BUNDESARBEITSKAMMER

PRINZ EUGEN STRASSE 20-22
1040 WIEN
T 01 501 65 0

www.arbeiterkammer.at

Bundesministerium für Verkehr, Innovation
und Technologie
zH Frau Dr Eva-Maria Weissenburger
Ghegastraße 1
1030 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel 501 65	Fax 501 65	Datum
-	AK-KS/GSt/DZ/SK	Mag Daniela Zimmer	DW 2722	DW 2693	08.01.2010

Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird (Umsetzung der RL Vorratsdatenspeicherung)

Sehr geehrte Damen und Herren!

Die Bundesarbeitskammer (BAK) dankt für die Übermittlung des im Betreff genannten Gesetzesentwurfs und nimmt dazu wie folgt Stellung:

1. Allgemeines

Grundrechtlich problematische Richtlinie

Die BAK hat sich im Zuge des Entstehungsprozesses der mit dem vorliegenden Entwurf umgesetzten Richtlinie 2006/24/EG gegen das Vorhaben einer Vorratsdatenspeicherung ausgesprochen. Eine anlasslose Speicherung von Kundendaten für Zwecke der Strafverfolgung (über den für Verrechnungszwecke nötigen Zeitraum hinaus) steht mit elementaren Datenschutzprinzipien nicht im Einklang. Die verdachtsunabhängige Weiterverarbeitung millionenfacher Kundendaten dürfte in der Praxis dazu führen, dass der Durchschnittskonsument unnötig erfasst wird, im Zentrum von Ermittlungen stehende kriminelle Vereinigungen sich dagegen ganz leicht einer Datenerfassung (durch Wertkartennutzung, Ausweichen auf außereuropäische Serverstandorte usw) entziehen können. Völlig ungelöst ist außerdem das Problem, dass von vielen Verbindungsdaten (zB Mailkontakt mit Selbsthilfegruppen, Rechtsanwälten usw) mühelos auf die strengst geschützten Kommunikationsinhalte geschlossen werden kann.

DVR NR. 1048384

Mindestumsetzung mit flankierenden Rechtsschutzgarantien wird grundsätzlich begrüßt

Bezüglich der Richtlinienumsetzung in Österreich begrüßen wir, dass das Ludwig Boltzmann Institut für Menschenrechte in die Ausarbeitung des Entwurfs eingebunden wurde und es dabei sichtbarer Leitgedanke war, die Richtlinie nur in ihrem Mindestumfang umzusetzen und angemessene Rechtsschutzgarantien zu verankern.

Nicht-Umsetzung trotzdem weiterhin erwägenswert

Grundsätzliche Bedenken, dass die Speicherung entgegen Art 8 EMRK bzw GRC massiv in die Privatsphäre der Kunden eingreift, können damit freilich nicht ausgeräumt werden. Darüber hinaus ist das Vorhaben geeignet, Berufsgeheimnisse und unter Umständen auch das Recht auf freie Meinungsäußerung auszuhöhlen: Dass von bestimmten Verbindungsdaten mittelbar ziemlich treffsicher auf den Kommunikationsinhalt geschlossen werden kann, wurde eingangs bereits erwähnt, weshalb folgerichtig u.a. Ärzte- und Rechtsanwaltskammer auch einen indirekten Zugriff auf die Kommunikation mit Klienten ablehnen bzw Ausnahmen fordern. Journalisten befürchten zudem eine faktische Einschränkung ihrer Informationsmöglichkeiten (durch Informanten) und beanstanden das Vorhaben in Hinblick auf Art 11 der europäischen Grundrechte-Charta (Freiheit, Informationen ohne behördliche Eingriffe empfangen/weitergeben zu können).

