AK EUROPA

Positionspapier
Dezember 2019
KonsumentInnen

Verordnung über Privatsphäre und elektronische Kommunikation:

Die digitale Privatsphäre muss besser geschützt werden!

COM (2017) 10 final

Die Position der AK

Die Absicherung eines hohen VerbraucherInnenschutzniveaus und die Entwicklung eines sektorspezifischen Datenschutzrechts in Europa ist uns ein besonderes Anliegen. Wir setzen uns daher mit besonderem Nachdruck dafür ein, dass die Bedürfnisse der Telekom- und InternetnutzerInnen an einem zeitgemäß strengen Schutz ihrer Privatsphäre und persönlichen Daten ausreichend berücksichtigt werden.

Überwachung „zum Quadrat“

KonsumentInnen bewegen sich durch einen dicht vernetzten Alltag. Wer elektronisch kommuniziert, hinterlässt unweigerlich Spuren: die Liste der gewählten Rufnummern im Handy, die für Verrechnungszwecke und anonymisierte Standortauswertungen gespeicherten Verkehrsdaten beim Mobilfunkbetreiber, „Cookies“ im Webbrowser, Zugriffsprotokolle auf Webservern, das Mailserver-Protokoll beim Internet Service Provider (ISP), das Nutzungsprofil beim Smart-Home-Anbieter usw. Geodaten eines Smartphones können sogar sensible Informationen liefern: ob jemand wiederholt ein Krankenhaus oder eine religiöse Einrichtung besucht etc. Auch scheinbar harmlose (Beschleunigungs-) Sensordaten können offenlegen, ob eine Person am Arbeitsplatz sitzt, sich zu Hause aufhält oder gerade mit dem Auto unterwegs ist. Die Speicherung und die Nutzung solcher Daten berühren den Kern der Privatsphäre.

Jeder Berührungspunkt mit smarten Geräten hinterlässt persönliche Datenspuren, die in umfassenden individuellen Nutzungs- und Standortprofilen oder in nicht weniger brisanten Zuordnungen zu pseudonymisierten/anonymisierten Gruppen nach bestimmten Verhaltensmustern bzw. Prognosen über künftiges Verhalten münden können. Die Schnittstellen mit dem Internet, an denen VerbraucherInnenverhalten beobachtet, gespeichert, ausgewertet und Dritten übermittelt werden kann, ergeben ein einzigartig genaues Bild über das, was wir tun, lassen, denken, mit wem wir in Kontakt stehen u.v.m.

Zum Hintergrund

Der von der EU-Kommission 2017 veröffentlichte Entwurf soll die bisherige e-Privacy-Richtlinie ablösen. Art 1 der neuen Verordnung legt als Ziel den Schutz der Grund- und Freiheitsrechte natürlicher Personen bei der Nutzung von elektronischen Kommunikationsdiensten fest. Leitende Maxime soll das Recht der InternetnutzerInnen auf Privatsphäre, Datenschutz und Vertraulichkeit der Kommunikation sein. Das klingt zunächst vielversprechend. Immerhin zeigte eine Eurobarometerumfrage schon 2015, wie sehr sich KonsumentInnen um ihre digitalen Rechte sorgen: 78 % finden, dass OnlineanbieterInnen zu viel KundInnendaten besitzen; 73% wollen immer um ihre ausdrückliche Zustimmung gefragt werden. Jahre später und um etliche Eindrücke (wie den Datenmissbrauch durch Facebook/Cambridge Analytica) reicher hat sich das Stimmungsbild kaum geändert.

Zusammengefasste Kritik

Die aktuelle Diskussion im Rat löst die Erwartungen der KonsumentInnen nicht ein. Im Gegenteil: Die Überarbeitungen dienen dazu, den freien Datenfluss in Europa zu fördern.

- **Bisher** dürfen die Metadaten der Telekom- und InternetanbieterInnen (etwa Standort oder Verbindungszeitpunkt der KonsumentInnen) nur für die Herstellung der Verbindung, Netzsicherheit, Abrechnung und – Zustimmung vorausgesetzt – für eigene Marketingzwecke und Zusatzdienste genutzt werden.

