universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„Das datenschutzrechtliche Einwilligungserfordernis für den Einsatz von Identifikatoren zur Wiedererkennung von Internetnutzern im World Wide Web“

verfasst von / submitted by

Dipl.-Ing. Christoph Diemberger, LL.B.

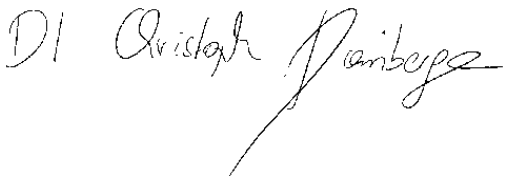
angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, September 2018 / Vienna 2018

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 942
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von / Supervisor:	ao. Univ.Prof. Dr. Dietmar Jahnel

Ich versichere, dass ich die Master Thesis selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen. Ich erkläre mich hiermit einverstanden, dass die Arbeit auf Verlangen der/des Prüfenden mit Hilfe eines Plagiatserkennungsprogrammes auf ggf enthaltene Plagiate überprüft wird.



Wien, 15.09.2018

Gliederung

Abstract

English title: "*Data privacy end-user consent requirement when using identifiers for the sake of tagging and matching users on the World Wide Web*". This thesis examines data privacy aspects of identifiers as they are used to tag and match internetusers on the WWW for the sake of creating user personalized content. In general, identifiers used for this purpose are pseudonyms which are created and maintained by the provider of the respective webservice. If such an identifier qualifies to be personal data in the meaning of the GDPR, the entire webservice might be subject to the user's consent.

The analysis follows a 2-step approach: First, the technological methods are examined with respect to their inherent processing of personal data. Three methods have been chosen to be analysed more deeply: *HTTP cookies*, *device fingerprints* and *MSISDN forwarding*. In a second step the analysis extends onto the use case level where the above mentioned technological methods come into play, for instance: Web audience measurement, persistent storage of user inputs, direct carrier billing, online behavioural targeting and others.

Since 25th May 2018 there is an interdependency of the GDPR with the national data privacy regulations for the telecommunication sector. In this context the thesis elaborates the applicable provisions and their extent as needed for the assessment of the necessity for end-user consent. As a side topic, a de lege ferenda approach also touches the upcoming ePrivacy Regulation. For the assessment whether there is a technology inherent processing of personal data or not, the "theory of pseudonymized IP Addresses concatenation" was derived during the creation of this paper. The theory combines some major findings of the EuGH *Breyer* decision with the predominant opinions on classification of pseudonyms under the GDPR. The thesis argues for a broad understanding of the criteria *identifiable* to classify data as to be personal but still requires the real person to be *identifiable* and not only his/her virtual representation. The identifier must be unique in a mathematical sense to represent a distinct and reoccurring relationship to the users IP Address – the latter is the key element for the *identification* of the real person.

As a result, some of the technologies listed above inevitably lead to the processing of personal data. This is caused by their design in conjunction with the internet transportprotocol TCP/IP. However, the respective use case of the webservice may still legitimate the processing of personal data without the need for the user's consent. On the other hand: If there is no mandatory processing of personal data on the technical level involved, the realized use case in general is not subject to end-user consent in the meaning of data privacy laws. This qualification might lead to inappropriate results - internetusers often have the feeling of being spied on, their behaviour analysed, their online movements tracked. Addressing this shortcoming, the thesis also introduces the protection regime as proposed within the ePrivacy regulation as well as a possible protection on the grounds of fundamental rights as laid down in Art 8 of the European Convention of Human Rights.

1. Einführung

„MEPs today have a very clear choice: You can either disappoint the vast majority of citizens who want their confidentiality to be protected, or you can give in to the demands and lies of some industrial lobbyists."

MEP *Birgit SIPPEL*, Berichterstatterin des Innenausschusses zur ePrivacy VO unmittelbar vor der Abstimmung im EU Parlament zur Zuweisung des Verordnungsentwurfs an den EU Rat [26. 10.2017]

Diese pointierte Formulierung, verbunden mit der Tatsache, dass es während dieser Rede zu einem Ordnungsruf des Leiters der Plenarsitzung gegenüber diversen Zwischenrufen aus dem Plenarsaal kam, verdeutlicht das Maß an Zerstrittenheit über den notwendigen Umfang datenschutzrechtlicher Vorgaben in der elektronischen Kommunikation. Am 25. Mai dieses Jahres trat die Datenschutz-Grundverordnung (DSGVO) in Kraft. In ErwGr 173 ist dort zu lesen: „Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden". Daraus lässt sich ableiten, dass der EU Gesetzgeber die derzeitige Situation eigentlich vermeiden wollte und ein gleichzeitiges Inkrafttreten von DSGVO und ePrivacy VO angestrebt hat. Für Internetdienstleister ergibt sich nun die Situation, dass sie seit dem 25. Mai anhand ihrer DSGVO-Konformität beurteilt werden, ohne dass die für sie so wesentlichen Konkretisierungen zum Umgang mit personenbezogenen Daten auf ihren Webangeboten an die neue Gesetzeslage angepasst wurden. Dies soll erst durch das Inkrafttreten der ePrivacy VO erfolgen, welche zum jetzigen Zeitpunkt inhaltlich nicht abschließend ausverhandelt ist.

Die vorliegende Master Thesis[1] beurteilt die Zulässigkeit von Datenverarbeitungen durch Websitebetreiber bzw in einem untergeordnetem Maße auch durch Internetzugangsanbieter aus einer datenschutzrechtlichen Sichtweise und konzentriert sich dabei auf jene Verarbeitungen, die bei den Vorgängen der Identifikation und späteren Wiedererkennung des Websitebesuchers durchgeführt werden. Basis für die Beurteilung ist die DSGVO in Wechselwirkung mit den bestehenden nationalen Regelungen für die elektronische Kommunikation, speziell auch im Hinblick auf die Rechtsunsicherheiten, welche sich durch die Verschiebung des ePrivacy Gesetzgebungsprozesses ergeben. Generell findet für die Untersuchung ein zweistufiger Prozess statt: Zunächst wird anhand der Darstellung der technischen Grundlagen festgestellt, ob alleine durch den Einsatz der entsprechenden Technologie ein datenschutzrechtlicher Problemkreis eröffnet wird. In einem zweiten Schritt findet eine zweck- und anwendungsfallbezogene Analyse statt.

[1] **Redaktionelle Anmerkungen:** Alle Referenzen auf Internetressourcen wurden zuletzt am 30. August 2018 auf ihre Aktualität überprüft. Ein detailliertes Abkürzungsverzeichnis befindet sich am Ende der Ausarbeitung. Aus Gründen der besseren Lesbarkeit wird im vorliegenden Text auf eine geschlechtsspezifische Differenzierung verzichtet – die Verwendung der maskulinen Form umfasst im Sinne der Gleichbehandlung beide Geschlechter.

1.1 Problemaufriss

1.1.1 Die Motivation zur Identifikation und Wiedererkennung von Webbenutzern

Viele etablierte Internetangebote des World Wide Web sind bestrebt, dem jeweiligen Besucher einen personalisierten Gesamteindruck zu vermitteln, und zwar in inhaltlicher, in formaler und in optischer Hinsicht. Dies erhöht iA die Treffsicherheit im Hinblick auf die Erwartungshaltung des Benutzers und dadurch auch die wahrgenommene Relevanz der präsentierten Inhalte. Um ein personalisiertes Internetangebot bereitzuhalten, ist der Webseitenbetreiber auf Informationen über den Internetbenutzer angewiesen. Diese Informationen kann der Internetbenutzer entweder freiwillig mitteilen oder sie werden mit anderen Mitteln und Methoden erhoben.

Den genannten Ausprägungen einer Benutzer-Personalisierung ist gemein, dass dem einzelnen – iA nicht namentlich bekannten - Benutzer zunächst ein eindeutiges Kennzeichen zugordnet wird. Diese Kennzeichnung ist einerseits technisch notwendig, um das personalisierte Benutzungserlebnis durch die beteiligten Computersysteme direkt beim Besuch der Website in Echtzeit zu erstellen und zu präsentieren. Anderseits wird diese Kennzeichnung aber auch dafür genutzt, zusätzliche unterscheidungsrelevante Informationen über den Benutzer, zB während des Besuchs auf der Website[2], zu sammeln und zu speichern. Dadurch ist es möglich, dem Benutzer bei einer späteren Wiederkehr ein nochmals verbessertes Personalisierungsergebnis anzubieten. **Der Begriff der „Identifikation", wie er in dieser Arbeit gebraucht wird, steht also nicht primär für die Feststellung der (realen) Identität des Benutzers als Person, sondern zunächst nur für den Akt der Zuweisung eines Wiedererkennungsmerkmals (=Kennzeichen, Identifikator) des Besuchers einer Website.** Wie zu zeigen sein wird, bezieht sich dieses Wiedererkennungsmerkmal oftmals nicht primär auf den Benutzer als Person, sondern auf das von ihm verwendete Endgerät. Insofern besteht daher kein Konflikt zur Terminologie aus den Datenschutzgesetzen, denn dort geht es um die *identifizierte* oder *identifizierbare* **reale Person**. Ob und in welchen Fällen dieses Wiedererkennungsmerkmal dazu führt, dass die Identität des Benutzers als reale Person festgestellt werden kann, ist eine der zentralen Fragestellungen dieser Arbeit.

