WIEN / 09. Mai 2019

STELLUNGNAHME

Zum Ministerialentwurf für ein Bundesgesetz, mit dem das Digitalsteuergesetz 2020 erlassen und das Umsatzsteuergesetz 1994 geändert wird (132/ME XXVI. GP)

Für epicenter.works
Ing. Mag. Dr. Christof Tschohl
Iwona Laub
Mag.ª Angelika Adensamer, MSc

1 VORWORT UND KURZFASSUNG

Die österreichische Bundesregierung hat am 6.4. einen Gesetzesentwurf zu einem Digitalsteuergesetz[1] vorgelegt und wenige Tage später am 10.4. ihre Pläne zum Ausweiszwang in digitalen Foren[2] veröffentlicht. Beide Vorschläge verletzen jeweils einzeln die Grundrechte auf Datenschutz nach Artikel 8 sowie auf Meinungs- und Informationsfreiheit nach Artikel 11 EU Grundrechte-Charta sowie die entsprechenden innerstaatlich gewährleisteten Grundrechte nach § 1 Datenschutzgesetz und Artikel 10 EMRK. In Summe verletzen sie den Wesensgehalt dieser Grundrechte.

Die vorgeschlagene Variante der Digitalsteuer bringt – angeblich als nicht beabsichtigter Nebeneffekt – eine für Österreich flächendeckende, staatlich vorgeschrieben Vorratsdatenspeicherung der meisten Internetzugriffe, die vor allem durch die größten AnbieterInnen von Diensten der Informationsgesellschaft durchgeführt wird. Dabei müssen verbundene Informationen über Inhalte und Verkehrsdaten (Zugangsdaten, IP-Adressen) gespeichert werden. Zugleich soll ein „digitaler Ausweiszwang" alle NutzerInnen, die sich aktiv an der Kommunikation in Internet-Foren beteiligen wollen, mit Ihrer richtigen Identität erfassen – natürlich sind auch hier die AnbieterInnen der Dienste der Informationsgesellschaft in der „Pflicht" (bzw. erhalten das Privileg!). Dabei handelt es sich vielfach um dieselben AnbieterInnen, die nach der Digitalsteuer Vorratsdatenspeicherung betreiben müssen (bzw. dürfen).

Mit dem Vorschlag zum Digitalsteuergesetz würde auf nationaler Ebene erlaubt, was bisher durch die E-Privacy Richtlinie verboten ist und was dem Datenschutzgrundrecht widerspricht. Die Speicherung der IP-Adresse von NutzerInnen und der Internet-Ressource, auf die zugegriffen wurde, nur weil dort Werbung angezeigt wird, wäre jedenfalls allein im Interesse der verpflichteten AnbieterInnen nicht rechtmäßig. Das heißt, der nationale Gesetzgeber dürfte keine gesetzliche Regelung erlassen, die es den AnbieterInnen für deren eigene Interessen erlaubt, diese Daten zu speichern. Der Entwurf schafft nun eine Verpflichtung, verbietet aber nicht ausdrücklich die Nutzung der Daten für andere Zwecke.

Durch eine gesetzliche Verpflichtung im nationalen Steuerrecht wird damit auch indirekt in Unionskompetenzen im Rahmen der Telekommunikations- und Informationsdienste-Regulierung eingegriffen. Damit ist jedenfalls auch der Anwendungsbereich der EU Grundrechte-Charta betroffen.

Gerade die großen AnbieterInnen aus Drittstaaten, die bereits massive Datensammlungen betreiben, haben durch dieses Gesetz große Vorteile. Unternehmen wie Google werden damit dazu getrieben, Daten über alle Webseitenzugriffe für mindestens sieben Jahre zu speichern. Die Erfahrung zeigt, dass trotz der gesetzlich strengen Zweckgebundenheit der Datenverarbeitung, solche Datenbestände nach und nach auch für andere Zwecke verwendet werden, sei es durch neue Auskunftsrechte, erweiterte Gesetzesbestimmungen, etc. Der sog. „Function-Creep", also die schrittweise spätere Ausdehnung über den ursprünglichen Zweck hinaus ist damit praktisch perpetuiert und die AnbieterInnen werden im Rahmen des Art 6 Abs 4 DSGVO auch durchaus „kompatible" Spielräume zu begründen versuchen. Der wirtschaftliche Wert des Datenbestands für die verpflichteten AnbieterInnen, der von denselben AnbieterInnen zwingend über Zeiträume von mindestens sieben Jahren und länger gespeichert

1 https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00132/index.shtml.

