

Digitalcourage e.V. · Marktstraße 18 · 33602 Bielefeld

Berlin, 5. Januar 2015

Stellungnahme von Digitalcourage e.V.

zur schriftlichen Anhörung zum Entwurf einer Regelung zum Profiling (Art. 20 und Art. 20a)

Digitalcourage bedankt sich beim Bundesministerium des Innern (BMI) für die Möglichkeit einer schriftlichen Stellungnahme zur Regelung des Profilings in der EU-Datenschutzverordnung und steht für einen weiteren Austausch auch in Zukunft gerne zur Verfügung.

Der Entwurf der Datenschutzverordnung seitens der Kommission enthält in Art. 20 eine spezielle Regelung zum Profiling und der Verwendung von Profilen. Grundsätzlich möchten wir anmerken, dass Profilbildung ein in höchstem Maße kritischer Anwendungsbereich für alle Menschen, insbesondere in ihrer Rolle als Verbraucherinnen und Verbraucher, ist. Deshalb braucht es eine umfassende Definition von Profiling, die gleichzeitig verbraucherfreundlich und zukunftsweisend ist. Weiterhin ist zu berücksichtigen, dass Profiling an verschiedenen Schnittpunkten des Datenschutzrechts steht: Zum einen könnten auch nicht-persönliche Daten für ein Profil gesammelt werden um persönliche Profile „anzureichern“ (etwa mit zunächst unpersönlichen Merkmalen, aggregierten Aufenthaltsdaten oder öffentlichen Social-Media-Daten), zum anderen sind auch Profile ex negativo denkbar, dann nämlich, wenn bestimmte Personen dem Profiling widersprechen (und genau dieser Widerspruch selbst Bestandteil eines Profils wird) oder sozusagen das Profiling (etwa bei Versicherungstarifen) zum Standard erklärt wird und zum Beispiel ein Vertrag ohne Profiling dadurch automatisch teurer wird. Eine solche Entwicklung und die damit einhergehende Aufhebung des Solidaritätsprinzips lehnt Digitalcourage entschieden ab.

Forderungen:

- Profiling muss eng begrenzt werden. Die „besondere Zulässigkeitsanforderungen“ finden sich auch im Koalitionsvertrag, sind im vorliegenden Entwurf des BMI und BMJV allerdings viel zu weit gefasst.
- Der Profilbildung an sich muss widersprochen werden können, nicht erst den Entscheidungen, die auf Profilen beruhen.
- Wenn Profile erstellt werden, müssen die betroffenen Personen umfassende Informationsrechte haben.
- Bestimmte Datenkategorien dürfen nicht für die Erstellung von Profilen herangezogen werden.
- Pseudonyme Daten dürfen keine Generalvollmacht für die Profilbildung sein.

Eine Aufteilung in „Profilbildung“ und „Entscheidung auf der Basis von Profilbildung“ ist nicht sinnvoll abzulehnen. Profiling als solches ist eine Datenverarbeitung unter vielen, die nur deshalb eines eigenen Paragraphen bedarf, weil sie besonders kritisch in das Recht auf informationelle Selbstbestimmung eingreift. Würde man Profiling allerdings so weitgehend erlauben, wie im vorliegenden Entwurf, würde der Artikel 6 für diese Art der Datenverarbeitung vollkommen ausreichen. Da aber Profiling als solches und seine Auswirkungen auf das informationelle

Selbstbestimmungsrecht besonders kritisch sind, bedarf es einer Einschränkung schon bei der Erstellung der Profile, nicht erst bei deren Anwendung.

Erläuterung:

Die Definition des Profilings im vorgeschlagenen Art. 4, Abs 12a ist zu umfangreich für die erklärten Ziele. Profiling stützt sich nicht nur auf persönliche Daten der betroffenen Person, sondern auch auf aggregierte, nicht persönliche Daten, die dennoch ein sehr genaues Bild zeichnen und erst durch die Aggregation zu personenbezogenen Daten werden. Beispiele dafür seien der Browserfingerabdruck, der als solcher pseudonym ist, und eine betroffene Person dennoch in über 90 % der Fälle eindeutig identifiziert. Auch bloße Aufenthaltsdaten sind als solche pseudonym, da sie nicht mit dem Namen der betroffenen Person verknüpft sind, und dennoch individuell und eindeutig. Auch geht nicht klar aus der Definition hervor, was die „data subject’s personality“ sein soll, die als neuer Begriff in die Datenschutzverordnung eingeführt werden würde.

Die Ausführungen der Anwendungsmöglichkeiten im neuen Artikel 20 spiegeln im wesentlichen Artikel 6 der DSGVO wider, der die Datenverarbeitung unter bestimmten Bedingungen erlaubt, weiten diese für das besonders kritische Profiling aber sogar noch aus.