[2] Als „Website" soll hier und in weiterer Folge die gesamte web-basierte Onlinepräsenz des Websitebetreibers unter *einem* Domain-Namen verstanden werden. Der Begriff „Webseite" wird hingegen dann verwendet, wenn eine einzelne Webseite (iSe HTML Dokuments) innerhalb dieser Website angesprochen wird.

Zur Verdeutlichung seien an dieser Stelle einige gängige Beispiele für diese Vorgangsweise genannt:

- Eine Website bietet dem Benutzer die Möglichkeit, eine Sprachauswahl zu treffen. Die gewählte Spracheinstellung bleibt über den einmaligen Besuch hinaus erhalten, sodass der Benutzer bei seinem zweiten Besuch die Inhalte sogleich in „seiner" Sprache präsentiert bekommt.
- Der Benutzer teilt einem Webshop im Zuge einer erstmaligen Bestellung seinen Namen und seine Adresse mit. Beim nächsten Besuch bzw beim nächsten Einkauf „weiß" die Website bereits Namen und Adresse, ohne dass der Internetbenutzer diese Daten erneut eingeben muss oder seine Daten wissentlich zur späteren Verwendung freigegeben hat.
- Dem Benutzer wird personalisierte Werbung beim Besuch der Website eingeblendet. Die Auswahl des anzuzeigenden Werbebanners erfolgt anhand von Informationen (zB Interessen, Vorlieben), die über den Benutzer bei den letzten Besuchen dieser Website bzw bei Besuchen auf anderen Websites gesammelt wurden.

Neben der Motivation zur Erhöhung des Nutzungserlebnisses durch Personalisierung gibt es allerdings auch andere Gründe, warum eine Identifikation und Wiedererkennung eines Benutzers notwendig werden kann. Anschauliches Beispiel hierfür ist, dass der Websitebetreiber eine aussagekräftige Besucherstatistik seines Web-Angebots erstellt und hierfür Erstbesucher von Wiederkehrern voneinander unterscheiden möchte.

1.1.2 Technische Ausgangssituation

Vernetzte Endgeräte im Internet werden primär durch ihre IP Adresse voneinander unterschieden. Die IP Adresse ist eine technische Notwendigkeit, um den Datentransfer zwischen den Endgeräten abzuwickeln[3] und sie wird in jedem einzelnen Kommunikationsdatenpaket mitübertragen. Während IP Adressen von Websites oft über Jahre hinweg konstant bleiben[4], können sich IP Adressen der Zugangsgeräte von normalen Internetzbenutzern (zB Smartphones) mehrmals täglich ändern[5]. Dazu kommt, dass sich aus Sicht des Websitebetreibers oftmals mehrere Benutzerendgeräte eine einzige IP Adresse teilen[6] und somit auf dieser Ebene ununterscheidbar werden.

Für den Zweck der Identifikation und Wiedererkennung genügt die IP Adresse daher aus den oben genannten Gründen nicht. Daher wird in der Praxis neben der IP Adresse ein zusätzliches Identifikationselement („Kennzeichen", „ID", „Identifikator", „UUID"[7]) für einen Benutzer bzw sein Endgerät erstellt, zugeordnet und gespeichert. Das Identifikationselement

[3] *Alich/Voigt,* Mitteilsame Browser – Datenschutzrechtliche Bewertung des Trackings mittels Browser-Fingerprints, CR 2012, 344.
[4] Sogenannte „statische" IP Adresse.
[5] Sogenannte „dynamische" IP Adresse.
[6] Sogenanntes *IP Masquerading*.
[7] *Universally unique identifier* - Quelle wikipedia: <en.wikipedia.org/wiki/Universally_unique_identifier>.

ist eine Zeichenkette, die vom Webserver mithilfe mathematischer Methoden, oft kombiniert mit Zufallsgeneratoren, erzeugt wird. Die Notwendigkeit für diese Zuordnung ergibt sich schon alleine daraus, dass die Basistechnologie des World Wide Web (WWW), das Übertragungsprotokoll HTTP, ansonsten die Aktivitäten eines einzelnen Benutzers über verschiedene Unterseiten der Website nicht logisch zusammenhängen und auch nicht einzelne Benutzer mit derselben IP Adresse voneinander trennen könnte. Das Zusammenfassen dieser Aktivitäten eines Benutzers im Rahmen seines Besuchs auf der Website nennt man *session*[8]*.* Die *session* ist vorüber, wenn der Benutzer die Website verlässt oder den Webbrowser beendet. Streng genommen findet bereits bei einer einfachen Webapplikation (zB: einem Warenkorb in einem Online-Shop) eine Identifikation und Wiedererkennung des Benutzers statt - und zwar bei jedem einzelnen Aufruf einer Unterseite des Webangebots. Ansonsten könnten die vom Benutzer getätigten Eingaben nicht von einer Unterseite zur nächsten übernommen werden.

Um den Komfort für den Benutzer zu erhöhen, wird in der Praxis oftmals die Zuordnung zu „seinem“ Warenkorb über die aktuelle *session* hinaus beibehalten. Der Benutzer, der nach einem Verbindungsabbruch oder aber auch zielgerichtet am nächsten Tag zurückkommt, soll auf Basis seines unveränderten Warenkorbes den Einkauf fortsetzen können. Spätestens jetzt ist es für den Benutzer offensichtlich, dass ihn die Website *wiedererkannt* hat.

1.1.3 Juristischer Problembereich

Bei der erstmaligen Identifikation und bei der darauffolgenden Wiedererkennung findet serverseitig und auf dem Endgerät des Benutzers eine Datenverarbeitung statt. Wie noch zu zeigen sein wird, werden dabei uU auch personenbezogene Daten verarbeitet. Dem allgemeinen Verbot der Verarbeitung von personenbezogenen Daten folgend muss daher entweder ein gesetzlicher Erlaubnistatbestand iSd Datenschutzrechts einschlägig sein oder eine Einwilligung durch den Betroffenen erfolgen. Dies soll in weiterer Folge für verschiedene Technologien und Anwendungsfälle untersucht werden.

1.2 Themeneingrenzung, Schwerpunktsetzung und inhaltlicher Aufbau

Gegenstand der Arbeit ist die datenschutzrechtliche Beurteilung von gängigen Anwendungsfällen im WWW, bei denen ein Besucher nach seinem ersten Besuch auf eine Website zurückkommt, die Website ihn als Wiederkehrer erkennt und daraufhin personalisierte Funktionen zur Verfügung stellt. Ebenfalls sollen ausgewählte Fälle untersucht werden, bei denen der Websitebetreiber von einer anderen Entität, einem Dritten, Informationen übermittelt bekommt, die eine Identifikation und Wiedererkennung des Besuchers erlauben. Es werden nur Methoden untersucht, bei denen eine geeignete Kennzeichenzuordnung stattfindet, die über die allseits offengelegte IP Adresse des

[8] Definition entnommen von: <https://tomcat.apache.org/tomcat-5.5-doc/servletapi/javax/servlet/http/HttpSession.html>.

Besuchers hinausgeht und zumindest für einen vorübergehenden Zeitraum server- und/oder clientseitig gespeichert wird. Die Eingrenzung der Untersuchung auf das WWW ergibt sich durch die oben erwähnte Eigenart des zugrundeliegenden Übertragungsprotokolls HTTP in Verbindung mit der strengen Standardisierung der Technologie auf Seiten des Webservers und des Webbrowsers. HTTP wird als Technologie vereinzelt auch innerhalb von mobilen Applikationen („*apps*“) benutzt, zB bei der Einblendung von Werbebannern. In diesem Sinne sind die gefundenen Erkenntnisse - mit Einschränkungen - auch auf Anwendungsfälle außerhalb des klassischen WWW übertragbar. Auf spezifische Eigenarten des Endgeräts bzw des Betriebssystems, zB Smartphone gegenüber Computer, wird allerdings nur sehr beschränkt eingegangen. Eine genauere Betrachtung von Identifikationsmethoden im Umfeld von *mobile apps* findet nicht statt.

Dort wo eine exakte Erkennung der einzelnen Person und nicht bloß ihres Endgeräts notwendig ist, zB bei einer Online-Banking Applikation oder bei der rechtsgültigen Unterfertigung eines Kaufvertrags, ist im Allgemeinen ein Authentifizierungsmechanismus, zB *Username* und *password*, erforderlich, dem eine vorherige Registrierung vorausgeht. Solche Methoden stehen zwar nicht im Zentrum der hier durchgeführten Untersuchung, müssen aber zT mitberücksichtigt werden.

Als Spezialfall werden auch Identifikationsmethoden untersucht, welche im Zusammenwirken mit bzw komplett durch Drittanbieter stattfinden. Dieser Vorgang ist für den Benutzer oftmals intransparent, da er nur die von ihm willentlich - zB durch Eingabe der WWW-Adresse („URL“)[9] - aufgerufene Website als Kommunikationsgegenstelle wahrnimmt. Falls eine Verarbeitung von personenbezogenen Daten auch auf Seiten des Drittanbieters erfolgt, ist auch bei diesem nach einem datenschutzrechtlichen Erlaubnistatbestand zu suchen.