- **Künftig** dürften Unternehmen, Wissenschaft und Forschung, die direkten - oder über den Zukauf anonymisierter Daten indirekten - Zugang zu Metadaten haben, Metadaten zu unzähligen Zwecken, vielfach ohne Zustimmung der Betroffenen und – wenn pseudonymisiert - zeitlich unlimitiert nutzen. Unternehmen dürften ohne Zustimmung der KonsumentInnen über Cookies und andere Techniken für ungenau bestimmte Zwecke wie Sicherheit, Betrugserkennung oder statistische Zählung auf deren Endgeräte zugreifen.

Die Pflicht von BrowserherstellerInnen, zumindest Privacy-Einstellungsoptionen anzubieten, wurde hingegen ersatzlos gestrichen. Die gar nicht grundrechtliche Begründung dafür: Vorteile für US-BrowserherstellerInnen.

- **Ausblick**: Die Letztentwürfe haben sich vom Grundrechtsziel abgewandt und streben Wachstumsimpulse für die Digitalindustrie an. Digitalwirtschaft und wirtschaftsnahe Wissenschaft bzw Forschung möchten die Möglichkeiten datengetriebener Geschäftsmodelle noch viel weiter ausschöpfen. Die herabgesetzten Schranken für die Nutzung von Metadaten und den Zugriff auf Endgeräte werden als Hürde betrachtet – etwa für das lukrative Ausspähen des Verhaltens von InternetnutzerInnen via Cookie-Walls (als Gegenleistung für angebotene Internetinhalte), das physische Tracking der Bewegung von Personen über die Handys in ihrer Hosentasche bspw in Shops oder Einkaufszentren, die kommerzielle Verwertung von „Big Data", die smarte Geräte massenhaft erzeugen oder den Bedarf an zusätzlichen Trainingsdaten für die Entwicklung künstlicher Intelligenz.

- **Was KonsumentInnen wollen**: Die Alltagsabhängigkeit von elektronischer Kommunikation ist groß. KonsumentInnen haben kaum Wahlmöglichkeiten. Sie unterwerfen sich auch Bedingungen der BetreiberInnen, die sie eigentlich ablehnen, um am digitalen Leben teilhaben zu können. Ohne Bekenntnis zu einem strikten Grundrechtsschutz in der e-Privacy Verordnung, der auch klare Ge- und Verbote umfasst, gibt es keine Selbstbestimmung für NutzerInnen von Smartphones, PCs, smarten Autos und Heizungen usw. in Bezug auf ihre Daten und ihre Privatsphäre. Mit Blick auf die eingangs zitierten Anliegen der KonsumentInnen („Anbieter greifen online viel zu viele Daten ab"; „Wir wollen stets um unsere Zustimmung zur Datennutzung gefragt werden") müsste das Selbstbestimmungsrecht und der Datenminimierungsgrundsatz eigentlich gestärkt statt immer weiter abgesenkt zu werden.

- **Die rote Linie**: Der Kommissionsentwurf aus 2017 erweiterte den Spielraum für die kommerzielle Datennutzung im Vergleich zum Schutz, den die europäische BürgerInnen gem. der Richtlinie 2002/58/EG derzeit noch genießen. Eine noch weitergehende Aufweichung der Schutzstandards ist unakzeptabel.

VerbraucherschützerInnen fordern daher: Die digitale Privatsphäre muss besser geschützt werden!

Was sich ändern muss

Keine Kommerzialisierung von Metadaten ohne Zustimmung der KonsumentInnen

Für Datenverwendungszwecke, die für die Diensterbringung unerheblich sind, ist ausnahmslos die Zustimmung der Betroffenen einzuholen. Die Nutzung von Metadaten für andere „kompatible" Zwecke muss ohne Zustimmung der Betroffenen untersagt sein (ein bloßes Widerspruchsrecht reicht nicht). Eine Datennutzung zur Erkennung von Missbräuchen durch NutzerInnen ist zu unbestimmt und kann stets behauptet werden, um die Daten nicht sofort löschen oder anonymisieren zu müssen. Eine Datennutzung für statistische oder wissenschaftliche Zwecke (in verschlüsselter oder pseudonymisierter Form) ist ohne Zustimmung der KonsumentInnen ebenfalls undenkbar. Bei Verarbeitungen im besonderen öffentlichen Interesse kann eine Genehmigung der Datenschutzbehörde Einzelzustimmungen ersetzen.