2 Siehe dazu https://epicenter.works/content/das-mitmach-internet-in-gefahr-bundesregierung-will-ausweiszwang-im-internet-einfuehren (abgerufen am 9.5.2019).

werden muss, übersteigt mit großer Wahrscheinlichkeit das geschätzte Steueraufkommen, welches der Entwurf bezweckt. Dass die Datennutzung im Interesse der verpflichteten AnbieterInnen selbst auf Dauer unzulässig bliebe, darf nach der allgemeinen Erfahrung bezweifelt werden. Damit wird eine zynische digital-kapitalistische Spirale in Gang gesetzt, bei der die große Mehrheit der Menschen mit Ihren Grundrechten bezahlt und als SteuerzahlerIn einen äußerst nachteiligen Handel eingeht.

Nichtsdestotrotz lehnt auch der Providerverband ISPA die Vorschläge mit massiver Kritik an den Grundrechtseingriffen ab und kooperiert dabei mit VertreterInnen der Zivilgesellschaft. Wir verweisen daher auch auf die Stellungnahme[3] der ISPA im parlamentarischen Begutachtungsverfahren vom 7.5.2019. Insbesondere wird auf deren Kritik an der grob mangelhaften Bestimmtheit der eingeführten Begriffe verwiesen, die bei einem so weit gehenden Grundrechtseingriff den Rechtsstaatsgrundsatz verletzt. Insgesamt wird eine der Komplexität angemessene, bisher fehlende öffentliche Debatte gefordert.

Inhaltsverzeichnis

3 ISPA Stellungnahme: https://www.parlament.gv.at/PAKT/VHG/XXVI/SNME/SNME_04317/index.shtml (abgerufen am 9.5.2019).

2 ALLGEMEIN

Die vorliegende Stellungnahme beschäftigt sich mit dem Vorschlag zum Digitalsteuergesetz und nicht dem zum Umsatzsteuergesetz, der auch Teil der Novelle ist, und widmet sich dabei insbesondere den datenschutzrechtlichen Aspekten des vorliegenden Entwurfs. Dennoch ist es dringend geboten, den Blick auf das größere Bild nicht zu verlieren. Dazu gehört auch, dass für die Begutachtung zu diesem Gesetzesvorschlag eine Frist von vier Wochen eingeräumt wurde, wobei dazwischen Ostern und der Staatsfeiertag zum 1. Mai gelegen sind und parallel dazu das nur unwesentlich längere Begutachtungsverfahren zum „digitalen Ausweiszwang" läuft. epicenter.works appelliert an die Bundesregierung und das Parlament, die demokratiefeindliche Praxis unangemessen kurzer Begutachtungsphasen zu unterlassen und einen sachlichen Diskurs nicht willkürlich zu beschneiden.

Aufgrund der knappen Zeit konzentriert sich die vorliegende Stellungnahme vor allem auf die Pflicht zur Speicherung aller Zugangsdaten von Seitenzugriffen sowie Standortdaten der Geräte durch Online-Werbeträger wie z.B. Facebook und Google. Der Umfang ist eher kurz gehalten und auf das Wesentliche konzentriert, wo möglich wird auf andere bereits ausformulierte Positionen verwiesen. Es wird dringend gefordert, eine öffentliche Debatte über alternative Möglichkeiten der Feststellung des Steueraufkommens ohne Verarbeitung von NutzerInnendaten zu führen. epicenter.works steht für eine offene, sachliche und ernsthafte Debatte wie immer zur Verfügung.