Der eigentlichen juristischen Untersuchung vorauseilend erfolgt eine in der notwendigen Tiefe durchgeführte Vorstellung der technischen Methoden, die im Internet zum Zwecke der Identifikation und Wiedererkennung von Internetbenutzern zum Einsatz kommen. Die Auswahl der technischen Methoden ist dabei bereits auf diejenigen beschränkt, welche die ausgewählten Anwendungsfälle der Folgekapitel praxistauglich realisieren. Der Schwerpunkt der Arbeit liegt nicht in der Ausarbeitung und Beschreibung dieser technischen Methoden, sondern in der Beurteilung der datenschutzrechtlichen Implikationen der jeweiligen auf diesen technischen Methoden beruhenden Anwendungsfälle.

Im Anschluss an die Darstellung der technischen Methoden erfolgt die Ermittlung des datenschutzrechtlichen Prüfungsmaßstabs anhand der DSGVO sowie anhand anderer Datenschutzrechtsquellen.

Den Hauptteil der Untersuchung bildet eine Auswahl von gängigen Anwendungsfällen im World Wide Web, welche auf Methoden zur Identifikation und Wiedererkennung von

[9] URL steht für *Uniform Ressource Locator*. Quelle Wikipedia: <en.wikipedia.org/wiki/URL>.

Benutzern angewiesen sind. Alle Anwendungsfälle werden nach demselben Muster und anhand des zuvor ausgearbeiteten datenschutzrechtlichen Prüfungsmaßstabes beurteilt. Die wesentliche Frage wird dabei die Reichweite der gesetzlichen Erlaubnistatbestände sein. Diese Klärung erfordert vorgelagert die Einordnung der Rollen als Auftragsverarbeiter bzw als Verantwortlicher, sowie die technische Darstellung, wann und von wem eine Verarbeitung von personenbezogenen Daten durchgeführt wird. Auf die konkrete Ausgestaltung – Stichwort Cookie Banner – und Reichweite der allenfalls notwendigen datenschutzrechtlichen Einwilligungserklärung wird nur eingeschränkt eingegangen. Die näheren Vorgaben zur Einwilligung, zB zur Informiertheit, Freiwilligkeit oder Unmissverständlichkeit sowie die Anforderungen an die Ausgestaltung der Informationspflicht gemäß Art 13,14 DSGVO stehen ebenfalls nicht im Fokus der Untersuchung.

2. Technische Methoden zur Identifikation und Wiedererkennung

Wie bereits in Kapitel 1.1.2 angedeutet ist das wesentliche Element für eine Identifikation und Wiedererkennung eines Internetbenutzers das Zuweisen eines eindeutigen Kennzeichens (ID, Identifikator). Aus den oben genannten Gründen (Kapitel 1.1.2) ist eine Identifikation und Wiedererkennung alleine anhand der IP Adresse nicht ausreichend und wird daher hier nicht als eigene Methode geführt. Die IP Adresse des Internetbenutzers wird aber von einigen Verfahren ergänzend als zusätzliches Identifikationsmerkmal eingesetzt um die Wahrscheinlichkeit einer korrekten Wiedererkennung zu erhöhen.

2.1 HTTP Cookie

2.1.1 Technische Funktionsweise

Durch die sogenannte Cookie-Richtlinie[10] wurde ein vermeintlich technisch unscheinbares Element einer breiten Öffentlichkeit bekannt. Der *HTTP Cookie* ist eine Erweiterung des Übertragungsprotokoll HTTP und von der Internet Engineering Task Force standardisiert[11]. Für sich alleine genommen ist ein Cookie ein kleines Datenelement (nur wenige KByte groß), welches auf Anweisung der besuchten Website vom Endgerät des Benutzers bei dessen erstmaligem Besuch erzeugt und auch dort gespeichert wird[12]. Dieses clientseitig gespeicherte Datenelement ist zwar das Charakteristikum der Cookie-Technologie, die Gesamtfunktion geht allerdings darüber hinaus und beschreibt einen vorgegebenen Ablauf in der Wechselwirkung zwischen Website und Endgerät des Benutzers.

Der Cookie wurde ursprünglich zu dem Zweck spezifiziert und entwickelt, um einzelne Benutzeraktivitäten auf einer Website zusammenfassen zu können, sodass Anwendungsfälle wie der „Warenkorb“ (siehe Kapitel 1.1.2) technisch realisiert werden konnten[13]. Getätigte Nutzereingaben und benutzerspezifische Einstellungen müssen zumindest für die Dauer des einzelnen Besuchs beibehalten werden, damit der erwartete Workflow des Benutzers technisch abgewickelt werden kann. Bei der Speicherung dieser Daten muss unterschieden werden in:

- Clientseitig gespeichert
- Serverseitig gespeichert

[10] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz (Änderungs-Richtlinie), Abl L 2009/337, 11.

[11] RFC 2109, RFC 2965 – RFCs sind Publikationen von techn. Standards und verfügbar unter <www.ietf.org/standards/rfcs>.

[12] Vgl *Christl*, Datenschutz im Internet: Cookies, Web-Logs, Location Based Services, eMail, Webbugs, Spyware (2014) 20. Allerdings wird der Cookie in modernen Browsern nicht als Textdatei sondern in einer lokalen Datenbank gespeichert – vgl <kb.mozillazine.org/Cookies>, <stackoverflow.com/questions/31021764/where-does-chrome-store-cookies>.

[13] World Wide Web Consortium <www.w3.org/2001/tag/2010/09/ClientSideStorage.html>.

Zusätzlich unterscheidet man noch anhand der Speicherdauer:

- Non-persistent gespeichert (zB Sekunden, Minuten, bzw für die Dauer der *session*)
- Persistent gespeichert (zB Tage, Wochen oder mehr)

Zur Klarstellung: Auch bei der serverseitigen Speicherung wird auf dem Endgerät des Benutzers ein Cookie Datenelement gespeichert. In diesem Fall enthält es allerdings nicht die tatsächlichen Eingaben und Einstellungen des Benutzers, sondern lediglich einen Identifikator, der auf den jeweils zugeordneten serverseitigen Speicherbereich verweist (siehe übernächster Absatz). Im Gegensatz dazu werden bei der clientseitigen Speicherung sämtliche Benutzereingaben und Einstellungen physisch tatsächlich in der Cookie-Datei auf dem Endgerät des Benutzers abgelegt.

Ganz wesentlich für das Funktionieren – und auch das Verständnis – der Cookie-Technologie ist nun das Folgende: Bei jedem darauffolgenden Zugriff des Benutzers auf dieselbe Website bzw eine Unterseite der Website wird das Cookie Datenelement komplett an den Webserver übertragen. Der Webserver hat nun Zugriff auf die gespeicherten benutzerspezifischen Eingaben und Einstellungen des jeweiligen Benutzers, kann die Inhalte oder die Darstellung der Unterseiten entsprechend dynamisch anpassen und so den vom Benutzer erwarteten Workflow fortsetzen.

In der überwiegenden Zahl der komplexeren Web-Anwendungen erfolgt eine serverseitige Speicherung der Benutzereingaben[14], zB in einer Datenbank des Webservers. Zu diesem Zweck findet spätestens beim erstmaligen Besuch und der dabei erfolgten Übermittlung von spezifischen Benutzereingaben eine initiale Zuweisung einer ID für den Websitebesucher statt. Diese ID wird clientseitig in der Cookie-Datei gespeichert und auch serverseitig als Zuordnungselement beibehalten. Bei jedem darauffolgenden Zugriff des Benutzers auf die Website bzw eine Unterseite der Website wird der Inhalt der Cookie-Datei vom Webbrowser an den Webserver gesendet – Der Webserver erkennt anhand der erstmalig erstellten und übermittelten ID den Benutzer bzw sein Endgerät „wieder“ und stellt die Relation zu den serverseitig vorgehaltenen Benutzerdaten her[15]. Aus technischen Gründen findet das Zurücksenden der Cookie-Datei an den Webserver bei jedem einzelnen Aufruf einer Unterseite der jeweiligen Website statt – es spielt keine Rolle, ob dieser Aufruf in der nächsten Sekunde oder am nächsten Tag erfolgt[16].

Die Speicherung der Cookies muss nicht notwendigerweise auf der Festplatte des Benutzers erfolgen – so genannte *Session Cookies*[17] werden regelmäßig nur im Speicher des Computers gehalten und gehen beim Schließen der Browser Applikation oder beim Absturz

[14] Die serverseitige Speicherung erlaubt eine wesentlich höhere Flexibilität für die Webapplikation. Außerdem sind Benutzerdaten, die clientseitig in Cookies gespeichert werden, gegenüber unautorisierten Fremdzugriffen bzw Manipulationen schlecht geschützt (zB „Cookie theft“ und andere Angriffsmuster) – vgl <www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/h/*HTTP*_cookie.htm>.

[15] *Schleipfer*, Datenschutzkonformer Umgang mit Nutzungsprofilen, ZD 2015, 399 (400).

[16] *Christl,* Datenschutz im Internet, 21.

[17] *Mutz*, Flash CS3 – AJAX & PHP (2007) 50.

des Computers verloren[18]. Ob ein Cookie clientseitig permanent gespeichert wird oder nicht, bestimmt der Websitebetreiber in seiner Programmierung, indem er für den Cookie ein Ablaufdatum festlegt. Wird kein Ablaufdatum angegeben, so wird lediglich ein *Session Cookie* angelegt[19]. Der Webbrowser ist jeweils selbst dafür verantwortlich, das Cookie-Datenelement nach Ablauf seiner Gültigkeitsdauer zu entfernen. Setzt der Websitebetreiber ein Ablaufdatum, das Tage oder Wochen in der Zukunft liegt, so will er damit offenkundig erreichen, dass der Benutzer auch noch nach Tagen oder Wochen über die ihm zugeordnete ID wiedererkannt wird. In diesem Fall geht der Zweck des Cookies über die Identifikation einer *session* hinaus, denn der Websitebetreiber möchte nicht nur die aktuelle *session* des Benutzers bei dessen Streifzug über seine Website verfolgen, sondern den Benutzer auch wiedererkennen, wenn er seine Website verlassen hat und möglicherweise erst Tage später wieder zurückkehrt. Falls in dem Cookie ein Identifikator gespeichert ist, wird nach der Speicherdauer des Cookies daher zwischen *SessionID* und *BenutzerID* unterschieden.