Mit Inkrafttreten des Vertrags von Lissabon ist die Menschenrechtscharta zwingender Auslegungsgrundsatz bei der Beurteilung von Richtlinien geworden. Der rumänische Verfassungsgerichtshof hat in seiner jüngsten Entscheidung derart elementare Einwände gegen eine verdachtslose Vorratsspeicherung mit der Folge geäußert, dass in diesem Mitgliedsstaat voraussichtlich kein Spielraum für eine Richtlinienumsetzung mehr besteht. Medienberichten zufolge gibt es auch in Bulgarien ein Gerichtsurteil mit ablehnenden Tenor gegenüber der Vorratsdatenspeicherung. Die endgültige Entscheidung des ebenfalls befassten deutschen Bundesverfassungsgerichts ist noch ausständig. Vor dem Hintergrund dieser Entwicklung sollte unbedingt die Möglichkeit ins Auge gefasst werden, sich auf eine Fortführung des Vertragsverletzungsverfahrens einzulassen, im Zuge dessen die mutmaßliche Nichtigkeit der Richtlinie auf Basis der Artikel 263 (ex-Art 230 EGV) iVm 277 (ex-Art 241 EGV) weiterhin gerügt werden könnte.

Gesetzespaket gemeinsam mit BMJ und BMI erforderlich

Unser vordringlichstes Anliegen im Fall der Umsetzung der Richtlinie ist es, Änderungen im Telekomgesetz nicht losgelöst von einer Einigung mit den mitbetroffenen Ressorts Justiz- und Innenministerium über Änderungen der Strafprozessordnung (StPO) und des Sicherheitspolizeigesetzes (SPG) vorzunehmen. Die grundrechtliche Verhältnismäßigkeit der vorgeschlagenen Bestimmungen im Telekomgesetz hängt entscheidend davon ab, wie die flankierenden Regelungen in den Verweisungsmateriengesetzen StPO (Festlegung der „schweren" Straftaten) aber auch im SPG (zB Informationspflichten) gestaltet werden. Ohne Verabschiedung eines Gesetzespakets ist eine abschließende Beurteilung der datenschutzrechtlichen Auswirkungen nicht möglich.

Unsere wichtigsten Anliegen

Um Telefon- und Internetkunden bestmöglich vor überschießender Überwachung zu schützen, wären aus BAK-Sicht außerdem nötig:

- **Festlegung einer maximalen Speicherdauer für die verschiedenen Arten von Billingdaten:** Eine präzise Vorgabe, wie lange Telefon- und Internet-Verkehrsdaten für Verrechnungszwecke von den Dienstebetreibern maximal gespeichert werden dürfen (zB bei Internet-Flatrates, unter Berücksichtigung von Rechnungseinspruchsfristen usw), damit die Schutzstandards für Vorratsdaten (etwa Abfragen nur bei schweren Straftaten) nicht durch die Betreiberpraxis, die Verrechnung generell auf sechs Monate auszudehnen, unterlaufen werden können.

- **Restriktive Auslegung schwerer Straftaten:** Zeitgleich mit der Telekomreform eine klare Definition in der Strafprozessordnung, was schwere Straftaten, die einen Zugriff auf Vorratsdaten erlauben, sind (vorzugsweise Strafdrohung mehr als 5 Jahre, keinesfalls aber weniger als 3 Jahre)

- **Kein Zugang zu Vorratsdaten bei bloßen Urheberrechtsverletzungen:** Folglich kein Zugriff auf Vorratsdaten bei behaupteter Verletzung geistigen Eigentums

- **Keine Speicherung von Vorratsdaten aus Präventionsgründen:** absolut abzulehnen ist eine Datenspeicherung bzw ein Datenzugriff zur bloßen Gefahrenabwehr zB bezüglich IP-Adressen (einzige akzeptable Ausnahme: Standortdaten im lebensbedrohlichen Notfall)

- **Kein direkter Behördenzugriff auf Kundendaten:** Den Betreiber trifft die Verantwortung, von ihm ausgewählte Datensätze weiterzuleiten. Ein Behördenzugriff auf die Betreiberinfrastruktur sollte jedenfalls (bezogen auf Verrechnungs- und Vorratsdaten) untersagt sein.