3 ARTIKEL I – DIGITALSTEUERGESETZ 2020 (DISTG 2020)

Grundrechtseingriff durch die Bestimmung des Inlandsbezugs anhand der IP-Adresse

Nach dem Entwurf gilt „eine Onlinewerbeleistung [...] als im Inland erbracht, wenn sie auf dem Gerät eines Nutzers mit inländischer IP-Adresse erscheint und sich ihrem Inhalt und ihrer Gestaltung nach (auch) an inländische Nutzer richtet." (§ 1 Abs 1 DiStG) Demnach soll also die IP-Adresse als entscheidendes Kriterium zur Bestimmung des Abgabentatbestands durch den „Onlinewerbeleister" in Verbindung mit den Inhalten, über welche die Werbung bei den NutzerInnen erscheint, gespeichert werden.

Die IP-Adresse ist nach der Rechtsprechung des EuGH in der Rechtssache Breyer (C-582/14) jedenfalls als personenbezogenes Datum zu sehen. In Verbindung mit den jeweiligen Inhalten entsteht zu allen NutzerInnen eine personenbezogene Informationssammlung, die dem Schutz des Datenschutzgrundrechts nach § 1 DSG unterliegt. Der vorgeschlagene Gesetzesentwurf greift in dieses Grundrecht ein und bietet dafür keine hinreichende Rechtfertigung. Außerdem liegt ein Eingriff in die Meinungs- und Informationsfreiheit vor, der durch die flächendeckende Speicherung bewirkte „chilling-effect" oder „ripple-effect" ist in der Judikatur des EuGH mittlerweile Legion (siehe dazu zB die Entscheidungen zur Vorratsdatenspeicherung[4]).

Der Informationshinweis nach Art 13 DSGVO auf Webseiten mit Werbe-Tracking müsste in Zukunft lauten: „Aus steuerrechtlichen Gründen sind wir verpflichtet, ihre Interessen unseren Werbekunden vollumfänglich offen zu legen". Wenn z.B. auf Seiten mit medizinischen Inhalten Werbung angezeigt wird, werden beim „Onlinewerbeleister" regelmäßig wohl sensible Daten anfallen. Es wird hier zwar zugestanden, dass dieser Effekt nicht in allen Fällen in dieser Intensität vorkommt. Allerdings hängt

4 Vgl. zB EuGH C-293/12 and C-594/12, Rz 28.

dies von der Gestaltung der Inhalte ab (z.B. ob bestimmte Inhalte als eigene Website gestaltet sind und die Informationen daher höher auflösen), in deren Umfeld die Werbung an die Nutzer angezeigt wird. Vor allem haben die NutzerInnen darauf aber keinen Einfluss. Es wäre gerade Gegenstand einer (verpflichtenden) Datenschutz-Folgenabschätzung herauszuarbeiten, wie wahrscheinlich und häufig eine informationsreiche Beziehung zu den Inhalten vorliegt und welche (hohen) Risiken damit verbunden sind. Eine derartige Risikoabschätzung fehlt jedoch vollständig.

Der Grundrechtseingriff dient einem legitimen Zweck. Das grundsätzliche Anliegen einer Digitalsteuer wird ausdrücklich begrüßt. Zugleich ist zu bedauern, dass offenbar alle bisherigen Bemühungen auf Unionsebene nicht nur gescheitert sind, sondern offenbar auch keine Spuren beim nationalen Alleingang der österreichischen Bundesregierung hinterlassen haben. Auch aus den begleitenden Materialien geht nicht hervor, ob und was zur Frage der Bestimmung des geographischen Bezugs als geeignetes Mittel in der seit längerem andauernden Debatte auf EU-Ebene diskutiert wurde. Also hat man national schlicht eine neue Lösung erfunden und die Frage der Grundrechtseingriffe ausgeblendet.