Beim Einsatz der Cookie Technologie finden demnach (zumindest) die folgenden technischen Verarbeitungsvorgänge statt:

- Das initiale „Setzen“ des Cookies. Hierbei werden serverseitig und/oder clientseitig Daten erhoben bzw erzeugt und gespeichert.
- Zweitens kommt es beim nächsten Besuch des Benutzers zum Auslesen von Daten auf dem Endgerät des Benutzers, zur Übermittlung der Daten zurück an den Webserver und gegebenenfalls zu einer Aktualisierung der am Endgerät gespeicherten Daten nach Anforderung durch den Webserver.
- Schließlich erfolgt auch noch ein gezieltes Löschen des Cookies auf dem Endgerät des Benutzers, entweder durch eine manuelle Operation des Benutzers oder automatisch durch das Endgerät, indem das Ablaufdatum des Cookies erreicht wird.

Der Fokus der weiteren Untersuchung liegt auf Cookies die clientseitig zum Zwecke der Wiedererkennung zumindest eine ID für den Benutzer bzw dessen *session* gespeichert haben, aber die restlichen benutzerspezifischen Daten serverseitig vorhalten. Falls im textuellen Zusammenhang dieser Arbeit eine Unterscheidung zu Cookies notwendig wird, die keine Benutzer- bzw Endgerätespezifische ID gespeichert haben, so wird in diesem Zusammenhang von *non-ID Cookies* gesprochen.

2.1.2 First-Party Cookie und Third-Party Cookie

Als Internetbenutzer rechnet man im Allgemeinen damit, dass nur diejenige Website, welche man gerade willentlich aufgerufen hat – erkennbar durch den Domain-Namen in der

[18] Moderne Webbrowser haben auch für *Session Cookies* eine Wiederherstellungsfunktion. Darauf soll aber hier nicht eingegangen werden.
[19] *Russel,* Dojo: The definitive guide (2008) 63.

Adresszeile des Webbrowser – Cookies versendet und deren lokale Speicherung auf dem eigenen Computer veranlasst. Solche Cookies nennt man *First-Party Cookies*[20] – sie beinhalten als Absenderadresse genau jenen Domain-Namen, der aktuell in der Adresszeile des Browser erscheint und werden auch nur bei einem erneuten Besuch eben dieser Website verarbeitet und an den Webserver zurückgeschickt.

Bei komplexeren Internetangeboten werden allerdings regelmäßig auch Fremdinhalte in die dargestellte Webseite eingebunden. Das sind zB Bilder oder Videos, die sich physisch auf anderen Websites befinden, vom Browser während des Seitenaufbaus von diesen Dritt-Webservern geladen werden und dennoch auf dem Endgerät des Benutzers auf der aktuellen Webseite dargestellt werden[21]. Ein klassisches Beispiel dafür sind Werbebanner die von Dritt-Webservern - sogenannten AdNetworks - geliefert werden. Der ursprüngliche Websitebetreiber (zB die Online Ausgabe einer Tageszeitung) macht dabei auf der Webseite nur eine Referenz zu diesem AdNetwork und weiß oft gar nicht, welcher Inhalt letztlich tatsächlich von dem Adnetwork geliefert wird und auf dem Endgerät des Benutzers erscheint. Ein *Third-Party Cookie* ist ein Cookie, der von diesen Dritt-Webservern gesendet wird und auf dem Computer des Benutzers mit dem Domain-Namen dieses Dritt-Webservers abgelegt wird – die ursprüngliche Website ist weder beim Erstellen noch beim Auslesen dieses Cookies involviert[22]. Auch *Third-Party Cookies* können eine benutzerspezifische ID enthalten. Das AdNetwork ist oftmals auf vielen verschiedenen Website-Angeboten eingebunden[23]. Durch den *Third-Party Cookie* erkennt es ein und denselben User auf unterschiedlichen Web-Angeboten und kann somit ein Profil erstellen, auf welchen Websites der Benutzer in der Vergangenheit war und welche er regelmäßig besucht[24]. Diesen Vorgang der Verfolgung der Internetaktivitäten zum Zwecke der Informationsbeschaffung über einen Internetbenutzer nennt man *tracking*.

Durch den Einsatz von dynamischen, mittels scripting zur Laufzeit modifizierten Webseiten, verschwimmt allerdings die klare Unterscheidung zwischen *First-* und *Third-Party Cookie,* zumindest auf der rein technischen Ebene. Daher wird in weiterer Folge die funktionale Trennung der beiden Cookie Typen hervorgehoben: Das Unterscheidungsmerkmal ist demnach, ob die ursprüngliche Website oder die Dritt-Website den Cookie erzeugt, verwaltet und ausliest und somit Initiator und Nutznießer des Vorgangs der Identifikation und Wiedererkennung ist.

Als eine weitere Methode für das *tracking* von Internetbenutzern existieren auch sogenannte *web beacons*, auch bekannt unter der Bezeichnung *web bugs*. Im Hinblick auf die Identifikation und Wiedererkennung von Webbenutzern unterscheiden sich diese allerdings

[20] *Kaushik*, Web Analytics 2.0 (2010) 128.
[21] *Christl,* Datenschutz im Internet, 100.
[22] *Kaushik,* Web Analytics 2.0, 128.
[23] Das weltweite größte AdNetwork *Google Adsense* ist auf mehr als 15 Millionen Websites eingebunden, Quelle: <www.similartech.com/compare/distroscale-vs-google-adsense>.
[24] *Venzke-Caprarese,* Retargeting in der Onlinewerbung, DuD 2017, 577.

nicht von einer Fremdeinbettung von Webinhalten verbunden mit einem *Third-Party Cookie*. Eine weitere Unterscheidung ist daher an dieser Stelle nicht notwendig. Dasselbe gilt für sogenannte *ETags*, *DOM Web storage*, *supercookies*[25], *flash cookies* usw[26]. Sie alle speichern zum Zwecke der Wiedererkennung Identifikatoren clientseitig ab.

2.1.3 Einschränkungen

Ausgelöst durch die öffentliche Diskussion in Verbindung mit der Cookie-Richtlinie, die darin enthaltenen Einschränkungen sowie dem tw überbordenden Einsatz dieser Technologie durch Websitebetreiber hat sich die generelle Akzeptanz von Cookies auf Seiten der Internetbenutzer stark verschlechtert. Benutzer haben nun vermehrt die Möglichkeit, den Einsatz von Cookies bewusst abzuwählen. Dazu kommt, dass der Benutzer seinen lokalen Cookie-Speicher jederzeit löschen kann. In diesem Fall geht der Bezug zum Websitebetreiber verloren und der Benutzer wird bei einem Folgebesuch, sofern nicht andere Identifikationstechnologien zusätzlich eingesetzt werden, als neuer Nutzer eingeordnet und bekommt eine neue ID zugewiesen.

2.2 Device Fingerprints

Mit Cookies, wie oben dargestellt, ist eine eindeutige Identifikation und Wiedererkennung von Benutzerendgeräten realisierbar. Durch die vermehrten Gegenmaßnahmen auf Seiten der Benutzer und der Browser-Hersteller sind Websitebetreiber auf der Suche nach Alternativen.

Beim *device fingerprinting* wird die Tatsache genutzt, dass Webbrowser beim Aufrufen von Webseiten eine Vielzahl von Informationen übergeben, die das benutzte Endgerät, das Betriebssystem, den Browser sowie die vom Nutzer an diesen Elementen durchgeführten Einstellungen (Konfiguration) beschreiben. Die technische Begründung für dieses Verhalten ist, dass die aufgerufene Website möglichst viele Informationen bekommen soll, um für eine optimale Darstellung der Webseiten auf dem Endgerät des Benutzers zu sorgen[27] – es geht hier also primär um eine Verbesserung der Kompatibilität des Webangebots zu den unterschiedlichen Benutzerendgeräten und -umgebungen. Beispiele für diese Informationen sind: Die Bildschirmauflösung, die Softwareversion des Webbrowsers, die Zeitzone, die eingestellte Sprache des Computersystems/Betriebssystems, diverse Netzwerkeinstellungen, das verwendete Betriebssystem, installierte Browser-Plugins, installierte Fonts etc[28]. Einige dieser Elemente werden bei jeder einzelnen Anfrage an eine beliebige Website im *HTTP header* mitgeschickt. Aus der Zusammensetzung dieser automatisch übermittelten Informationselemente ergibt sich das sogenannte *passive*

[25] Die Terminologie „Supercookie“ ist nicht eindeutig und wird teilweise auch für die Identifikationsmethode *MSISDN Forwarding* benutzt – siehe Kapitel 2.3.
[26] Quelle Wikipedia: <en.wikipedia.org/wiki/*HTTP*_cookie#Alternatives_to_cookies>.
[27] *Alich/Voigt,* CR 2012, 344 (345).
[28] AaO; *Karg/Kühn,* Datenschutzrechtlicher Rahmen für "Device Fingerprinting", ZD 2014, 285.

fingerprinting[29]. Andere Elemente wiederum werden erst durch eine gezielte Programmierung der Website, meistens in Form von Scripts die im Webbrowser des Endgeräts ablaufen, clientseitig erhoben und dann an den Webserver geschickt – Dadurch ergibt sich das sogenannte *active fingerprinting*. Der Code dieser Scripts wird zwar in der Umgebung des Webbrowsers ausgeführt und verlässt diese Umgebung auch nicht, dennoch wird hier – überspitzt formuliert – nichts anderes als Spähsoftware an das Endgerät des Benutzers gesendet und dort ausgeführt. Erst diese Spähsoftware erlaubt ein gezieltes Auslesen von computer- und benutzerspezifischen Einstellungen. Die einzelnen ausgelesenen Informationselemente werden kombiniert und auf dem Webserver abgespeichert – diese Kombination ergibt dann den sogenannten *fingerprint,* der von nun an als Identifikator fungiert.