Die Nutzbarkeit von Metadaten ginge künftig über das bisherige Maß (Netzsicherheit, Gebührenabrechnung, Vermarktung von Kommunikationsdiensten oder Bereitstellung von Diensten mit Zusatznutzen jeweils mit vorheriger Zustimmung der/des NutzerIn) hinaus. Auch die EU-Kommission erkennt an, dass die NutzerInnen „die Kontrolle über die Verwendung ihrer elektronischen Kommunikationsdaten für andere Zwecke als die Übertragung der Kommunikation" haben wollen (EG 17). Für andere Verwendungszwecke sollte daher ausnahmslos die Zustimmung der Betroffenen einzuholen sein. Ohne Zustimmung der Betroffenen sollte die Nutzung von Metadaten für mit dem Ursprungszweck „kompatible" Zwecke untersagt sein. Auch für statistische oder wissenschaftliche Nutzungen sollte eine Zustimmung eingeholt werden müssen. Denn auch die Nutzung pseudonymisierter (jederzeit auf die Person rückführbarer) Daten ist ein Grundrechtseingriff. Selbst die Zuordnung zu anonymisierten Gruppen anhand von Verhaltensmerkmalen kann negative Folgen für KonsumentInnen nach sich ziehen (Verhaltenssteuerung, Manipulation, Diskriminierung uvm). Nach Wunsch der online-Wirtschaft bestünde dagegen nicht einmal ein ausdrückliches Widerspruchsrecht.

E-Privacy heißt vor allem „Do not track!“

Pflicht zu strikten Voreinstellungen bei Hard- und Software: Die Verordnung muss konkretisieren, wie Handys und Webbrowser datensparsam voreinzustellen sind.

Quer durch Europa klagen KonsumentInnen- und DatenschützerInnen, dass ein wirksamer Schutz vor einer der größten Bedrohungen für die Privatsphäre, dem Ausspähen des Verhaltens von InternetnutzerInnen, fehlt. DatenanalystInnen übertreffen sich mit der algorithmischen Auswertung des Surfverhaltens: Ob Klassifizierung von Personen nach ihren Eigenschaften und Vorlieben oder Prognosen über ihr künftiges Verhalten – der Zugriff auf die Endgeräte der NutzerInnen und das Schürfen mit Analysetools in den abgesaugten Geräteinformationen bedeutet für Internetkonzerne Gewinne, für die Betroffenen den Verlust ihrer Privatsphäre.

Cookies (und andere Technologien) dienen dem Ausforschen des Surfverhaltens. Dem Entwurf zufolge ist jede von NutzerInnen nicht selbst vorgenommene Nutzung der „Verarbeitungs- und Speicherfunktion“ von Endgeräten grundsätzlich verboten (vorbehaltlich weitreichender Ausnahmen). Die DSGVO ordnet technischen Datenschutz „by default“ (strengst mögliche Voreinstellung bei Geräten und Software) an. Diese Vorschrift muss in der Verordnung konkretisiert werden - sonst bleibt sie totes Recht. Die Zustimmung zum Zugriff auf Endgeräte kann auch über die vom NutzerInnen vorausgewählte Browsereinstellung eingeholt werden. „Do Not Track“ ist der Name einer Webtechnologie, die in modernen Browsern als Option angeboten wird. Wer sie aktiviert, teilt besuchten Websites automatisch mit, dass er/sie der Speicherung von Daten bspw zur Erstellung von NutzerInnenprofilen widerspricht. Browser mussten dem Erstentwurf zufolge aber nicht auf die datenschutzfreundlichste Variante voreingestellt sein. NutzerInnen soll lediglich eine Reihe von Einstellungsmöglichkeiten angeboten werden. Art 10, der diese Anordnung enthielt, wurde ersatzlos gestrichen. Dabei ergab eine Eurobarometer-Umfrage der EU-Kommission aus 2016, dass 40% der befragten ÖsterreicherInnen ihre Browsereinstellungen aus Überforderung nicht ändern. Wenig internetaffinen Personen müsste durch datenschutzfreundliche Voreinstellungen unbedingt unter die Arme gegriffen werden.

