kommission*, Kommissionsentscheidung vom 25. April 2023, https://digital-strategy.ec.europa.eu/de/library/designation-decisions-first-set-very-large-online-platforms-vlops-and-very-large-online-search (abgerufen am: 17.10.2024).

II. Aus der Bewerbung von Stalking-Apps ergeben sich systemische Risiken

49 Die Bewerbung von Stalking-Apps über Google Ads führt zu systemischen Risiken im Sinne des Art. 34 Abs. 1 UAbs. 1, UAbs. 2 Satz 2 lit. b und lit. d DSA.

50 Bei den nachteiligen Auswirkungen der Bewerbung von Stalking-Apps in Bezug auf geschlechtsspezifische Gewalt und auf die Ausübung der Grundrechte handelt es sich um systemische Risiken (**1.**). Diese ergeben sich aus dem Betrieb des mit der Suchmaschine der Beschwerdegegnerin verbundenen Werbeprogramms (**2.**).

1. Systemische Risiken

51 Die Voraussetzungen eines systemischen Risikos (**1.1**) sind gegeben (**1.2**).

1.1 Definition und Bewertungsmaßstab systemischer Risiken

52 Der DSA definiert den Begriff des „systemischen Risikos“ nicht. Seine Bedeutung ist deshalb durch Auslegung zu ermitteln (**1.1.1**). Ob ein Risiko systemisch ist, lässt sich – in Ermangelung von Rechtsprechung dazu – anhand eines von der Kommission entwickelten Bewertungsmaßstabs bestimmen (**1.1.2**). Die Bewertung erfolgt ausgehend von den in Art. 34 Abs. 1 UAbs. 2 Satz 2 lit. a bis lit. d DSA enthalten Risikokategorien, zu denen insbesondere alle tatsächlichen oder absehbaren nachteiligen Auswirkungen in Bezug auf geschlechtsspezifische Gewalt (lit. d Var. 1) sowie etwaige tatsächliche oder vorhersehbare nachteilige Auswirkungen auf die Ausübung der Grundrechte (lit. b) gehören (**1.1.3**).

1.1.1 Auslegung des Begriffs des systemischen Risikos

53 Unter systemischen Risiken sind Gefährdungen zu verstehen, die – in Abgrenzung zu individuellen Rechtsverstößen und Gefahren, die sich auf einzelne Betroffene beschränken – eine übergreifende, öffentliche Belange berührende Qualität aufweisen. Systemisch sind sie deshalb, weil die Struktur und Funktionsweise von VLOSEs dazu beitragen, dass einzelne Gefährdungen regelmäßig eine große Streubreite entfalten oder dass aus einer Vielzahl an

Rechtsverletzungen ein Risiko entsteht, welches eine systemische Bedeutung über die Summe der Einzelfälle hinaus bekommt.[84]

54 Systemische Risiken können insoweit als strukturelle Gefahren des Plattform- oder Suchmaschinenbetriebs verstanden werden.[85]

1.1.2 Bewertungsmaßstab

55 Gem. Art. 34 Abs. 1 UAbs. 2 DSA a.E. sind bei der Bewertung des Risikos die Eintrittswahrscheinlichkeit und Schadensschwere zu berücksichtigen. Anbieter*innen könnten beispielsweise prüfen, ob die möglichen negativen Auswirkungen eine große Zahl von Personen betreffen können, unumkehrbar sind oder wie schwierig es ist, die möglichen Auswirkungen zu beheben und die vorherige Situation wiederherzustellen (Erwägungsgrund 79 Satz 5 f. DSA).