Der *fingerprint* repräsentiert ein bestimmtes Maß an Eindeutigkeit des Endgeräts gegenüber anderen und ermöglicht dadurch eine Wiedererkennung. Sowohl Anbieter von *device fingerprinting* Produkten als auch unabhängige Studien zeigen, dass bis zu 90% aller weltweit im WWW eingesetzten Endgeräte einen eindeutigen *fingerprint* haben[30]. Trotzdem bleibt festzuhalten, dass das Verfahren einer engen Definition des Begriffs *Identifikation* nicht gerecht wird - Die Abbildung zwischen Endgerät und zugeordneter Kennzeichnung ist nur beschränkt eindeutig[31] und schon gar nicht eineindeutig[32]. Somit ist die Wiedererkennung eines Benutzers nur über statistische Methoden realisierbar und es besteht das Risiko für *false positives*[33]. Die Technologie ist daher nicht für Anwendungsfälle geeignet, die auf eine fehlerfreie Wiedererkennung angewiesen sind. Für Anwendungsfälle, wo eine exakte und eindeutige Wiedererkennung nicht erforderlich ist, sondern eine ausreichend hohe Wahrscheinlichkeit der korrekten Wiedererkennung genügt, ist die Technologie allerdings eine brauchbare Alternative zu Cookies bzw kann auch in Kombination dazu eingesetzt werden.

Wie oben erläutert, ist die IP Adresse für die meisten Internetbenutzer dynamisch zugewiesen, allerdings ändert der Internetbenutzer iA nur sehr selten seinen Internetprovider. Ein Internetprovider vergibt die dynamischen IP Adressen aus einem öffentlich bekanntgemachten[34] Pool – aus dieser Zuweisung lässt sich üblicherweise auch grob der Aufenthaltsort des Benutzers bestimmen (Ort, Stadtteil)[35]. Zwischen der aktuellen IP Adresse eines Benutzers und seiner vorangegangenen gibt es demnach eine statistisch

[29] Quelle World Wide Web Consortium: <w3c.github.io/fingerprinting-guidance>.
[30] *Peter Eckersley,* How Unique Is Your Web Browser?, 5 <panopticlick.eff.org/static/browser-uniqueness.pdf>; Internetprojekt „AmAbs 1Unique“ <amiunique.org>; Uni Erlangen, Study on Browser Fingerprinting <browserfingerprint.cs.fau.de/statistics/?lang=en>.
[31] Sobald ein Benutzer Änderungen an seiner Endgerätekonfiguration vornimmt – zB zusätzliche Fonts, Software Updates, neue Browser Plug-ins - ändert sich sein *fingerprint*.
[32] Dh mehrere unterschiedliche Benutzer/Computer haben denselben *fingerprint.*
[33] Damit ist die „vermeintliche“ Wiedererkennung eines bestimmten Internetbenutzers gemeint, obwohl es in Wirklichkeit ein anderer ist.
[34] Das Register wird von der Organisation RIPE geführt: <www.ripe.net>.
[35] Verschiedene Unternehmen bieten IP geolocation Dienste an, zB <www.maxmind.com/en/geoip2-precision-demo>.

erfassbare Beziehung die im Zusammenspiel mit der *device fingerprinting* Technologie besonders zur Erkennung von *false positives* genutzt wird[36]. Nach gängiger Definition ist die IP Adresse zwar kein Standard-Datenelement des *device fingerprints*[37], wird in der Praxis allerdings oftmalig als Zusatzinformation zum Zweck der Erhöhung der Trefferrate ebenfalls abgespeichert.

2.3 Identifikation mithilfe des Internetproviders (ISP)

Ein seit Jahren gängiges und in letzter Zeit verstärkt angebotenes Bezahlverfahren im Internet ist das sogenannte *Direct Carrier Billing,* früher auch unter der Bezeichnung *WAP Billing* geläufig. Dabei wird die Identifikation eines Internetbenutzers auf einer Website mittels Zusatzinformationen, die zwischen dem Internetprovider des Benutzers und dem jeweiligen Websiteanbieter ausgetauscht werden, durchgeführt. Das Verfahren findet bevorzugt im Mobilfunkbereich Anwendung, daher ist der Internetprovider (Access-Provider) hier ein Mobilfunkanbieter. Dieser hat iA verifizierte Stammdaten des Benutzers in seinem *Customer Relationship Management* System vorliegen - darunter Name, Adresse, Bankverbindung und zwingenderweise auch die jeweilige Mobilfunkrufnummer (MSISDN[38]) des Teilnehmerendgeräts. Durch eine vertragliche Vereinbarung zwischen dem Mobilfunkprovider und dem Websiteanbieter ist es nun möglich, dass ein Benutzer eine gekaufte Ware im Webshop des Websiteanbieters über seine Mobiltelefonabrechnung bezahlen kann. Der Mobilfunkbetreiber verpflichtet sich zur nachträglichen Weitergabe des eingezogenen Geldes an den Webshop-Betreiber und erhält daraus oft eine Provisionszahlung. Zivilrechtlich sind solche Konstruktionen tw mit Forderungsabtretungen gelöst[39]. Die dahinterliegende Technologie kann abseits von Bezahlungsdiensten allerdings auch für andere Anwendungsfälle eingesetzt werden, da aus Sicht des Websitebetreibers hier ebenfalls eine Identifikation und Wiedererkennung eines Internetbenutzers stattfindet.

Die in dieser Arbeit näher analysierte technische Realisierung dieser Identifikationsmethode ist das sogenannte *MSISDN forwarding*, auch bekannt unter der Bezeichnung *HTTP header enrichment.* Dabei wird die MSISDN des Mobilfunkkunden, entweder im Klartext oder in pseudonymisierter Form, bereits direkt beim ersten Aufruf der Website automatisch an den Websitebetreiber übermittelt und fungiert somit als Identifikator. Dieser Identifikator hat eine Doppelfunktion: Auf Seiten des Access-Providers identifiziert er den (namentlich bekannten) Mobilfunkkunden, also den Vertragspartner (Teilnehmer). Auf Seiten des Websiteanbieters

[36] Quelle: <https://resources.distilnetworks.com/all-blog-posts/device-fingerprinting-solution-bot-mitigation>.
[37] *Zimmeck/Li/Hyungtae/Bellovin/Jebara*, A Privacy Analysis of Cross-device Tracking (2017) 17.
[38] Die MSISDN ist diejenige Telefonnummer die gewählt werden muss um das Teilnehmerendgerät anzurufen. Intern identifiziert der Mobilfunkbetreiber seine Kunden bevorzugt mit der sogenannten IMSI, welche vom äußeren Erscheinungsbild her ebenfalls eine Telefonnummer ist, mit der MSISDN in einer fixen Beziehung steht aber nicht mit dieser identisch sein muss (zB Aufgrund einer Rufnummernportierung). Für den Mobilfunkbetreiber sind beide Kennzeichen Teil des Stammdatensatzes des Teilnehmers. Für Dritte ist die MSISDN die tatsächliche Telefonnummer der betroffenen Person und die IMSI iA ein Pseudonym.
[39] *Lust*, Telekommunikationsrechtliche Änderungen aus Kundensicht, VbR 2016/6, 16.

identifiziert er den aktuellen Besucher der Website – hier gibt es iA noch keine Referenz zur realen Identität des Besuchers. Im Endeffekt kann es sich hierbei durchaus um zwei unterschiedliche reale Personen handeln, etwa wenn Nutzer und Vertragspartner unterschiedliche Personen sind (zB Familienmitglieder). Aufgrund der automatischen, für den Benutzer unsichtbaren, Datenübermittlung der MSISDN an den Webserver des Webshop-Betreibers muss der Kunde beim Bezahlvorgang nicht mehr seine Telefonnummer manuell ein- bzw bekanntgeben (sogenannte „1-Click" Zahlung). Die MSISDN wird innerhalb des Übertragungsprotokolls HTTP in dessen Protokollheader (*HTTP header*) übermittelt. Der Mobilfunkbetreiber „injiziert" den Identifikator in die Kommunikationsverbindung zwischen dem Smartphone und der aufgerufenen Website. Während Mobilfunkprovider in der Vergangenheit teilweise freizügig mit dieser Informationsübermittlung umgegangen sind[40], wurden in den letzten Jahren hier mehrfach Einschränkungen gemacht. Derzeit ist es üblich, die MSISDN nur in pseudonymisierter Form, teilweise auch in zeitlich veränderlicher Darstellung (sogenannte *rotation*), und auch nur an gezielt ausgewählte Partner-Websites zu übermitteln (sogenanntes *whitelisting*).