Aus Verbrauchersicht ist es nicht verständlich, warum das **Listenprivileg** Einzug in die Datenschutzverordnung erhält. Dieses Privileg ist schon im derzeitigen BDSG höchst umstritten und lässt Verbraucherinnen und Verbraucher häufig schutzlos zurück, da sie, wenn überhaupt nur eine Einwilligung als Möglichkeit der Weitergabe vermuten und auch die Anzahl der Stellen, an die die Daten weitergegeben wurden, sehr schnell sehr unübersichtlich wird.¹ Diese Regelung in die Datenschutz-Grundverordnung zu übernehmen, hieße, Facebook und Co. noch weiterreichende Erlaubnisse zur Datenvermarktung zu geben.

Die Einwilligung in die Profilbildung darf nur zulässig sein, wenn zwischen der betroffenen Person und der profilbildenden Stelle kein Ungleichgewicht herrscht. Zum Beispiel dürfen Arbeitgeber die Einwilligung nicht zur Profilbildung über die Arbeitsgewohnheiten ihrer Mitarbeiter heranziehen, da Arbeitnehmer hier nicht frei einwilligen können.

Die Verarbeitung von **pseudonymen Daten** zur Profilbildung lehnt Digitalcourage generell ab. Werbetreibende und Webseitentracker wissen, wie lange wer auf welchen Seiten im Internet gesurft haben und verknüpfen diese Informationen häufig mit unserem Aufenthaltsort, mit Social-Media-Daten und in Zukunft auch mit den Daten unserer Wearables und unseres Smart Homes. All das als sogenannte „pseudonyme“ Daten, die doch ein lückenloses Bild unserer Person zeichnen. Da durch Art. 6 Abs. 5 gleichzeitig umfassende Re-identifizierung möglich ist, könnten in Zukunft Versicherungstarife bei Krankenkassen, Autoversicherungen oder auch Kreditverträge auf solchen angeblich pseudonymen Profilen beruhen, ohne dass die betroffene Person die Möglichkeit hat, zu widersprechen. Hier ist Diskriminierung vorprogrammiert.

1 Vgl. <http://www.stern.de/politik/deutschland/meldegesetz-und-adresshandel-die-datensammler-lauern-ueberall-1854271.html> und <https://krautreporter.de/163--ein-ausflug-in-die-datenminen>

Die Verarbeitung von **öffentlichen Daten** für die Profilbildung lehnt Digitalcourage generell ab. Bürgerinnen und Bürger sehen sich schon heute damit konfrontiert, dass Dritte Daten über sie veröffentlichen, die ihnen nicht recht sind. Solche Daten dürfen nicht für die Profilbildung herangezogen werden. Gleichzeitig kann diese Situation zu erheblicher Unsicherheit auf Seiten der Profilbildenden führen, ob diese Daten überhaupt rechtmäßig verwendbar sind. Nicht zuletzt dient das Verbot, Social-Media-Daten und Daten aus öffentlichen Quellen für die Profilbildung heranzuziehen auch der Vermeidung von „false positives“ und damit der Rechtssicherheit sowohl der Bürgerinnen und Bürger als auch der datenverarbeitenden Unternehmen. Außerdem stünde die Verwendung solcher Daten im Spannungsverhältnis mit dem Urteil des EuGH zum „Recht auf Vergessen“, in dem der EuGH geurteilt hat, dass Google als datenverarbeitende Stelle ein Profil (!) der betroffenen Person anlegt, das Google allerdings nicht zum Zweck des Profiling erstellt.

Profilbildung darf nicht zu **Diskriminierung** führen. Die im Entwurf vorgesehene Liste (Art. 20, Abs. 3) ist nicht vollständig, da zumindest auch die Kategorie „geschlechtliche Identität“ fehlt, aufgrund derer auch nicht diskriminiert werden darf. Gleichzeitig sind durch umfassendes Profiling auch etwaige andere Kategorien für eine mögliche Diskriminierung denkbar, etwa nach „Gewicht“, „Lebenswandel“, „Arbeitsleistung“ etc. Auch diese bisher noch nicht berücksichtigten Kategorien dürfen nicht zu Diskriminierung führen.

Die Profilbildung von **Kindern** muss untersagt werden.

Profiling ist eine in höchstem Maße in die Privatsphäre der Menschen eingreifende Methode, die aber in bestimmten Fällen durchaus gerechtfertigt sein kann. Um diese Fälle zu stärken und das Vertrauen der Menschen in die dahinterstehende Technologie zu fördern, bedarf es umfassender **Transparenz- und Informationsrechte** für Verbraucherinnen und Verbraucher. Profiling muss auf wissenschaftlich anerkannten Methoden basieren und die Datenkategorien, aufgrund derer ein Profil erstellt wird, müssen offengelegt werden.