56 Die EU-Kommission hat im August 2023 mit einer Veröffentlichung unter dem Titel „Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns“ ihre Auslegung der Anforderungen von Art. 34 DSA an die Risikobewertung konkretisiert. Der darin vorgezeichnete Bewertungsmaßstab bezieht sich zwar speziell auf Desinformationskampagnen und richtet sich an Forschende. Dennoch lassen sich der Veröffentlichung einige grundlegende Bewertungskriterien entnehmen. Damit ein Risiko als „systemisch“ Sinne des Art. 34 DSA gilt, ist eine Verhältnismäßigkeitsprüfung in Abhängigkeit quantitativer und qualitativer Faktoren durchzuführen.[86]

57 Dementsprechend sieht die Kommission eine Risikobewertung in zwei Schritten vor: Einer qualitativen, gefolgt von einer quantitativen Risikobewertung.[87] Die qualitative Risikobewertung erfolgt auf Grundlage der in Art. 34 Abs. 1 Satz 2 DSA gelisteten Risikokategorien.[88] Die darauffolgende quantitative Bewertung zielt darauf ab, die Reichweite, also in welchem Ausmaß der Inhalt verbreitet

---

84 *Beyerbach,* in: Müller-Terpitz/Köhler: Digital Services Act, 2024, Art. 34 Rn. 14.
85 *Beyerbach,* in: Müller-Terpitz/Köhler: Digital Services Act, 2024, Art. 34 Rn. 15.
86 *Europäische Kommission*, Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns, August 2023, 1. Edition, S. 15, https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1 (abgerufen am: 17.10.2024).
87 Ebd., S. 15 ff.
88 Ebd., S. 15.

wurde, zu ermitteln und zu bewerten.[89] Die Einstufung als systemisches Risiko folgt einer Je-desto-Logik: Je höher das mit dem Inhalt verbundene Risiko, desto kleiner muss das Publikum sein, das erforderlich ist, um insgesamt eine systemische Ebene zu erreichen. Je geringer das mit dem Inhalt verbundene Risiko, desto größer muss das erreichte Publikum sein, um die systemische Ebene zu erreichen.[90]

58 Die qualitativen und quantitativen Bewertungskriterien finden sich auch in den Leitprinzipien für Wirtschaft und Menschenrechte der Vereinten Nationen wieder („scale“ und „scope“).[91] Sie gelten als anerkannter Bewertungsmaßstab für negative Auswirkungen von Unternehmen auf Menschenrechte und werden durch ein drittes Kriterium, der Umkehrbarkeit („remediability“) der Auswirkung ergänzt. Dieses Kriterium ist auch in Erwägungsgrund 79 Satz 5 f. DSA angelegt.

1.1.3 Risikokategorien

59 Art. 34 Abs. 1 UAbs. 2 DSA enthält vier Kategorien systemischer Risiken, die nach der Bewertung in der deutschen rechtswissenschaftlichen Literatur als Regelbeispiele zu verstehen sind.[92]

60 Sie sind dem Wortlaut nach in jedem Fall zu berücksichtigen. Dazu gehören gemäß Art. 34 Abs. 1 UAbs. 2 Satz 1 DSA die Verbreitung rechtswidriger Inhalte, etwaige tatsächliche oder vorhersehbare nachteilige Auswirkungen auf die Ausübung der Grundrechte, alle tatsächlichen oder absehbaren nachteiligen Auswirkungen auf die gesellschaftliche Debatte und auf Wahlprozesse und die öffentliche Sicherheit sowie alle tatsächlichen oder absehbaren nachteiligen Auswirkungen in Bezug auf geschlechtsspezifische Gewalt, den Schutz der öffentlichen Gesundheit und von Minderjährigen sowie schwerwiegende nachteilige Folgen für das körperliche und geistige Wohlbefinden einer Person.

---

89 Vgl. ebd., S. 17.
90 Ebd., S. 15.
91 *United Nations*, Guiding Principles on Business and Human Rights, 2011, S. 16, https://www.undp.org/asia-pacific/bizhumanrights/publications/guiding-principles-business-and-human-rights (abgerufen am 31.10.2024).
92 *Beyerbach,* in: Müller-Terpitz/Köhler: Digital Services Act, 2024, Art. 34 Rn. 18; *Kaesling,* in: Hofmann/Raue: Digital Services Act, 1. Aufl. 2023, Art. 34 Rn. 57.