Nein zu „Verfolgungsdiensten“: Kein Zugriff auf Endgeräte aus Gründen statistischer Zählung und keine physische Überwachung durch „Verfolgungsdienste“ ohne Zustimmung der Betroffenen

Der Entwurf öffnet auch im Offline-Alltag ein Tor zur Überwachung von KonsumentInnen. Shops, die ihre KundInnen (über deren Smartphones und WLAN- oder Bluetooth-Verbindungen) identifizieren und ihre Bewegungen bzw. Aufenthaltsdauer verfolgen wollen, bräuchten nicht einmal deren Zustimmung einholen. Eine bloße Kennzeichnung – etwa im Laden - soll reichen. Der Erstentwurf bezeichnete das Scannen gerätebezogener Informationen äußerst treffend als „Verfolgungsdienst“ zwecks Zählung von Personen, Daten über die Zahl der in der Schlange wartenden Personen, Übermittlung von individuell abgestimmter Werbung oder Verfolgung einzelner Personen über einen längeren Zeitraum.

Dieses Offline-Tracking soll künftig ohne die Einwilligung der VerbraucherInnen erlaubt sein. VerbraucherInnen sollen lediglich durch Kennzeichnung darauf hingewiesen werden, dass sie einen überwachten Bereich betreten. Hinzuweisen ist auf den Zweck der Verfolgung, die dafür verantwortliche Person und was die/der Betroffene tun kann, um die Datenerhebung zu beenden oder auf ein Minimum zu beschränken. 54% der vom deutschen VerbraucherInnenverband VZBV befragten KonsumentInnen lehnen ein solches Personen-Tracking kategorisch ab. Sie halten ein ausdrückliches Verbot für die einzig adäquate Antwort auf diese Entwicklung. Auch für die AK sind solche Datennutzungen ohne ausdrückliche Einwilligung der Betroffenen undenkbar.

Kein Zugriff auf Endgeräte ohne Zustimmung der NutzerInnen, um technische Fehler oder Betrug zu erkennen

Ein solches Zugriffsrecht ist zu weitreichend und kann für rechtswidrige Datennutzungen missbraucht werden. Mit der Pflicht, eine wirksame Zustimmung einzuholen, wäre zumindest gewährleistet, dass KonsumentInnen über alle wichtigen Verarbeitungsdetails (wofür, auf welcher Rechtsgrundlage, in welchem Umfang, wie lange usw) auch tatsächlich informiert werden. Nur so können Betroffene überschießende Zugriffe hinterfragen und werden nicht ihrerseits Opfer intransparenter, missbräuchlicher Datennutzungen.

Kontaktieren Sie uns!

In Wien:

Daniela Zimmer
T +43 (0) 1 501 651 2722
daniela.zimmer@akwien.at

Bundesarbeitskammer Österreich
Prinz-Eugen-Straße 20-22
1040 Wien, Österreich
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

In Brüssel:

Peter Hilpold
T +32 (0) 2 230 62 54
peter.hilpold@akeuropa.eu

AK EUROPA
Ständige Vertretung Österreichs bei der EU
Avenue de Cortenbergh 30
1040 Brüssel, Belgien
T +32 (0) 2 230 62 54

www.akeuropa.eu

Über uns

Die Bundesarbeitskammer (AK) ist die gesetzliche Interessenvertretung von rund 3,8 Millionen ArbeitnehmerInnen und KonsumentInnen in Österreich. Sie vertritt ihre Mitglieder in allen sozial-, bildungs-, wirtschafts- und verbraucherpolitischen Angelegenheiten auf nationaler sowie auch auf der Brüsseler EU-Ebene. Darüber hinaus ist die Bundesarbeitskammer Teil der österreichischen Sozialpartnerschaft. Die AK ist im EU-Transparenzregister unter der Nummer 23869471911-54 registriert.

Die Aufgaben des 1991 eröffneten AK EUROPA Büros in Brüssel sind einerseits die Repräsentation der AK gegenüber europäischen Institutionen und Interessensorganisationen, das Monitoring von EU-Aktivitäten und die Wissensweitergabe von Brüssel nach Österreich, sowie gemeinsam mit den Länderkammern erarbeitete Expertise und Standpunkte der Arbeiterkammer in Brüssel zu lobbyieren.