DVD Deutsche Vereinigung für Datenschutz e. V.

Reuterstraße 157
53113 Bonn

Telefon: 0228 / 22 24 98
Telefax: 0228 / 24 38 470

dvd-presse@datenschutzverein.de
www.datenschutzverein.de

Presseerklärung der DVD
Bonn, 04. März 2020

Europäische Menschenrechts- und Digitalrechtsorganisationen warnen vor illegalen Online-Werbemethoden durch Apps

04. März 2020, Berlin – Auf Einladung der Civil Liberties Union for Europe (Liberties.eu) haben zehn Menschenrechts- und Digitalrechtsorganisationen in sieben EU-Ländern die Datenschutzbehörden in ihren Ländern aufgefordert[1], Verstöße gegen die europäische Datenschutz-Grundverordnung (DSGVO) durch Smartphone-Apps wie z. B. Grindr, Tinder und OkCupid zu untersuchen. In Deutschland appellieren die Digitale Gesellschaft, Digitalcourage, die **Deutsche Vereinigung für Datenschutz** und das Netzwerk Datenschutzexpertise an die Datenschutzaufsichtsbehörden, auf der Grundlage einer umfassenden Analyse[2] mit dem Titel „Out of Control“ (Außer Kontrolle) gegen App-Betreiber vorzugehen, die ohne wirksame Einwilligung der Nutzenden hochsensible Daten erheben und für Werbezwecke nutzen. An der Kampagne sind weitere Nicht-Regierungsorganisationen aus Kroatien, Italien, Ungarn, Slowenien, Spanien und Schweden beteiligt. Die Analyse wurde vom Norwegischen Verbraucherrat (Norwegian Consumer Council – NCC) und der österreichischen Organisation für digitale Rechte noyb durchgeführt[3].

Die in der Analyse untersuchten Mobil-Apps, darunter Dating- und Menstruationszyklus-Apps, leiten die sensiblen Informationen ihrer Nutzerinnen und Nutzer über deren genauen Standort, sexuelle Orientierung, religiöse und politische Überzeugungen und viele weitere persönliche Informationen an zahlreiche Drittfirmen in einem intransparenten Werbetechnologie-Ökosystem weiter. So verteilt die weltweit verbreitete Dating-App Grindr[4] die Nutzungsdaten, etwa auch die aktuellen Lokalisierungsangaben, an mehr als ein Dutzend weiterer Unternehmen. Die Dating-App OkCupid listet über 300 Werbe- und Analyse-„Partner“.

Friedemann Ebelt von Digitalcourage: „Smartphone-Nutzer haben regelmäßig keine Chance, sich vor den Folgen der Datenausbeutung und der massiven kommerziellen Überwachung zu schützen. Diese Folgen können für den Einzelnen gravierend sein bis hin zu einer Gefährdung von Leib und Leben. Die hochsensitiven

---

[1] Siehe „Schreiben an die deutschen Datenschutzaufsichtsbehörden“ in der Anlage
[2] Siehe https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf
[3] Siehe https://noyb.eu/out-of-control/?lang=de
[4] Grindr bezeichnet sich selbst als das weltgrößte soziale Netzwerk für schwule, queere, bi- und transsexuelle Menschen, mit der sich Menschen in der näheren Umgebung lokalisieren und kontaktieren können. Siehe https://www.grindr.com/

Persönlichkeitsprofile haben das Potenzial, die privaten Freiheiten in unserer Gesellschaft zu untergraben“.