61 Vorliegend sind vor allem zwei Risikokategorien bedeutend.

a) Kategorie 4: „Auswirkungen in Bezug auf geschlechtsspezifische Gewalt“

62 Zur vierten Kategorie gehören insbesondere alle tatsächlichen oder absehbaren nachteiligen Auswirkungen in Bezug auf geschlechtsspezifische Gewalt (Art. 34 Abs. 1 UAbs. 2 Satz 2 lit. d DSA). Der europäische Gesetzgeber erkennt damit die Bedeutung des strukturellen Problems von Gewalt gegen Frauen an (siehe oben **A. II. 2. 2.1**).

63 Im Hinblick auf das Risiko geschlechtsspezifischer Gewalt verlangt Art. 34 Abs. 1 UAbs. 2 lit. d DSA tatsächliche oder absehbare nachteilige Auswirkungen. Mithin müssen die nachteiligen Auswirkungen nicht eingetreten sein, es reicht die Wahrscheinlichkeit aus, dass sich diese Auswirkungen voraussichtlich ergeben werden.[93]

64 Anders als bei der Variante der nachteiligen Folgen für das körperliche und geistige Wohlbefinden einer Person (vergleiche Art. 34 Abs. 1 UAbs. 2 lit. d Var. 4 DSA: „schwerwiegende nachteilige Folgen“) gilt hinsichtlich der nachteiligen Auswirkungen in Bezug auf geschlechtsspezifische Gewalt keine Erheblichkeitsschwelle.[94] Darin, dass Formen geschlechtsspezifischer Gewalt als besondere strukturelle Ausprägung von Gewalt grundsätzlich schon von den ersten beiden Risikokategorien erfasst ein können, und dennoch vom Gesetzgeber als zusätzliche Risikokategorie gelistet wurden, zeigt sich, dass den Risiken in Bezug auf geschlechtsspezifische Gewalt ein besonderes Gewicht zukommt.

65 Zur Begriffsbestimmung von „geschlechtsspezifischer Gewalt“ lässt sich Erwägungsgrund 10 Satz 1 bis 3 der Richtlinie (EU) 2024/1385 des Europäischen Parlaments und des Rates vom 14. Mai 2024 zur Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt heranziehen. Demnach ist Gewalt gegen Frauen eine Form der geschlechtsspezifischen Gewalt, die in erster Linie von Männern an Frauen und Mädchen verübt wird und die ihre Wurzeln in gesellschaftlich

---

93 *Beyerbach,* in: Müller-Terpitz/Köhler: Digital Services Act, 2024, Art. 34 Rn. 16.
94 *Kaesling,* in: Hofmann/Raue: Digital Services Act, 1. Aufl. 2023, Art. 34 Rn. 109.

geprägten Rollen, Verhaltensweisen, Tätigkeiten und Merkmalen hat, die eine bestimmte Gesellschaft als für Frauen und Männer angemessen ansieht.

b) Kategorie 2: „etwaige tatsächliche oder vorhersehbare nachteilige Auswirkungen auf die Ausübung der Grundrechte“

66 Eine weitere Risikokategorie stellen etwaige tatsächliche oder vorhersehbare nachteilige Auswirkungen auf die Ausübung der Grundrechte dar (Art. 34 Abs. 1 UAbs. 1 lit. b DSA). Der DSA soll ein Online-Umfeld sicherstellen, in dem die in der Charta verankerten Grundrechte wirksam geschützt sind (Erwägungsgrund 9). Art. 34 Abs. 1 UAbs. 1 lit. b DSA zählt einzelne Grundrechte beispielhaft, aber nicht abschließend („insbesondere“) auf. Zu diesen gehören Art. 7 GrCh (Achtung des Privat- und Familienlebens) sowie Art. 8 der GRCh (Schutz personenbezogener Daten). Diese Risikokategorie bildet querschnittsartig zu den anderen benannten Risiken die grundrechtliche Dimension sämtlicher struktureller Risiken ab.[95] In ihr findet die mittelbare Wirkung der Grundrechte ihren Ausdruck.[96]

1.2 Bewertung für die Bewerbung von Stalking-Apps

67 Die Bewerbung von Stalking-Apps hat tatsächliche und absehbare nachteilige Auswirkungen in Bezug auf geschlechtsspezifische Gewalt gemäß Art. 34 Abs. 1 UAbs. 2 lit. d DSA und auf die in Artikel 7 und Artikel 8 der Charta verankerten Grundrechte gemäß Art. 34 Abs. 1 UAbs. 2 lit. b DSA.