Dabei hätte schon ein Blick in die einschlägige nationale Rechtsprechung einiges an Aufklärung gebracht. Wie auch in der ISPA Stellungnahme referenziert, hat der Verwaltungsgerichtshof in einem Verfahren, welches sich mit der Abgabenerhebung auf Online-Glücksspiel befasste, darauf hingewiesen hat, dass die Erhebung der IP-Adresse keinen eindeutigen Rückschluss auf den Inlandsbezug zulasse[5]. Diese kann daher lediglich als Indiz verwendet werden, wobei ihr die gleiche Bedeutung zukommt wie andere, von jeweiligen NutzerInnen selbst angegebene Daten zum Wohnort[6]. Die von der Bundesregierung vorgeschlagene Methode ist daher nicht geeignet, dem Zweck der Bestimmung des Inlandsbezugs hinreichend zu dienen.

Außerdem ist der durch die Speicherverpflichtung bewirkte Grundrechtseingriff nicht erforderlich. Es gibt gelindere Mittel – ohne Eingriff in die Grundrechte der EndnutzerInnen als WerbeempfängerInnen – um den Zweck der Einhebung einer Digitalsteuer zu erreichen. Gemäß dem Gesetzesentwurf soll als Bemessungsgrundlage analog zum Werbeabgabegesetz 2000 das Entgelt dienen, welches der Onlinewerbeleister vom jeweiligen Auftraggeber erhält. Daraus folgt, dass es zur Erhebung der Steuer bereits ausreicht, jene Werbeaufträge, welche sich an österreichische NutzerInnen richten als Grundlage heranzuziehen. Wie die Bemessung sollte sich auch die Feststellung und der zugehörige Nachweis auf das Verhältnis zwischen WerbedienstleisterInnen und InhaltsanbieterInnen konzentrieren, anstatt das Verhältnis zwischen NutzerInnen und InhaltsanbieterInnen in riesigen Datenbestände über längere Zeiträume zu dokumentieren. Für weitere Nachweise zur einfachen Umsetzbarkeit der alternativen Ansätze wird auf die Ausführungen in der ISPA Stellungnahme vom 7.5.2019 unter Punkt 3) verwiesen.

Schließlich ist die verpflichtende Datenverarbeitung ein unverhältnismäßiger Eingriff in die Grundrechte aller NutzerInnen. Gerade die großen AnbieterInnen aus Drittstaaten, die bereits massive Datensammlungen betreiben, haben durch dieses Gesetz große Vorteile. Unternehmen wie Google sind nun verpflichtet etwas zu tun, was sie selbst seit langem wollen: Daten über alle Webseitenzugriffe für mindestens sieben Jahre zu speichern. Der wirtschaftliche Wert des Datenbestands für die verpflichteten AnbieterInnen, der von denselben AnbieterInnen zwingend über Zeiträume von mindestens sieben Jahren und länger gespeichert werden muss, übersteigt mit großer

5 VwGH 20.11.2014 2013/16/0085

6 Vgl. ISPA Stellungnahme zum Digitalsteuergesetz 2020 vom 7.5.2019, Seite 3.

Wahrscheinlichkeit das geschätzte Steueraufkommen, welches der Entwurf bezweckt. Damit wird eine zynische digital-kapitalistische Spirale in Gang gesetzt, bei der die große Mehrheit der Menschen mit Ihren Grundrechten bezahlt und als SteuerzahlerIn einen äußerst nachteiligen Handel eingeht. Dem steht eine Risikolage für Millionen von Menschen und die gesamte Gesellschaft gegenüber, der mit dem angestrebten und realistisch erreichbaren Zweck in keinem angemessenen Verhältnis steht. In Zusammenschau mit anderen Vorhaben ist der Wesensgehalt der Grundrechte verletzt.

Anonymisierung der IP-Adresse als (unzureichende) Alternative

Das Bundesministerium für Finanzen hat in einer ersten Reaktion bereits positiv auf den öffentlich diskutierten Vorschlag einer Lösung reagiert, wonach eine anonymisierte Speicherung der IP-Adressen den Zweck der Bestimmung des Inlandsbezugs ebenfalls erfüllen würde[7]. Nach Auffassung des Finanzministeriums sollten hierdurch datenschutzrechtliche Bedenken grundsätzlich ausgeräumt werden können. Dem ist aus folgenden Gründen nicht zuzustimmen.