- **Schutz für Inhaltsdaten auf die bei einigen Internetverkehrsdaten indirekt geschlossen werden kann:** Das Institut für Menschenrechte weist eingehend auf dieses noch völlig ungelöste Problem hin (zB Anrufe bei der Aidshilfe)

- **Zugriffserlaubnis auf Verrechnungsdaten restriktiv und präzise definieren,** keinesfalls aber weniger streng als durch Sicherheitspolizeigesetz schon derzeit erlaubt

- **Wirksame Aufsicht setzt Ressourcen voraus:** Zusätzliche Mittel für die Aufsichtsfunktion der Datenschutzkommission

- **Ausbau der Betroffenenrechte:**

  Gewährleistung einer generellen, automatischen Informationspflicht gegenüber allen von Datenabfragen Betroffenen. Nur wenn Kunden Kenntnis davon erlangen, dass sie von einer Abfrage betroffen sind, können sie ihre Datenschutzrechte bei Bedarf wahrnehmen:

- durch Klarstellung der Anwendbarkeit von § 139 Strafprozessordnung spätestens sobald die Ermittlungen beendet sind. Es ist dabei im Telekomgesetz sicherzustellen, dass Staatsanwälte diesem Auftrag auch entsprechen und sich nicht auf die Ausnahme *(die Identität sei nicht bekannt oder nicht ohne besonderen Verfahrensaufwand feststellbar)* berufen können
- außerhalb der Anwendbarkeit der StPO die Verankerung einer generellen Informationspflicht der Betreiber gegenüber ihren Kunden (nicht nur bezogen auf Standortdaten, wie im Entwurf vorgesehen, sondern hinsichtlich aller Stamm- und Verkehrsdatenabfragen)

Ideelle Schadenersatzansprüche im Falle rechtswidriger Auskünfte bzw Abfragen (im TKG bzw Erweiterung des §1328 a ABGB)

Zu den Details des Entwurfes

§ 90 Abs 7 Informationspflichten

Die Erweiterung der Auskunftspflichten der Betreiber gegenüber Sicherheitsbehörden bezüglich Stammdaten *„soweit sie diese Auskunft als wesentliche Voraussetzung für die Erfüllung der ihnen nach dem SPG übertragenen Aufgaben benötigen"* ist nicht nur reichlich unbestimmt, sondern wirft auch die Frage nach dem Verhältnis dieser Norm zu den Ermächtigungsbestimmungen im SPG auf. Nutzen und Auswirkungen dieser Bestimmung sind kritisch zu hinterfragen. Eine zusätzliche einschränkende Funktion der Anordnung gegenüber den Ermächtigungsnormen zu Stammdaten-Abfragen nach dem SPG ist nicht erkennbar. Adressaten der Verpflichtung sind im übrigen Telekombetreiber, die die Erforderlichkeit der Auskunft für Zwecke sicherheitspolizeilicher Ermittlungen kaum abschätzen können.

§ 94 technische Einrichtungen

Da sich um eine öffentliche Aufgabe handelt, sollten keinesfalls die Telekomanbieter bzw mittelbar deren Kunden für die Unkosten der Vorratsdatenspeicherung aufkommen müssen. Abs 2 letzter Satz eröffnet leider im Hinblick auf die Festlegung eines angemessenen Kostenersatzes für Betreiber durch Verordnung einen weiten Interpretationsspielraum. Insbesondere die Tragweite der Anordnung, dass bei der Höhe der Kostenerstattung ein allfälliges Eigeninteresse der Anbieter an den zu erbringenden Leistungen zu berücksichtigen ist, ist unklar.

§ 98 Notrufdienste

In der Praxis bereitet die Zuordnung erhebliche Probleme, wer denn exakt jene Notrufträger sind, die bezüglich der Stammdaten von Kunden auskunftsberechtigt sind. Diese mangelnde Klarheit ist umso dringlicher zu beseitigen, als nun mit der vorgeschlagenen Verfassungsbestimmung auch Standortdaten abgefragt werden dürften.

§ 99 Verkehrsdaten

Abs 2

Gemäß Abs 2 gilt: *„Sofern dies für Zwecke der Verrechnung von Entgelten, einschließlich der Entgelte für Zusammenschaltungen, erforderlich ist, hat der Betreiber Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann."* Die Auslegung dieser Anordnung könnte unter Telekom- und Internetanbietern unterschiedlicher nicht sein. Während manche Anbieter etwa Internet-Logfiles nur ganz kurzfristig aus technischen Gründen speichern, berufen sich andere auf denkbare Zahlungsstreitigkeiten, für die die Daten zu Beweiszwecken nützlich sein könnten. Auch bei Telefoniedaten ist die gelebte Aufbewahrungspraxis sehr heterogen. Während manche (angesichts sechswöchiger Rechnungseinspruchsfristen) spätestens nach drei Monaten Verkehrsdaten löschen, gibt es Anbieter die sie sechs Monate aufbewahren oder in Hinblick auf die zivilrechtliche Verjährung sogar 3 Jahre für rechtlich gedeckt halten.