68 Die Schwelle des systemischen Risikos ist vorliegend erreicht. Dies ergibt sich aus der qualitativen (**1.2.1**) und quantitativen (**1.2.2**) Bewertung sowie der Unumkehrbarkeit der Auswirkungen (**1.2.3**).

1.2.1 Qualitative Bewertung der Bewerbung von Stalking-Apps

69 Das qualitative Risiko der Bewerbung einer Stalking-App ist besonders hoch. Stalking-Apps haben schwerwiegende Auswirkungen im Einzelfall und verletzen höchstpersönliche Rechte.

---

95 *Kaesling,* in: Hofmann/Raue: Digital Services Act, 1. Aufl. 2023, Art. 34 Rn. 75.
96 *Kaesling,* in: Hofmann/Raue: Digital Services Act, 1. Aufl. 2023, Art. 34 Rn. 76.

70 Stalking-Apps haben eine geschlechtsspezifische Dimension. Sie sind ein technisches Instrument zum Cyberstalking und Teil von Gewalt gegen Frauen (dazu **A.II.**). Sie haben mithin tatsächliche, mindestens aber absehbare Auswirkungen in Bezug auf geschlechtsspezifische Gewalt. Ausgehend vom Wortlaut des Art. 34 Abs. 1 UAbs. 2 lit. d DSA besteht bereits kein Erheblichkeitserfordernis. Selbst wenn ein solches bestehen sollte, ist aber davon auszugehen, dass dieses vorliegend erfüllt wäre, da die tatsächlichen Auswirkungen auf von Cyberstalking, also insbesondere vom Einsatz von Stalking-Apps betroffene Personen gravierend und regelmäßig mit anderen Formen psychischer und physischer Gewalt verbunden sind (dazu **A.II.2.**).

71 Hinzu kommen tatsächliche oder vorhersehbare nachteilige Auswirkungen auf die in Art. 7 und 8 der Charta verankerten Grundrechte auf Achtung des Privat- und Familienlebens und auf den Schutz personenbezogener Daten gemäß Art. 34 Abs. 1 UAbs. 2 lit. b DSA. Stalking-Apps ermöglichen einen vollumfänglichen Zugriff auf Geräte und darin enthaltene personenbezogene Daten (dazu **A.I.**). Die Daten sind zum Teil höchstpersönlich, wie beispielsweise Kommunikationsinhalte, Fotos, Daten in Zyklus-Apps usw.

1.2.2 Quantitative Bewertung der Bewerbung von Stalking-Apps

72 Ausgehend von der Je-desto-Formel der Kommission sind die Anforderungen an die Reichweite vorliegend gering: Je schwerwiegender sich das Risiko der beworbenen Stalking-Apps auf die betroffene Person im Einzelfall auswirken kann, desto geringer kann die tatsächliche Reichweite, also Zahl der ausgespielten Anzeigen sein, um die Schwelle des systemischen Risikos zu erreichen.

73 Da das Risiko von Stalking-Apps auf betroffene Personen qualitativ bereits sehr hoch ist, sind die Anforderungen an die Reichweite gering. Die Anzeige-Zahlen im Google Transparency Center zeigen jedoch, dass auch die Reichweite der Anzeigen erheblich (**A.IV.3.**) und damit auch die quantitative Dimension hoch ist. Hinzu kommt das Reichweitenpotential, das sich aus der Marktmacht der Beschwerdegegnerin ergibt (**A.IV.2.2**).