2.4 Nicht näher untersuchte Identifikationsmethoden - Auswahl

Zum Zwecke der Klarstellung und der Abgrenzung seien an dieser Stelle noch einige gängige Identifikationsmethoden genannt, die im Zuge dieser Arbeit nicht näher untersucht werden.

Eine freiwillige Registrierung zu einem geschlossenen Bereich einer Website („Login-Area") ist eine klassische Methode, um einen Websitebenutzer wiederzuerkennen. Diese Methode wird im Zuge dieser Arbeit allerdings nicht weiter untersucht, da es vorwiegend um automatisierte Verfahren zur Identifikation und Wiedererkennung geht und außerdem in diesem Fall der Websitebetreiber im Zuge der Registrierung ein Vertragsverhältnis mit spezifischen datenschutzrechtlichen Vereinbarungen anbieten kann und somit keine Allgemeingültigkeit vorherrscht.

Dann gibt es noch Methoden, wo ein Websitebetreiber mit einem hochgradig personalisierten Internetdienst - zB *Facebook* oder *Google* - zusammenarbeitet. Viele Internetbenutzer sind bei *Google* und/oder *Facebook* registriert. Beim Besuch der Website werden dann mit *Google* und/oder *Facebook* Identifikationsdaten ausgetauscht (zB über den sogenannten *Like-Button*). Die Internetnutzer stehen hier in einem Vertragsverhältnis mit *Google* und/oder *Facebook*. Eine Analyse dieser Verträge und das Zusammenwirken mit den

[40] Eine Untersuchung aus dem Jahr 2015 von 299 Mobilfunkprovidern in 112 Ländern kam zu dem Ergebnis, dass zwei Mobilfunkprovider die MSISDN im Klartext sowie sechs Mobilfunkprovider als Pseudonym ohne jegliches *whitelisting* verschickten - Quelle: *Narseo/Sundaresan/ Kreibich,/Paxson*, header Enrichment or ISP Enrichment? - Emerging Privacy Threats in Mobile Networks (2015) <www.icsi.berkeley.edu/~narseo/papers/hotm42-vallinarodriguez.pdf>. Eine andere Untersuchung, ebenfalls aus dem Jahr 2015, hat bei 15,3% der untersuchten Benutzer (Sample: 180.000) *tracking* taugliche Daten im *HTTP header* gefunden - Quelle: Access Now, <www.accessnow.org/aibt>.

anwendbaren Datenschutzgesetzen ist nicht Teil dieser Arbeit. Im Fokus steht derjenige Internetbenutzer, der das WWW ohne vorgelagerten Authentifizierungsmechanismus nutzt.

Das Betriebssystem mobiler Endgeräte generiert und persistiert einen gerätespezifischen Identifikator, die sogenannte *Advertising ID*[41]. *Mobile Apps*, die der Nutzer auf seinem Endgerät installiert hat, senden diese *Advertising ID* an den Server des jeweiligen Diensteanbieters zur Wiedererkennung des Endgeräts[42]. Die genannte Technologie wird in dieser Arbeit allerdings nicht näher behandelt, denn die *Advertising ID* wird nur in Verbindung mit *Mobile Apps* eingesetzt. Das Betriebssystem des Smartphones verhindert, dass der lokal installierte Webbrowser des Endgeräts Zugriff auf diesen Identifikator hat. Daher hat auch der im Zentrum der Untersuchung stehende Betreiber einer Internetwebsite im WWW keinen Zugriff auf die *Advertising ID*[43].

[41] Bezeichnung dieses Identifikators bei Apple Geräten: *IDFA*; bei Android Geräten: *AAID.*
[42] *Hanloser,* Geräte-Identifier im Spannungsfeld von DS-GVO, TMG und ePrivacy-VO, ZD 2018, 213.
[43] marketingland.com: <marketingland.com/google-replacing-android-id-with-advertising-id-similar-to-apples-idfa-63636>.

3. Ermittlung des rechtlichen Prüfmaßstabs

3.1 Annahmen und Einschränkungen

Für die weitere Untersuchung soll, sofern nicht anders angegeben, von einem österreichischen Unternehmen als Websitebetreiber sowie österreichischen Nutzern als natürliche Privatpersonen dieses Internetangebots ausgegangen werden. Der Websitebetreiber hat annahmegemäß für den Fortgang der Untersuchung auch Drittinhalte eingebunden. Dieser Dritte ist wahlweise entweder ein Unternehmen im EU Ausland oder ein US-amerikanisches Unternehmen, wobei letzteres annahmegemäß Waren oder Dienstleistungen an betroffene Personen innerhalb der EU anbietet.

3.2 Datenschutz-Grundverordnung

3.2.1 Allgemeiner, sachlicher und räumlicher Anwendungsbereich Art 2,3 DSGVO

Für den Internetnutzer und den Websitebetreiber ergibt sich die unmittelbare räumliche Anwendbarkeit der DSGVO aus Art 2 Abs 1 DSGVO. Für den Dritten ergibt sich im Falle eines europäischen Unternehmens die Anwendbarkeit der DSGVO ebenfalls aus Art 2 Abs 1 DSGVO über den Begriff der Niederlassung. Für das US-amerikanische Unternehmen ergibt sich die Anwendbarkeit aus Art 2 Abs 2 lit a DSGVO – unabhängig davon, ob es eine Niederlassung innerhalb der EU betreibt oder nicht und unabhängig von dem physischen Ort der Datenverarbeitung. Es gibt keine Anhaltspunkte für die Berücksichtigung der Haushaltsausnahme gemäß Art 2 Abs 2 lit c DSGVO. **Die zentrale Fragestellung für die Eröffnung des Anwendungsbereichs der DSGVO ist demnach, ob beim Einsatz der in Kapitel 2 vorgestellten Technologien eine Verarbeitung von personenbezogenen Daten durch einen Verantwortlichen stattfindet. Dies wird zunächst unabhängig von einem konkreten Anwendungsfall beurteilt.**

3.2.2 Anwendungsbereich beim Einsatz von *HTTP Cookies*

Mit Bezug auf das Einführungskapitel 2.1.1 sei erinnert, dass mithilfe von Cookies benutzerspezifische Daten serverseitig oder auch clientseitig gespeichert werden können. Clientseitig werden Benutzerdaten in sogenannten *non-ID Cookies* gespeichert. In dieser Ausprägung des *HTTP Cookies* ist keine Zuweisung einer *BenutzerID* oder *SessionID* notwendig. Gem. Art 4 Z 1 DSGVO werden nur dann personenbezogene Daten verarbeitet, wenn die verarbeitenden Informationen sich auf eine identifizierte (=bestimmte) oder identifizierbare (=bestimmbare)[44] Person beziehen. Auch wenn es aus dem direkten Wortlaut

[44] Die Gleichsetzung der beiden Begriffe *bestimmbar* und *identifizierbar* wäre im Hinblick auf das Verhältnis zwischen der DSGVO und der Datenschutzrichtlinie 95/46/EG zulässig (vgl *Ernst* in *Paal/Pauly* (Hrsg), Kommentar zu DS-GVO, BDSG² (2018) Art 4 Rn 8). Im Folgenden wird für die datenschutzrechtliche Prüfung des Personenbezugs vorwiegend der Begriff *Bestimmbarkeit* verwendet. Hingegen steht der Begriff der *Identifikation* in dieser Arbeit lediglich für den Vorgang einer Kennzeichenzuordnung und noch nicht für die Herstellung der Relation dieses Kennzeichen zu einer realen Person.

von Art 4 Z 1 DSGVO nicht mehr so klar hervorgeht wie aus den bisherigen nationalen Datenschutzgesetzen[45], so muss es sich bei diesen *Informationen* dennoch im weitesten Sinn um Informationen, konkreter um Aussagen, *über* eine Person handeln[46]. Um das Kriterium *bestimmbar*[47] zu erfüllen, ist jedenfalls ein ausreichendes Maß an Unterscheidbarkeit notwendig, um Datensätze die auf unterschiedliche Personen verweisen, voneinander abzugrenzen – sogenannte Individualisierbarkeit[48]. Dieses Maß ist beispielsweise dann nicht erreicht, wenn ein *non-ID Cookie* ausschließlich dafür verwendet wird, die vom Benutzer getätigte Spracheinstellung auf einer Website abzuspeichern. In Verbindung mit der tatsächlichen Bestimmung der realen Person könnte dies zwar sehr wohl als Eigenschaft oder zumindest als Vorliebe dieser Person aufgefasst werden. Aber: Annahmegemäß gibt es sehr viele unterschiedliche Nutzer, die genau dieselbe Einstellung gewählt haben. Vorausgesetzt es findet serverseitig keine Speicherung und Zusammenführung mit einer anderen Information wie bspw der IP Adresse statt, ist der Benutzer jedenfalls alleine anhand der Information über die gewählte Spracheinstellung nicht bestimmbar[49]. Andererseits sind Konstellationen denkbar, in welchen der Benutzer Eingaben oder Einstellungen auf der Website tätigt, die so individuell sind, dass deren Abbildung in einem *non-ID Cookie* den Benutzer von allen anderen ausreichend unterscheidbar macht. Genauso sind Eingaben und Einstellungen denkbar, die nach ihrem Informationsgehalt für sich selbst Rückschlüsse auf eine bestimmte Person zulassen. Ob beim Einsatz von *non-ID Cookies* personenbezogene Daten verarbeitet werden oder nicht, kann daher nicht allgemein gültig entschieden werden – Dies ist vom jeweiligen Anwendungsfall abhängig und wird in Kapitel 4.3 entsprechend differenziert untersucht.