Zunächst ist hier nochmals auf die oben formulierte Grundsatzkritik an der Eignung der IP-Adressen Speicherung für diesen Zweck zu verweisen. Wenn nach der Judikatur des Verwaltungsgerichtshofs schon die ganze IP-Adresse ein fragwürdiges Mittel darstellt, gilt dies natürlich umso mehr für die „halbe IP-Adresse", die nur noch den Gebietsbezug erkennen lässt aber keinen Rückschluss auf die einzelnen TeilnehmerInnen mehr zulässt.

Genau diese fragwürdige Eignung führt jedoch in einem Bumerang-Effekt doch wieder zu einer Speicherung der gesamten IP-Adresse. Wenn nämlich die WerbeanbieterInnen nur die „vordere Hälfte" der IP-Adresse speichern, haben die AnbieterInnen keine Handhabe, wenn ihnen fälschlicherweise hohe Umsätze aufgrund der anonymisierten IP-Adressen unterstellt werden. Dieses Problem kann nämlich zum Beispiel in der Praxis sehr leicht auftreten, wenn im Zuge einer „Distributed Denial of Service" Attacke („DDoS") extrem hohe Zugriffszahlen produziert werden und die angegriffene Seite steuerlich relevante Werbeinhalte bei den NutzerInnen anzeigt. Diese wären nach den – wohl automatisierten – Aufzeichnungen kaum von regulären NutzerInnenzugriffen zu unterscheiden, weil solche Attacken über sog. „Botnets" ausgeführt werden, die aus einer Armee von schlecht geschützten Rechnern besteht, die von den AngreiferInnen zuvor übernommen wurden. Die IP-Adressen zeigen nicht auf die TäterInnen sondern auf die vorgelagerten Opfer, Personen mit Rechnern mit unzureichendem Virenschutz. Eine wirklich anonymisierte Aufzeichnung der IP-Adressen würde aber zugleich einen Abgleich mit den AngreiferInnenadressen nicht zulassen. Damit würde der Anschein eines massiven Aufkommens steuerlich relevanter Vorgänge entstehen. Um sich davon freizubeweisen würden die AnbieterInnen mit hoher Wahrscheinlichkeit doch wieder die gesamte IP-Adresse speichern und sich dabei auf berechtigte Interessen (vgl. Art 6 Abs 1 lit f DSGVO) berufen – und damit vermutlich sogar rechtmäßig handeln.

Man müsste bei dieser Lösung tatsächlich ein strenges Verbot normieren, den personenbezogenen Teil der IP-Adresse zu speichern und eine Umsetzung nach dem Grundsatz „Privacy by Design" vorzuschreiben. Allerdings fehlt den Finanzbehörden in der Folge die Kompetenz, die Umsetzung dieser Vorschriften zu überprüfen. Wenn die Datenspeicherung im Sitzstaat erfolgt, der ein Drittstaat

7 Siehe die Stellungnahme der ISPA, 8/SN – 132/ME XXVI. GP, S. 8, https://www.parlament.gv.at/PAKT/VHG/XXVI/SNME/SNME_04317/imfname_751078.pdf.

ist (bei steuerlich relevanten Aufzeichnungen sehr wahrscheinlich), wäre für eine solche Überprüfung auch keine Kompetenz der EU-Datenschutzbehörden begründet. Damit ist nicht anzunehmen, dass angesichts der oben beschriebenen Haftungslage tatsächlich eine Anonymisierung „by Design" erfolgt. Zu den detaillierten Begründungen wird auf die Stellungnahme der ISPA verwiesen.

4 FEHLENDE DATENSCHUTZ-FOLGENABSCHÄTZUNG

Wir weisen außerdem darauf hin, dass gem Art 35 DSGVO und nach der Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl. II Nr. 278/2018 eine Datenschutz-Folgenabschätzung für dieses Vorhaben notwendig ist.