1.2.3 Unumkehrbarkeit der Auswirkungen

74 Bezieht man in Anlehnung an die Leitprinzipien für Wirtschaft und Menschenrechte der Vereinten Nationen und Erwägungsgrund 79 DSA bei der

Risikobewertung mit ein, ob eine Auswirkung unumkehrbar ist und wie schwierig es ist, die möglichen Auswirkungen zu beheben und die vorherige Situation wiederherzustellen, [97] verschärft sich der Befund. Die psychischen und physischen Auswirkungen auf von Stalking-Apps betroffene Personen können nicht rückgängig gemacht werden und belasten diese meist ein Leben lang.

2. Risiko durch das Werbeprogramm der Beschwerdegegnerin

75 Die dargelegten systemischen Risiken ergeben sich aus dem Betrieb des Werbeprogramms der Beschwerdegegnerin. Das Werbeprogramm stellt ein mit der Suchmaschine verbundenes System dar (**2.1**). Aus der Bereitstellung und dem Betrieb des Werbeprogramms ergeben sich die oben genannten Risiken (**2.2**).

2.1 Das Werbeprogramm der Beschwerdegegnerin als mit der VLOSE verbundenes System

76 Risikopotenziale können sich gemäß Art. 34 Abs. 1 UAbs. 1 DSA nicht nur aus dem Betrieb des Dienstes selbst, sondern auch aus den mit dem Dienst verbundenen Systemen, einschließlich algorithmischer Systeme, ergeben.

77 Das Werbeprogramm der Beschwerdegegnerin stellt ein mit dem Betrieb der Suchmaschine der Beschwerdegegnerin, und damit als ein mit der VLOSE verbundenes System – mit teilweise plattformartigem Charakter – im Sinne des Art. 34 Abs. 1 UAbs. 1 DSA dar.

78 Das Werbeprogramm selbst ist bislang nicht als sehr große Online-Plattform (*very large online platform*, VLOP) eingestuft. Es ist aber in den Suchmaschinendienst der Beschwerdegegnerin eingebettet und stellt ein mit der Google-Suchmaschine verbundenes System dar, das plattformartige Elemente aufweist.

79 Für die Einordnung des Werbeprogramms der Beschwerdegegnerin als Online-Plattform gemäß Art. 3 lit. i DSA spricht, dass den Werbenden durch das Programm die Speicherung und öffentliche Verbreitung von Informationen (hier

---

[97] Siehe hierzu auch *Ebert et al*, The Business & Human Rights Dimension oft he Digital Services Act, 31.08.2023, https://freiheitsrechte.org/uploads/publications/Digital/Grundrechte-im-Digitalen/The-Business-Human-Rights-Dimension-of-the-Digital-Services-Act.pdf (abgerufen am 31.10.2024).

in Form von Werbeanzeigen) an einen bestimmten Personenkreis ermöglicht wird. Dazu gehören alle Nutzer*innen der Suchmaschine, die die angegebenen Suchbegriffe nutzen. Allerdings kann das Werbeprogramm aus objektiven und technischen Gründen nicht ohne den Suchmaschinendienst genutzt werden. Der Suchmaschinendienst ist der Veröffentlichungsort der Anzeigen. Die Werbefunktion (Google Ads) und die Suchfunktion (Suchmaschine) stehen insbesondere durch die KI-Tools der Beschwerdegegnerin in enger Wechselwirkung (siehe oben **A.IV.1.**).

80 Dass sich systemische Risiken gerade auch aus Werbesystemen ergeben können, bestätigt Art. 34 Abs. 2 Satz 1 lit. d DSA. Demnach sollen die Anbieter*innen auch die Einflüsse der Systeme zur Auswahl und Anzeige von Werbung berücksichtigen. Auch Art. 35 Abs. 1 lit. e DSA zielt explizit auf Werbesysteme hinsichtlich der zu ergreifenden Risikominderungsmaßnahmen.

2.2 Zusammenhang zwischen Risiken und Werbeprogramm

81 Die systemischen Risiken stehen in direktem Zusammenhang mit dem Betrieb des Werbeprogramms.

82 Art. 34 Abs. 1 Satz 1 DSA setzt voraus, dass sich die Risiken aus der Konzeption oder dem Betrieb des Dienstes und seinen damit verbundenen Systemen, einschließlich algorithmischer Systeme, oder der Nutzung ihrer Dienste ergeben.