Elke Steven von der Digitalen Gesellschaft: „Die Daten der App-Nutzenden werden unter Verletzung der Regeln der Datenschutz-Grundverordnung verarbeitet. Die eingeholten Zustimmungen zur Auswertung sind absolut intransparent und verstoßen zudem gegen nationales und europäisches Verbraucherrecht.“

Frank Spaeing, Vorsitzender der Deutschen Vereinigung für Datenschutz: „Die europäischen Datenschutzbehörden müssen dringend schneller und effektiver zusammenarbeiten, um den täglich millionenfach stattfindenden Rechtsbruch zu ahnden und zu beenden. Dafür müssen sie besser als bisher ausgestattet werden.“

Thilo Weichert vom Netzwerk Datenschutzexpertise: „Der augenblickliche Zustand ist nur schwer zu ertragen: Kleinere Verstöße werden derzeit schon wirksam verfolgt. Doch bei den oft dramatischen Verletzungen des Datenschutzes durch internationale Internet-Unternehmen muss sich die Wirksamkeit der DSGVO erst noch erweisen. In dieser Auseinandersetzung gegen die Daten-Goliaths benötigen die Aufsichtsbehörden die Unterstützung der Öffentlichkeit, der Verbraucherschützer und der Politik.“

Weitere Informationen finden Sie auf der Webseite der Kampagne #StopSpyingOnUs[5].

Detaillierte Informationen zum Real Time Bidding, welches in der Analyse „Out of Control“ eine Rolle spielt, können Sie dem DANA-Sonderheft 3/2019[6] entnehmen.

(423 Wörter, 3540 Zeichen mit Leerzeichen) – Ansprechpersonen siehe unten

Für weitere Einzelheiten über die Kampagne wenden Sie sich bitte an:

- Friedemann Ebelt, friedemann.ebelt@digitalcourage.de
- Frank Spaeing,
  E-Mail: spaeing@datenschutzverein.de
  Tel.: 0172 / 6043135
- Elke Steven, elke.steven@digitalegesellschaft.de
- Thilo Weichert,
  E-Mail: weichert@netzwerk-datenschutzexpertise.de
  Tel.: 0431 / 9719742

Für Fragen zu den Organisationen in den anderen europäischen Staaten wenden Sie sich an: Orsolya Reich, o.reich@liberties.eu

[5] Siehe https://www.liberties.eu/de/campaigns/stopspyingonus-fixad-tech-kampagne/307
[6] Siehe https://www.datenschutzverein.de/wp-content/uploads/2019/09/DANA_19_3_Sonderheft_Real_Time_Bidding.pdf

---------- Schreiben an die deutschen Datenschutzaufsichtsbehörden ----------

Die Industrie für digitale Werbung verletzt die Privatsphäre der Verbraucher

Sehr geehrte Damen und Herren,

wir möchten Ihre Aufmerksamkeit auf einen am 14. Januar 2020 vom norwegischen Verbraucherrat (Norwegian Consumer Control) veröffentlichten Bericht [1] lenken, der sich mit den verborgenen Seiten der Datenwirtschaft auseinandersetzt. Der Bericht mit dem Titel "Out of Control" („Außer Kontrolle“) beschreibt, wie das Online-Marketing in der Werbebranche (Adtech) funktioniert. Er kommt dabei zu dem Schluss, dass das umfassende Nachverfolgen (Tracking) und das Erstellen von individuellen Profilen (Profiling), die das Herzstück des derzeitigen Ad-tech-Ökosystems bilden, von Grund auf missbräuchliche Praktiken sind, die gegen die Europäische Datenschutz-Grundverordnung (DSGVO) verstoßen.

Die Menschen tragen ihre Mobiltelefone überall mit sich herum und die Geräte zeichnen Informationen über sensible Themen wie Gesundheit, Verhalten, Interessen und sexuelle Orientierung auf. Der Bericht konzentriert sich auf die persönlichen Daten, die von mobilen Anwendungen gesammelt werden, und auf das dahinter verborgene informationstechnische Ökosystem. Er wirft ein Licht auf die kommerziellen Dritten, die im Hintergrund bleiben und heimlich, still und leise unsere persönlichen Daten erhalten und auswerten. Die Analyse in dem Bericht umfasst 10 Apps aus verschiedenen Kategorien (z.B. Dating, Fruchtbarkeits-Tracking, Kinder-Apps) und identifiziert die wesentlichen Probleme:

Persönliche Daten werden systematisch abgesaugt und von diversen Unternehmen unter fragwürdigem und falschem Verweis auf nicht anwendbare Rechtsgrundlagen und in jedem Fall ohne Wissen oder Kontrolle der Verbraucherinnen und Verbraucher verwertet. Insbesondere gilt dabei:

Die Unternehmen erhalten **keine wirksame Einwilligung** der Verbraucherinnen und Verbraucher zur Verarbeitung ihrer persönlichen Daten, auch nicht für die Verarbeitung von Daten, die unter Artikel 9 (besondere Datenkategorien) der DSGVO fallen und daher eine ausdrückliche Zustimmung erfordern.

Die **Unternehmen erfüllen auch nicht die Voraussetzungen, um berechtigte Interessen als Rechtsgrundlage** für die Datenverarbeitung (gemäß Art. 6 Abs. 1 lit. f DSGVO) anführen zu können. Diese Regelung würde ohnehin keine geeignete Rechtsgrundlage für die im Bericht analysierten Verarbeitungsvorgänge darstellen. Die umfassende Profilierung und Kategorisierung von Verbraucherinnen und Verbrauchern dient nicht nur der gezielten Werbung, sondern ist auch noch in verschiedenen anderen Bereichen schädlich und zwar sowohl für die einzelnen Bürgerinnen und Bürger als auch für die Gesellschaft als Ganzes. Zu den negativen Auswirkungen gehören verschiedene Formen der Diskriminierung und der Exklusion, weit verbreiteter Betrug, Manipulation und nicht zuletzt die abschreckende Wirkung, die **massive kommerzielle Überwachungssysteme** sowohl auf Einzelpersonen als auch ganz allgemein auf demokratische Debatten haben können.

Die **einzelnen Personen können dem Tracking nicht ausweichen**, erstens, weil sie nicht mit den notwendigen Informationen versorgt werden, um beim ersten Start der Apps eine informierte Entscheidung zu treffen, zweitens aber auch, weil ihnen als Betroffenen das Ausmaß der Verfolgung, des Datenaustauschs und der allgemeinen Komplexität des Adtech-Ökosystems unverständlich bleibt. Der Einzelne kann nicht wirklich entscheiden, wie seine persönlichen Daten gesammelt, geteilt und verwendet werden.

Selbst wenn einzelne Bürgerinnen und Bürger umfassende Kenntnisse über die Funktionsweise der Adtech-Technologie hätten, gäbe es immer noch nur sehr begrenzte Möglichkeiten, die Datenausbeutung zu stoppen oder zu kontrollieren. Die Anzahl und Komplexität der Akteure, die am Adtech-Ökosystem beteiligt sind, ist erschütternd. Den einzelnen Personen steht so keine sinnvolle Möglichkeit zur Verfügung, sich zu wehren oder sich anderweitig zu schützen.

Aus all dem folgt, dass die im gesamten Adtech-Ökosystem stattfindende massive kommerzielle Überwachung in einem systematischen Widerspruch zu den notwendigen Rahmenbedingungen der Demokratie steht. Studien haben gezeigt, dass Individuen ihr Verhalten entsprechend verändern, wenn sie das Gefühl haben, dass ihre Handlungen erfasst werden und möglicherweise gegen sie verwendet werden können. **Im System des Ad-Tracking wird im Grunde alles aufgezeichnet und für nicht vorhersehbare Zwecke nutzbar gemacht.** Dies kann Folgen auf die Art und Weise haben, wie wir das Internet nutzen und darauf, ob wir bereit sind, nach bestimmten Informationen über die Arbeitsweise unserer Institutionen oder über das Handeln der Politik zu suchen. Und das ist auch der Grund, warum die kommerzielle Überwachung langfristig schwerwiegende Folgen für den Zugang der Menschen zu Informationen, für ihre Meinungsfreiheit, für die demokratischen Institutionen und für die Gesellschaft als Ganzes haben kann.