Für die serverseitige Speicherung von Benutzerdaten ist allerdings zunächst das Erzeugen, Zuweisen und Abspeichern einer ID erforderlich. In diesem Zusammenhang ist somit fraglich, ob die server- bzw clientseitige Verarbeitung und Speicherung dieser ID bereits eine Verarbeitung von personenbezogenen Daten iSv Art 4 Z 1, 2 DSGVO ist – vorerst unabhängig davon beurteilt, ob die weiteren serverseitig vorgehaltenen Benutzerdaten (zB die gewählte Spracheinstellung oder der aktuelle Warenkorb) personenbezogen sind. Dabei gilt es ebenfalls zu beachten, dass in diesem Fall unmittelbar nur das Endgerät des Benutzers identifiziert wird und vorerst keine direkte Referenz auf den Benutzer selbst hergestellt wird[50].

[45] Volltextauszug DSG 2000: „Angaben über Betroffene"; Volltextauszug BDSG (alte Fassung): „Einzelangaben über persönliche oder sachliche Verhältnisse".
[46] *Art-29-Datenschutzgruppe*, WP 136, 9.
[47] Das Konzept der *indirekt personenbezogenen Daten* aus dem DSG 2000 ist spätestens seit dem 25.5.2018 obsolet und wird daher nicht mehr betrachtet - vgl dazu EuGH 19.10.2016, C-582/14 (Breyer) = jusIT 2016, 252 (*Jahnel*)
[48] Dieser Begriff wird in der datenschutzrechtlichen Literatur sehr unterschiedlich gebraucht. Hier soll *Individualisierbarkeit* als notwendige Vorstufe zur *Bestimmbarkeit* verstanden werden.
[49] Vgl dazu Kapitel 4.1.1.
[50] *Jahnel,* Datenschutzrecht, in *Jahnel/Mader/Staudegger* (Hrsg), IT-Recht³ (2012) 415 (426).

Bei der erstmaligen Identifikation des Benutzers wird serverseitig ein eindeutiges Identifikationselement („ID“) für den Computer des Benutzers erzeugt. Diese ID wird serverseitig eine gewisse Dauer vorgehalten (*SessionID*, *BenutzerID*), an das Endgerät des Benutzers übermittelt sowie dort als Datenelement (=Cookie) abgespeichert. Eine Verarbeitung gemäß Art 4 Z 2 DSGVO von Informationen findet somit sowohl serverseitig als auch clientseitig statt - fraglich bleibt jedoch der Personenbezug dieser Verarbeitung. Das Endgerät des Benutzers ist ab sofort mit einem Identifikator versehen und wiedererkennbar. Unklar ist jedoch, ob diese ID eine Information ist, die sich iSv Art 4 Z DSGVO auf eine bestimmbare Person bezieht. Dafür muss es zwischen dem Benutzer und seinem Endgerät eine aufrechte Beziehung geben, welche den Rückschluss vom Endgerät auf die Person ausreichend genau zulässt, und diese Beziehung muss von einem Verantwortlichen oder einem Dritten mit real existierenden Mitteln, welche nach allgemeinem Ermessen wahrscheinlich genutzt werden, herstellbar sein[51]. Eine solche Beziehung kann bspw die Eigentümerstellung, die regelmäßige Benutzung oder der Standort des Geräts in der Wohnung des Benutzers sein.

Bereits im Jahr 2008 formulierte die *Art-29-Datenschutzgruppe*[52]: „Wenn ein Cookie eine eindeutige Benutzerkennung enthält, handelt es sich bei dieser Kennung eindeutig um personenbezogene Daten“[53]. Eine juristische Begründung erfolgt an der genannten Stelle nicht. Im darauffolgenden Satz wird allerdings die Motivation für diese Einordnung geliefert: „Die Benutzung von *persistenten* Cookies mit einer eindeutigen Benutzerkennung erlaubt das *tracking* von Benutzern (...) Diese Verhaltensprofile erlauben eine verstärkte Fokussierung auf persönliche Eigenschaften des Datensubjekts“. Eine Aussage zu *nicht-persistenten* Cookies wird allerdings hier nicht getroffen - Diese erlauben eben gerade nicht eine Wiedererkennung des Benutzers über die derzeitige *session* hinaus und somit auch kein *tracking* nach der gängigen Definition. Eine ID, welche nur für die derzeitige *session* vergeben und danach gelöscht wird und per definitionem nicht dazu geeignet ist, den Benutzer beim nächsten Besuch wiederzuerkennen, kann auch keine eindeutige Benutzerkennung im Sinne des obigen Zitats sein. Es ist vielmehr eine zeitlich begrenzt gültige Kennung des Endgeräts.

Diese ist auch nur für den Zeitraum der aktiven *session* eindeutig und kann danach in identischer Art und Weise an ein anderes Endgerät vergeben werden[54]. Der wiederkehrende Benutzer erhält eine neue S*essionID. O*hne zusätzliche Verknüpfungselemente gibt es keinen Bezug zu seinem vorangegangenen Besuch. Nach dem in dieser Arbeit vertretenen Wortsinn von „eindeutiger Kennung“, welcher die theoretische Möglichkeit der

[51] ErwGr 26 DSGVO.

[52] Die *Art-29-Datenschutzgruppe* wurde am 25.5.2018 aufgelöst. An ihre Stelle trat *das European Data Protection Board.* In dieser Arbeit wird aber ausnahmslos auf Dokumente verwiesen, die unter dem alten Namen veröffentlicht wurden.

[53] *Art-29-Datenschutzgruppe*, WP148, 9.

[54] Das ist bei gängigen Implementierungen von Webanwendungen tatsächlich auch so der Fall - Quelle: <stackoverflow.com/questions/138670/how-unique-is-the-php-session-id>.

Wiedererkennung voraussetzt, ist eine *SessionID* daher nicht *eindeutig* und daher auch nicht unter der obigen Aussage der *Art-29-Datenschutzgruppe* subsumierbar.

Die *Art-29-Datenschutzgruppe* erwähnt den Personenbezug von Cookies textuell sehr oft in einem systematischen Zusammenhang mit IP Adressen[55]. Ähnlich auch ErwGr 30 DSGVO, allerdings geht man dort noch weiter: Dort werden IP Adressen und „Cookie-Kennungen"[56] unter dem Begriff „Online Kennungen" zusammengefasst und ebenfalls mit dem Vorgang des *tracking* in Zusammenhang gebracht. Daraus kann man aber nicht die Schlussfolgerung ableiten, dass die Annahme eines Personenbezugs von IP Adressen[57] für sich alleine eine schlüssige Begründung für die Annahme eines Personenbezugs von Cookies liefert. Die Argumentationslinie des EuGH für die Begründung des Personenbezugs von IP Adressen geht auf die Bestimmbarkeit des Internet-Anschlussinhabers als Kunde des Access-Providers zurück: Wenn für den Websitebetreiber rechtlich zulässige Mittel existieren, die Verknüpfung zwischen der ihm vorliegenden IP Adresse und dem tatsächlichen Anschlussinhaber über eine Anfrage beim Access-Provider herauszufinden, muss er die ihm vorliegende IP Adresse als personenbezogenes Datum behandeln[58]. Die Argumentation geht zutreffenderweise davon aus, dass es beim Access-Provider eine zu jedem Zeitpunkt eindeutige Zuordnungstabelle zwischen der aktuellen IP Adresse und den Stammdaten[59] des Anschlussinhabers gibt[60]. **Eine vergleichbare Zuordnungstabelle zu Stammdaten einer natürlichen Person gibt es jedoch im Falle einer in einem Cookie gespeicherten Benutzerkennung nirgends und zu keinem Zeitpunkt.** Solange die IP Adresse nicht in nicht-anonymisierter[61] Form als zusätzliches Identifikationselement herangezogen wird, gibt es daher vorerst nur eine Zuordnung zwischen dem Endgerät des Benutzers und der zugewiesenen ID. Aus Sicht des Websitebetreibers ist diese Zuordnung zwar eine Individualisierung eines bestimmten Endgeräts, aber keine physische Zuordnung zu dem einen realen Gerät – er weiß nicht einmal, wo sich das Gerät befindet. Eine physische Zuordnung ergibt sich erst durch die Kenntnis, auf welchem Gerät der entsprechende Cookie lokal abgespeichert ist. Und erst über diesen Umweg wäre es möglich den regelmäßigen Benutzer bzw Eigentümer dieses Geräts, zB durch Beobachtung oder andere Informationen, zu bestimmen.