Einheitliche gesetzliche Maximalvorgaben für die Speicherdauer von Verrechnungsdaten (samt Sanktionsbestimmungen) sind deshalb notwendig,

- um Kunden diesbezüglich nicht mehr dem großen Ermessensspielraum der Anbieter auszuliefern und
- um in Hinblick auf die Vorratsdatenspeicherung zu verhindern, dass die Anbieter in aufwandsminimierender Absicht Verkehrsdaten generell sechs Monate als Billingdaten betrachten. Ein solcher taktischer Schritt ist zu befürchten, da damit einfach und nach derzeitiger Rechtslage meist sogar zulässigerweise bzw zumindest sanktionslos technisch/organisatorisch hoher Aufwand für das Anlegen eines getrennten Vorratsdatenspeichers umgangen werden kann.

Abs 5 Z 2

Jedenfalls unterstützt wird die Intention, den Umfang der Zugriffsmöglichkeiten auf Verkehrsdaten dadurch zu begrenzen, dass die Abfrageberechtigungen im TKG abschließend genannt werden und weitere Zugriffswünsche in anderen (künftigen) Bestimmungen von Materiengesetzen hintangehalten werden. Bezogen auf die Formulierung der Verfassungsbestimmung in Ziffer 2 bestehen aber Bedenken. Demnach könnten Sicherheitsbehörden, soweit *„dies zur Abwehr einer konkreten Gefahr für das Leben oder die Gesundheit eines Menschen notwendig ist"*, Auskunft über Stamm- und Verkehrsdaten verlangen. Die Bestimmung ist unter Umständen weiter gefasst als jene des § 53 Abs 3a SPG, die zumindest auf eine „unmittelbare Gefährdung" abstellt. **Da schon die mangelnde Bestimmtheit der SPG-Norm zu Recht kritisiert wird, sollte die TKG-Ermächtigung weit restriktiver und präziser gestaltet werden.**

Begrüßt wird die Informationspflicht des Betreibers gegenüber seinen Kunden im Fall der Abfrage von Standortdaten. Diese Anordnung ist ganz entscheidend, um in der Praxis überschießende Abfragen zu verhindern. **Der BAK ist es allerdings ein zentrales Anliegen, dass sich diese Informationsverpflichtung auf alle Abfragen erstreckt.** Würde diese Transparenz (nach Abschluss des Ermittlungsverfahrens) nicht hergestellt, könnten Betroffene mangels Kenntnis der sie betreffenden Abfragen von Rechtsschutzmöglichkeiten keinerlei Gebrauch machen.

- Vor diesem Hintergrund wäre unbedingt klarzustellen, dass entsprechend **§ 139 Abs 2 StPO** Staatsanwaltschaften betroffene Kunden von der „Durchführung der Ermittlungsmaßnahme" zu unterrichten haben. Es ist dabei im TKG sicherzustellen, dass die Verpflichteten diesem Auftrag auch entsprechen und sich nicht auf die Ausnahme *(die Identität sei nicht bekannt oder nicht ohne besonderen Verfahrensaufwand feststellbar)* berufen können.

- Auch außerhalb der Anwendbarkeit der StPO ist eine generelle nachträgliche Informationspflicht der Betreiber gegenüber ihren Kunden (nicht nur bezogen auf Standortdaten, wie im Entwurf vorgesehen, sondern hinsichtlich aller Stamm- und Verkehrsdatenabfragen von Sicherheitsbehörden) unbedingt erforderlich. Die **Sicherheitsbehörden haben die Betreiber vom Abschluss des Ermittlungsverfahrens zu informieren**. Alternativ zu einer Betreiberpflicht im TKG könnte auch eine entsprechende Infoverpflichtung den Sicherheitsbehörden im SPG auferlegt werden.