Eine massive kommerzielle Überwachung kann unsere Grundrechte und Freiheiten auch auf direktere Weise gefährden. In Ägypten zum Beispiel hat die Polizei die Dating-App Grindr eingesetzt, um Homosexuelle zu identifizieren und zu verhaften [2]. Wenn Standortdaten an Hunderte von Unternehmen weitergegeben werden, muss nur eines dieser Unternehmen die Daten selbst weitergeben oder gehackt werden, um Menschen in physische Gefahr zu bringen.

Auf Grundlage dieser Erkenntnisse hat der norwegische Verbraucherrat bei der norwegischen Datenschutzbehörde eine Reihe von Beschwerden gegen verschiedene Adtech-Firmen und die Dating-App Grindr eingereicht. Die nationalen Regulierungs- und Aufsichtsbehörden müssen aktive Maßnahmen ergreifen, um diese Probleme anzugehen und um durchzusetzen, dass die Adtech-Industrie ihre Arbeitsweise grundlegend ändert.

Wir hoffen, dass Sie unsere Bedenken bezüglich der in diesem Bericht angesprochenen Themen teilen. Die Untersuchung wurde in Norwegen durchgeführt, aber einige der analysierten Anwendungen (z.B. Grindr, siehe https://de.wikipedia.org/wiki/Grindr und dort Entstehung und Verbreitung, oder auch Tinder, siehe https://tinder.com/?lang=de) sind auch in Deutschland tätig, und die Adtech-Firmen, gegen die sich die Beschwerde des norwegischen Verbraucherrats wie auch von noyb [3] richtet, verarbeiten mit hoher Wahrscheinlichkeit auch Daten deutscher Verbraucherinnen und Verbraucher.

Wir bitten Sie daher dringend, diesen dargestellten Problemen nachzugehen und die norwegische Aufsichtsbehörde bei der Bearbeitung der Originalbeschwerden durch parallele Bemühungen innerhalb der EU zu unterstützen. Die Bedenken, die durch die kommerzielle Überwachung und die Praktiken der Adtech-Industrie aufgeworfen werden, betreffen die gesamte EU.

Über eine Rückmeldung zu Ihren geplanten Aktivitäten zu diesen Problemen möchten wir Sie bitten.

Dieses Schreiben ist in enger Zusammenarbeit der Deutschen Vereinigung für Datenschutz mit Digitalcourage, der Digitalen Gesellschaft, dem Netzwerk Datenschutzexpertise und Liberties.eu entstanden.

Als Anlage zu diesem Schreiben haben wir Ihnen das DANA-Sonderheft 2-2019 mit dem Themenschwerpunkt Real Time Bidding beigefügt [4], in diesem werden einige Themen besprochen, die auch im Bericht angesprochen werden.

[1] Siehe https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf
[2] Siehe z.B. Article 19: LGBTQ ONLINE Summary Report. Apps, arrests and abuse in Egypt, Lebanon and Iran. February 2018. https://www.article19.org/wp-content/uploads/2018/02/LGBTQ-Apps-Arrest-and-Abuse-report_22.2.18.pdf
[3] Siehe https://noyb.eu/out-of-control/?lang=de
[4] https://www.datenschutzverein.de/wp-content/uploads/2019/09/DANA_19_3_Sonderheft_Real_Time_Bidding.pdf

---

Über die Deutsche Vereinigung für Datenschutz (DVD):

Die DVD nimmt seit ihrer Gründung 1977 als gemeinnütziger Verein die Interessen der verdateten BürgerInnen wahr. Die DVD sieht ihre Aufgabe vorrangig darin, die Bevölkerung über Gefahren des Einsatzes elektronischer Datenverarbeitung und der möglichen Einschränkung des Rechts auf informationelle Selbstbestimmung zu beraten und aufzuklären Inhaltlich beschäftigt sich die DVD mit so unterschiedlichen Fragestellungen wie dem Datenschutz in Polizei und Justiz, dem Beschäftigten-datenschutz, Verbraucherdatenschutz und Datenschutz im Internet.