83 Angesichts der Wirkung von Online-Werbung über Search-Ads (dazu **A.IV.1.**) sowie des eingeschränkten Vertriebswegs außerhalb der gängigen App-Stores (dazu **A.III.**) erreicht erst die Bewerbung über die Suchmaschine der Beschwerdegegnerin die Sichtbarkeit und anschließende Nutzung von Stalking-Apps. Die Reichweite, die dieser Art von Anzeigen durch die Marktmacht der Beschwerdegegnerin zu Teil wird, ist erheblich (dazu **A.IV.2.2**).

84 Darüber hinaus veröffentlicht die Beschwerdegegnerin nicht nur rein passiv die von den Anbieter*innen erstellten Anzeigen. Sie trägt sogar aktiv zur Erhöhung der Wirksamkeit und Reichweite der Anzeigen bei, indem sie KI-gestützte Produkte bereitstellt und sowohl in den Prozess des Erstellens als auch des Ausspielens von Suchanzeigen integriert hat (siehe dazu oben **A.IV.1.**). Gerade den Einsatz solcher algorithmischen Systeme hatte der Unionsgesetzgeber bei der Begründung systemischer Risiken ausdrücklich im Blick, wie der Wortlaut des Art. 34 Abs. 1 UAbs. 1 a.E. DSA zeigt. Da die Anzeigen ohne das Ausspielen der

Werbung durch die Beschwerdegegnerin nicht in gleichem Maße auffindbar wären (siehe **A.IV.2.**), erhöht sie mit dem Ausspielen der Werbeanzeigen das Risiko der Nutzung solcher Apps und damit auch der mit dieser Nutzung einhergehenden geschlechtsspezifischen Gewalt und der nachteiligen Auswirkungen auf die Ausübung der Grundrechte.

III. Mangelhafte Risikominderung durch die Beschwerdegegnerin

85 Die Beschwerdegegnerin hat keine ausreichenden Maßnahmen ergriffen, um die dargestellten Risiken zu verringern.

86 Gemäß Art. 35 Abs. 1 S. 1 DSA haben Anbieter*innen von VLOSEs die Pflicht, angemessene, verhältnismäßige und wirksame Risikominderungsmaßnahmen zu ergreifen, die auf die gemäß Art. 34 DSA ermittelten besonderen systemischen Risiken zugeschnitten sind. Hierzu gehören gemäß Art. 35 Abs. 1 Satz 2 lit. e DSA insbesondere die Anpassung ihrer Werbesysteme und Annahme von gezielten Maßnahmen zur Beschränkung oder Anpassung der Anzeige von Werbung in Verbindung mit dem von ihnen erbrachten Dienst. Erwägungsgrund 88 Satz 4 DSA sieht vor, dass Korrekturmaßnahmen insbesondere die Beendigung von Werbeeinnahmen für bestimmte Informationen umfassen können.

87 Das von Stalking-Apps ausgehende Problem und auch die Bewerbung der Apps durch die Beschwerdegegnerin wird seit mehreren Jahren in der Öffentlichkeit diskutiert (siehe oben **A.IV.3.**). Die mit der Bewerbung verbundenen Gefahren hat die Beschwerdegegnerin offenbar im Grundsatz anerkannt, indem sie Stalking-Apps aus ihrem Play-Store verbannt und die Bewerbung dieser Apps auf ihren Plattformen untersagt hat (siehe oben **A.III.**).

88 Trotzdem lässt die leichte Auffindbarkeit mittels Werbeanzeigen den Schluss zu, dass die Beschwerdegegnerin keine ausreichenden Maßnahmen ergriffen hat, um das Risiko angemessen zu verringern. Statt die eigenen Werberichtlinien durchzusetzen, generiert die Beschwerdegegnerin sogar noch Einnahmen aus dem Werbegeschäft mit den Anbieter*innen der Stalking-Apps (siehe oben **A.IV.2.1**).