Zu § 102 a Vorratsdaten

Abs 1 Einschränkung des Speicherzwecks von Vorratsdaten auf schwere Straftaten

Verkehrsdaten müssen nach der Richtlinie 2002/58/EG über den Schutz der Privatsphäre bei Kommunikationsdiensten gelöscht oder anonymisiert werden, sobald sie für die Herstellung der Verbindung bzw. Abrechnungszwecke nicht mehr benötigt werden. Die Richtlinie hat in Hinblick auf Art 8 der EU-Grundrechtscharta ein angemessenes Grundrechtsschutzniveau für Telekom- und Internetnutzer zum Ziel. Entsprechend Artikel 8 EMRK sind Eingriffe in die Grundrechte nur in begründeten Fällen bei Vorliegen bestimmter Voraussetzungen zulässig. Jeder Eingriff in das elementare Grundrecht auf unverzügliche Löschung muss daher erforderlich, verhältnismäßig sowie geeignet sein, das angestrebte Schutzziel überhaupt zu erreichen. Eine generelle routinemäßige Vorratsspeicherung, die sich auf alle Personen erstreckt, die Kommunikationsdienste nutzen, ist vor diesem Hintergrund eigentlich unverhältnismäßig. Der datenschutzrechtliche Anspruch auf Löschung kann deshalb keinesfalls in eine allgemeine Speicherpflicht zum Zweck jeder Form von Strafverfolgung verkehrt werden.

Um die Verhältnismäßigkeit auch nur annähernd zu wahren, muss das TKG bereits auf eine parallel ausgearbeitete, korrespondierende StPO – Bestimmung, die „schwere Straftaten" sehr restriktiv definiert, verweisen („Paketlösung TKG-StPO-SPG") oder direkt im TKG eine restriktive Definition von „schweren Straftaten" vorgenommen werden.

- Die RL bezieht sich ausdrücklich und ausschließlich auf den Zweck, die Aufklärung **schwerer Straftaten, insbesondere terroristische Akte**, zu erleichtern. Der Richtlinien-Anwendungsbereich ist insoweit eindeutig beschränkt und kann im Zuge der nationalen Umsetzung nicht nach Belieben auf Straftaten von geringer Brisanz, etwa Vergehen, ausgeweitet werden. Was unter schweren Straftaten im einzelnen zu verstehen ist, bestimmt sich grundsätzlich nach den Definitionen im jeweiligen Mitgliedsstaat (Art 1 der RL). Von Bedeutung sind in diesem Zusammenhang aber auch die Erwägungsgründe 7 bis 10 der RL, die ausschließlich auf die Terroranschläge in London/Madrid und den Kampf gegen organisierte Kriminalität bzw. Terrorismus Bezug nehmen.

- In der **Erklärung des Rates Justiz und Inneres** aus Februar 2006 wird bezüglich der Auslegung des Begriffes „schwere Straftat" auf Delikte verwiesen, die in Art 2 Abs 2 des Rahmenbeschlusses über den EU-Haftbefehl angeführt sind bzw unter Verwendung von Telekom-Einrichtungen begangen werden. Diese Interpretation kann und sollte auch aus unserer Sicht **keinesfalls übernommen** werden, da ihr bezüglich einer verfassungs- und gemeinschaftsrechtskonformen RL-Umsetzung kein verbindlicher Wert zukommt.

- Eine **Anknüpfung an § 17 SPG** (Verfolgung von mit beträchtlicher Strafe bedrohten Handlungen) **wird abgelehnt**. Die Einbeziehung von bloßen strafrechtlichen Vergehen, die mit mehr als einjähriger Freiheitsstrafe bedroht sind, geht über die Richtlinien-Ziele und die nötige Abwägung der Verhältnismäßigkeit des Eingriffes in nicht vertretbarer Weise hinaus. Solcherart könnten bspw auch vermutete **Verletzungen des § 91 Urheberrechtsgesetz (zB Nutzung von Filesharingangeboten im Internet)** von Verwertungsgesellschaften zum Anlass genommen werden, Privatpersonen strafrechtlicher Verfolgung unter optimaler Verwertung ihrer Verkehrsdaten auszusetzen. Da die Gewerbsmäßigkeit einer Handlung selten von vornherein völlig ausgeschlossen werden kann, wäre die massenhafte Auswertung der Rufdaten belangter KonsumentInnen zulässig (einfacher Verstoß bis zu 6 Monaten, bei gewerbsmäßigem Verstoß Strafdrohung bis zu 2 Jahren). In Hinblick auf § 1 DSG 2000 und Art 8 EMRK sehen wir weder Anlass noch Berechtigung für eine derart weitreichende Übermittlungsbefugnis.

- Daten dürften aus BAK-Sicht an die Strafverfolgungsbehörden jedenfalls dann übermittelt werden, wenn der Verdacht auf ein **Verbrechen nach § 278 und § 278 a bis d StGB** besteht (Kriminelle Vereinigung, Kriminelle Organisation, Terroristische Vereinigung, Terroristische Straftaten und Terrorismusfinanzierung).

- Wir verweisen weiters auf das Gutachten des Ludwig Boltzmann Instituts für Menschenrechte, das als Ansatz für die Definition einer „schweren Straftat" auf die jüngste Wertung des Gesetzgebers (EBRV 25 BlgNR XXII.GP 133) verweist, wonach ein schwerwiegendes Verbrechen in der Regel dann vorliegt, wenn für eine Tat eine **Strafdrohung von mehr als 5 Jahren Freiheitsstrafe** gilt.

- Allenfalls wäre noch eine Bezugnahme auf **§ 17 StGB (mit mehr als dreijähriger Freiheitsstrafe bedrohte Verbrechen)** diskutierbar. Eine noch weitere Öffnung der Zugriffsmöglichkeiten halten wir mit Blick auf den Verhältnismäßigkeitsgrundsatz für ausgeschlossen.

Zu Abs 8

Abs 8 sieht einen Auskunftszeitraum von 6 Monaten vor, der sich nicht mit dem Löschungszeitraum der Vorratsdaten (7 Monate) deckt. Unklar bleibt, ob nicht mit dem Einsatz von Zwangsmitteln zur Datenherausgabe auch bspw eine Beschlagnahme nach Ablauf von 6 Monaten erzwungen werden kann. Vor diesem Hintergrund wird eine einheitliche **Auskunfts- und Löschfrist von 6 Monaten unbedingt präferiert.**

Zu Abs 9

Abs 9 sieht vor, dass Anbieter, die Vorratsdaten speichern, diese Tätigkeit in der Eigenschaft als Auftraggeber öffentlichen Rechts durchführen. Diese Klarstellung wird begrüßt, da es Betreibern im Vergleich zu den verantwortlichen Ressorts vermutlich leichter fällt, hohe Datensicherheitsstandards zu gewährleisten. Es ist jedoch zu beachten, dass die Konstruktion so gewählt wird, dass die **Datenschutzkommission (DSK) der ihr zugewiesenen Aufsichtsrolle auch nachkommen kann**. Die DSK kann Beschwerden nach derzeitiger Rechtslage gegen privatwirtschaftliche Rechtsträger nur dann behandeln, wenn diese in Vollziehung der Gesetze tätig werden. Ob die Vorratsdatenspeicherung dem Vollziehungsbegriff des DSG entspricht, ist unklar.

Zu §102c Abs3 Z2

Protokolldaten über Datenzugriffe sind dem Entwurf zufolge dem Justizministerium einmal pro Jahr vorzulegen. Darüber hinaus sind aus BAK-Sicht aber unbedingt auch jährliche Berichtspflichten gegenüber dem Parlament und Datenschutzrat vorzusehen. Dieses Kontrollinstrument gibt es derzeit etwa bereits beim Einsatz besonderer Ermittlungsmaßnahmen. Der Umfang des Grundrechtseingriffs durch die Vorratsdatenspeicherung rechtfertigt jedenfalls umfangreichere Kontrollmaßnahmen.