89 Nach den Werberichtlinien der Beschwerdegegnerin ist es zwar unzulässig, Stalking-Apps über Google Ads zu bewerben. Das reicht aber nicht als Risikominderungsmaßnahme. Denn die Beschwerdegegnerin setzt diese

Richtlinien offensichtlich nicht, jedenfalls nicht konsequent durch, wie die weiterhin ausgespielten und durch die von der Beschwerdegegnerin bereitgestellten KI-unterstützten Tools mutmaßlich entscheidend mitgestalteten Werbeanzeigen belegen (siehe oben **A.IV.1.**). Hier steht also nicht nur eine unverhältnismäßig lange Umsetzungsdauer in einigen Einzelfällen im Raum, sondern die Umsetzung des Verbots überhaupt. Darüber hinaus hat die EU-Kommission festgestellt, dass das bloße Vorhandensein eines Regelwerks zur Behebung eines systemischen Risikos nicht ausreicht. Stattdessen sei bei einer solchen Risikominderungsmaßnahme unter anderem zu berücksichtigen, wie schnell und wie regelmäßig die Regelungen im Einzelfall durchgesetzt werden.[98]

90 Vor diesem Hintergrund ist die Beschwerdegegnerin verpflichtet, weitere Maßnahmen zur Risikominderung zu treffen, um eine Bewerbung von Stalking-Apps zu verhindern und das Verbot in ihren Werberichtlinien effektiv durchzusetzen.

IV. Art. 65 Abs. 2 DSA

91 Da es sich vorliegend um einen Verstoß gegen die Bestimmungen des Kapitels III Abschnitt 5 handelt, regen wir schließlich an, gemäß Art. 65 Abs. 2 DSA eine Aufforderung an die Kommission zu richten, die Angelegenheit zu prüfen, da Grund zur Annahme besteht, dass die Beschwerdegegnerin als Anbieterin einer VLOSE gegen Art. 35 Abs. 1 Satz 1 i.V.m. Art. 34 DSA verstößt.

---

98 *Europäische Kommission*, Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns, August 2023, 1. Edition, S. 21, https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1 (abgerufen am: 17.10.2024).

Anlagenübersicht

Polizeiliche Kriminalstatistik Bund 2023, Tabelle 01, Zeile 207, Spalte P bis R (Anlage 1)

Bundeskriminalamt, Bundeslagebild Häusliche Gewalt, 2023, V. 1.0 (Anlage 2)

Office for Victims of Crime, Intimate Partner Violence, kein Veröffentlichungsdatum, S. 1, (Anlage 3)

Bayer, E. et al.: The impact of online display advertising and paid search advertising relative to offline advertising on firm performance and firm value, In: International Journal of Research in Marketing, Dezember 2020, Ausgabe 37 Heft 4, S. 789 (S. 790, 801) (Anlage 4)

mSpy (Anlage 5.1, 5.2)

Spynger (Anlage 6.1, 6.2)

ClevGuard (Anlage 7.1, 7.2, 7.3, 7.4)

SpyX (Anlage 8.1, 8.2)

Haqerra (Anlage 9.1, 9.2)

spyera (Anlage 10.1, 10.2)

Spytech SpyAgent (Anlage 11.1, 11.2, 11.3)

GuardW (Anlage 12.1, 12.2, 12.3)

SpyBubble (Anlage 13.1, 13.2)

Msafely (Anlage 14.1, 14.2)

TiSpy (Anlage 15.1, 15.2)

Spylix (Anlage 16.1, 16.2)

Cicispy (Anlage 17.1, 17.2, 17.3, 17.4)

FamiSpy (Anlage 18.1, 18.2)

Spy366 PRO (Anlage 19.1, 19.2)

phonemonitor (Anlage 20.1, 20.2, 20.3)

geistertrupp (Anlage 21.1, 21.2)

zyslen (Anlage 22.1, 22.2)

mektabyt (Anlage 23.1, 23.2)