Zu § 102 b

Auch die näheren Voraussetzungen unter denen Telefon- und Internetanbieter Strafbehörden Daten übermitteln dürfen, bedürfen einer präzisen Verfahrensregelung. Vor diesem Hintergrund sollte auch klargestellt werden, dass Anbieter nur dann verpflichtet sind, Daten auszufolgen, wenn der **gerichtliche Auftrag hinreichend präzise und begründet das Abfragemotiv und den -zeitraum** darlegt. In Zweifelsfällen muss sich der Betreiber an eine Kontrollstelle (Rechtsschutzbeauftragter, DSK) wenden können, bevor Daten aufgrund eines zu unbestimmten Auftrages ausgefolgt werden.

Abs 2 sollte dahingehend ergänzt werden, dass es Betreibern (bei sonstiger Sanktion) **untersagt ist, Behörden einen direkten Zugriff auf Kundendaten** einzuräumen. Den Betreiber trifft die Verantwortung, von ihm ausgewählte Datensätze weiterzuleiten. Ein Behördenzugriff auf die Betreiberinfrastruktur sollte jedenfalls (bezogen auf Verrechnungs- und Vorratsdaten) nicht möglich sein.

Zum Thema Rechtsschutz – bspw. Ergänzung des § 69 (Schutz der Nutzer)

Angesichts der besonderen Eingriffstiefe in die Privatsphäre bedarf es auch neuer Rechtsschutzmöglichkeiten der von unzulässigen Auskünften bzw Abfragen Betroffenen.

§ 1328 a ABGB sieht zwar vor, dass *„wer rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingreift oder Umstände aus der Privatsphäre eines Menschen offenbart oder verwertet, ihm den dadurch entstandenen Schaden zu ersetzen hat“.* In der Regel werden die Betroffenen jedoch keinen materiellen, sondern „nur“ einen ideellen Schaden erleiden. Ersatz wird nur gewährt *„bei erheblichen Verletzungen der Privatsphäre, etwa wenn Umstände daraus in einer Weise verwertet werden, die geeignet ist, den Menschen in der Öffentlichkeit bloßzustellen.“*

Da der Datenfluss zwischen Betreiber und Behörde erfolgt, ist mit der Rechtsverletzung in der Regel keine öffentliche Bloßstellung im Sinne des Gesetzes verbunden, ein Erstattungsanspruch wegen erlittener persönlicher Beeinträchtigung deshalb auch nicht gesichert. In gleicher Weise bietet auch die Schadenersatznorm des § 33 Datenschutzgesetz keine gesicherte Anspruchsbasis.

Ein zivilrechtlicher immaterieller Schadenersatzanspruch gegen rechtswidrige Datenauskünfte der Betreiber ließe sich ohne weiteres im TKG verankern. Vorzugsweise könnte jedoch eine allgemeine Anspruchsgrundlage (die auch unzulässige Behördenabfragen umfasst) durch Überarbeitung des § 1328 a ABGB geschaffen werden.

Weiterer Änderungsbedarf im TKG, um zeitgemäßen Konsumentenschutz sicherzustellen

Die BAK nimmt die vorliegende Novelle zum Anlass, darauf hinzuweisen, dass abseits der Richtlinien-Umsetzung auch Handlungsbedarf besteht, den Kundenschutz im Telekomrecht zeitgemäß auszubauen.

§ 107 Unerbetene Werbeanrufe

So ist Telefonwerbung gegenüber Verbrauchern zwar ohne deren Einwilligung schon nach geltendem Recht verboten, allerdings beachten viele Anbieter dieses Verbot nicht. Da unerwünschtes Telefonmarketing stark zunimmt und die Belästigung für Betroffene unzumutbar ist, sind die derzeitigen Schutzmaßnahmen zu erweitern:

Strenge Anforderungen an die Zustimmung zur Telefonwerbung

- Schriftform oder aktiver Schritt im Internet statt Datennutzungsklauseln versteckt im Kleingedruckten;
- genaue Bezeichnung der begünstigten Firmen
- Die Anbieter dürfen die Bereitstellung ihrer Dienste nicht von einer solchen Zustimmung abhängig machen (Koppelungsverbot)

Verbot des anonymisierten Anrufs durch Unternehmen und allen Institutionen

Nur private Anrufer dürfen ihre Rufnummer unterdrücken. Unternehmen, Organisationen und Behörden sollen ihre Telefonnummer anzeigen müssen, wenn sie anrufen. Eine Fälschung der mit gesendeten Rufnummerninfo ist untersagt (Anrufer müssen durch Rückrufmöglichkeit bzw im Falle einer Anzeige wegen Cold Callings ansprechbar und identifizierbar sein). Telekomunternehmen dürfen für die Rufnummernanzeige kein zusätzliches Entgelt verlangen.

Bei Telefonmarketing: Quelle der Zustimmung nennen

Auch im Falle erlaubter Telefonmarketingaktivitäten muss der Anrufer gegenüber dem Verbraucher die Zustimmungsbasis offenlegen. Deshalb sollten kommerzielle Anrufer verpflichtet sein, die Quelle der Zustimmung (wann, welcher Firma gegenüber) zu diesem Werbeanruf auf Nachfrage am Telefon zu nennen (um KonsumentInnen den Widerruf zu erleichtern).

Einstweilige Verfügung der Vollzugsbehörden

Die Vollzugsbehörde soll ermächtigt werden, zum sofortigen Schutz vor Belästigungen von Verbrauchern durch Cold Calling einstweilige Verfügungen (zB Rufnummernsperren) zu erlassen (die rechtskräftige Klärung im Rahmen eines Verwaltungsstrafverfahrens dauert lange, vorläufige Maßnahmen wären deshalb wichtig).

Unwirksamkeit von auf Cold Calling basierenden Verträgen

Vorzugsweise ist diese Maßnahme, die Teil des Regierungsübereinkommens ist, systematisch passend im Konsumentenschutzgesetz umzusetzen. Sollte dies nicht gelingen, wäre die Nichtigkeit von Verträgen, die im Zuge von unerbetenen Werbeanrufen zustande kommen, in § 107 TKG vorzusehen.

Kostenkontrolle bei Internettarifen mit im Grundpreis inkludierten Datenvolumen

Bei etlichen Internetprodukten ist im Grundpreis ein pauschaliertes, monatliches Datentransfervolumen enthalten. Darüber hinaus wird mengenabhängig verrechnet. Die Preise für den Mehrverbrauch von Megabytes betragen oft ein Vielfaches vom Preis für das Megabyte innerhalb der Pauschale. Die Folgen einer Überschreitung sind oft überraschend hohe Kosten für den Mehrverbrauch. Gefährdet sind Verbraucher vor allem, wenn sie den Datenverbrauch bei ihrem Anbieter nicht gut nachvollziehen können. Die Anbieter ermöglichen ihren Kunden zwar, ihren Verbrauch über passwortgeschützte Internetseiten abzurufen. Allerdings geben die Seiten nicht immer den aktuellen Verbrauchsstand wieder.Vor diesem Hintergrund ist es unbedingt erforderlich, Betreiber zu verpflichten,

- knapp vor Ausschöpfung der inkludierten Datenmenge Kunden (bspw durch ein Warn-SMS) darüber zu informieren,
- ein kostenloses Sperrservice ab Erreichen eines individuellen Höchstbetrages anzubieten, (Der Kunde ist zu informieren, wie er den Dienst bei Bedarf fortsetzen kann.)
- Internetabfragetools in knappen Intervallen zu aktualisieren.

Weitere Anliegen sind

- Anspruch auf eine kostenlose Papierstandardrechnung
- Gesetzliche Grenzen für die Verrechnungstaktung
- Anbieterpflicht, die wichtigsten Tarifinformationen bei Vertragsabschluss auszuhändigen
- Formvorschriften für die Verständigung der Kunden im Falle der nachteiligen Änderung von Geschäftsbedingungen (bspw nicht ausschließlich per SMS oder Mail)
- Klarstellung, dass Fangschaltungen (zwangsweise Aufhebung der Rufnummernunterdrückung) nur beim Betreiber (nicht beim Kunden) eingerichtet werden dürfen, Kunden Rufnummern folglich nicht selbst speichern, sondern anlassbezogen beim Betreiber abfragen dürfen.

Mit freundlichen Grüßen

Herbert Tumpel
Präsident

BUNDESARBEITSKAMMER

Werner Muhm
Direktor