[55] So beispielsweise nicht nur in WP148 sondern auch in WP171, 11.
[56] Aus dem Zusammenhang geschlossen muss man annehmen, dass hier persistente Benutzer-Kennungen gemeint sind
[57] Dies war für dynamische IP Adressen lange Zeit umstritten, soll aber für den Fortgang der Untersuchung ausgehend von der jahrelangen Argumentationslinie der *Art-29-Datenschutzgruppe* und letztlich entschieden durch EuGH 19.10.2016, C-582/14 (*Breyer*) als zutreffend angenommen werden. aA *Geuer/Reinisch*, Direktwerbung und Cookies im Spannungsfeld des TKG und der DSGVO, MR 2018, 123 (133) - die Autoren lehnen die Übertragung dieser Schlussfolgerung aus der *Breyer* Entscheidung für den österreichischen Rechtsrahmen ab.
[58] AaO Rn 49.
[59] Beispielhaft: Name, Adresse, Kontaktdaten (zB: Telefonnummer, email Adresse), Kontodaten etc.
[60] An dieser Stelle sei noch offen gelassen, ob der Access-Provider die Zuordnungstabelle persistiert und somit für spätere Abfragen – bspw nach Tagen oder Wochen – vorhält oder nicht.
[61] Eine gängige Methode zur Anonymisierung ist die verkürzte Darstellung/Abspeicherung, zB: 192.168.XXX.XXX .

Für eine Entscheidung über den Personenbezug der *BenutzerID* bzw *SessionID* könnte daher letztlich wiederum eine Differenzierung der beiden Theorien zur Bestimmbarkeit erforderlich sein – die *relative* und die *absolute*[62] Theorie[63]. In der *Breyer* Entscheidung folgt der EuGH und im Anschluss auch der BGH[64] einer verschärften Variante der relativen Theorie[65] und stellt auf die „rechtlichen Mittel" ab, denen sich ein Verantwortlicher bedienen kann, um mithilfe eines Dritten die Person zu bestimmen. Der BGH hat im Anschluss an die EuGH Entscheidung die rechtlich existierende Möglichkeit des Websitebetreibers, den Bezug zur natürlichen Person des Internet-Anschlussinhabers über den Umweg der Strafverfolgungsbehörden und über den Access-Provider (welcher bekannt ist) herzustellen, genügen lassen[66]. Der oben genannten Auslegung der relativen Theorie des EuGH soll hier gefolgt werden - Eine vertiefte Analyse der absoluten Theorie erfolgt nicht[67].

Betrachtet man nun die *BenutzerID* bzw die *SessionID* für sich alleine und nimmt vorerst keine Zusammenführung mit der IP Adresse des Benutzers an, dann führt die obige Auslegung des Kriteriums der *Bestimmbarkeit* zu der folgenden Schlussfolgerung: Der Websitebetreiber hat überhaupt keinen Anhaltspunkt an welchen Dritten er sich für eine etwaige Zusammenführung mit anderen Informationen wenden soll. Einen solchen Dritten, der das notwendige Zusatzwissen für die Bestimmbarkeit der Person systematisch vorhält, gibt es auch gar nicht. Das Zusatzwissen, welches mit Hilfe der ID zumindest die Bestimmbarkeit des Endgeräts liefern könnte, ist durch Abhören der Internetkommunikation des Benutzers oder durch einen Einbruch in seinen Computer herstellbar. In diesen theoretisch möglichen Fällen liefert aber gerade die ID im Cookie keine zusätzliche Information für die Bestimmbarkeit des Endgeräts, denn bei diesen Angriffen wird die IP Adresse des Endgeräts offengelegt. In diesem Fall wären Endgerät - und über den Umweg des Access-Providers - auch der Benutzer des Endgeräts ohnehin voll bestimmt[68].

Allerdings: Aus einer streng technischen Perspektive heraus geschieht die serverseitige Verarbeitung der ID immer gemeinsam mit der IP Adresse des Benutzers. Das ist beim Einsatz des Internetprotokolls TCP/IP unvermeidlich, da sowohl Quell-IP als auch Ziel-IP Adresse in jedem übermittelten Datenpaket vorhanden sind. Auch wenn die IP Adresse serverseitig nicht gespeichert wird, so könnte man dennoch zumindest ein *Auslesen* iSv

[62] Gemeinhin auch *objektive* Theorie genannt.
[63] *Dammann* in *Simitis* (Hrsg), Kommentar zum BDSG[8] (2014) §3 Rn 23, 24.
[64] EuGH 19.10.2016, C-582/14 *(Breyer)*; BGH 16.5.17, VI ZR 135/13 = NJW 2017, 2416 (*Bierekoven*) = WuB 2017/11, 606 (*Hoeren*) = GRUR-Prax 2017, 333 (*Schreiber*) = GSZ 2018, 113 (*Breyer*) = CR 2017, 662 (*Keppeler*).
[65] Südwest Datenschutz Rechtsanwaltsgesellschaft , <www.suedwest-datenschutz.com/sind-ip-adressen-personenbezogene-daten-die-sicht-des-eugh>.
[66] In Österreich gilt: § 76a Abs 2 Z 1 StPO iVm § 99 Abs 5 TKG zur Ermittlung des Anschlussinhabers und dann weiter mit dem Recht auf Akteneinsicht für die Verfahrensbeteiligten (vgl *Feiler/Horn*, Umsetzung der DSGVO in d. Praxis (2018) 97). AA *Geuer/Reinisch*, MR 2018, 123 (133) – die Autoren rekurrieren auf das Zivilverfahren, wo derzeit die Ermittlung des Anschlussinhabers prozessual sehr schwierig ist. Diese prozessuale Hürde kann für sich alleine allerdings nicht genügen, den Personenbezug von dynamischen IP Adressen per se abzulehnen.
[67] Anmerkung: Auch die absolute Theorie ist im Lichte von ErwGr 26 DSGVO (Volltext: „nach allg. Ermessen wahrscheinlich genutzt werden" bzw „vernünftigerweise angewendet") nicht beliebig weit auszudehnen (vgl *Riesz* in *Riesz/Schilchegger* (Hrsg), Telekommunikationsgesetz (2016) § 92 Rn 12; EBRV 1613 BlgNR XX. GP 37; *Dammann* in *Simitis* BDSG § 3 Rn 23).
[68] Annahmegemäß über den Umweg des Anschlussinhabers.

Art 4 Z 2 DSGVO annehmen, und zwar indem das TCP/IP Datenpaket vom Computersystem des Webservers gelesen und intern verarbeitet wird[69]. Die Quell-IP Adresse steht auch temporär für die Dauer der Verbindung im Hauptspeicher des Webserver-Computers als sogenannte Umgebungsvariable der Webserversoftware zur Verfügung und kann von der Applikation des Websitebetreibers sehr einfach ausgelesen werden[70]. Letztlich entscheidet der Websitebetreiber durch seine Programmierung, ob er die IP Adresse aus dem Hauptspeicher übernimmt und innerhalb seiner Applikation weiterverarbeitet, zB um sie abzuspeichern[71] oder mit anderen Daten zu verknüpfen. Für die Zurverfügungstellung eines Webangebots, selbst wenn dieses komplexere Interaktionselemente beinhaltet, ist dies iA aber nicht erforderlich. Dennoch muss an dieser Stelle die Frage aufgeworfen werden, ob nicht jedes einzelne Datum, welches über das Internet übertragen wird, letztlich als personenbezogenes Datum angesehen werden muss, alleine aufgrund der Tatsache, dass es in den beteiligten Protokollstacks jedenfalls gemeinsam mit der IP Adresse verarbeitet wird. Das Ergebnis dieser Schlussfolgerung wäre, dass der Websitebetreiber als Verantwortlicher keine Maßnahme setzen kann, den Personenbezug von aus dem Internet empfangenen Daten zu verhindern und sich auch schon für den alleinigen Empfang von Datenpaketen ein datenschutzrechtliches Rechtfertigungserfordernis ergibt. Das ist abzulehnen. Es würde die Zielsetzung des Datenschutzes zu weit ausdehnen, wenn man alleine die Tatsache „Benutzer XY hat ein beliebiges Datum an Websitebetreiber YZ versendet“ als datenschutzrelevanten Vorgang einordnet. Im Falle der Nicht-Speicherung der Absender IP Adresse auf Seiten des Websitebetreibers muss die Begrifflichkeit der *Verarbeitung personenbezogenen Daten* iSv Art 4 Z 1,2 DSGVO beim Empfangen von beliebigen Inhaltsdaten über das Internet daher teleologisch reduziert werden. Der alleinige, singuläre Empfang von TCP/IP Paketen ist weder ein Auslesen, ein Erheben, ein Erfassen, ein Abfragen noch eine andere Verarbeitungsform iSd DSGVO. Dieses Ergebnis steht auch nicht im Widerspruch zur *Breyer* Entscheidung, wo ausdrücklich nur „IP Adressen, die vom Anbieter *gespeichert* werden“[72] als personenbezogenes Datum eingeordnet werden. Solange auf Seiten des Verantwortlichen keine *aktive* Verarbeitung der Absender-IP Adresse stattfindet, muss es möglich sein, einzelne Daten innerhalb der Nutzdaten der Übertragung als nicht-personenbezogen anzusehen. **Alleine aus der kommunikationstechnischen, serverseitigen Verarbeitung der *BenutzerID* bzw *SessionID* ergibt sich demnach noch kein Personenbezug dieser beiden Identifikatoren.**

Die *SessionID* könnte hingegen als ein Pseudonym aufgefasst werden, welches der Websitebetreiber selbst vergibt und verwaltet und statt der IP Adresse des Besuchers intern

[69] Jedenfalls im sogenannten TCP/IP Protokollstack des Betriebssystems.
[70] Wikipedia, Common Gateway Interface: <en.wikipedia.org/wiki/Common_Gateway_Interface> .
[71] Zum sogenannten *HTTP Access Log,* welches alle Zugriffe auf die Website speichert, siehe Kapitel 4.1.1.
[72] Tenor zu EuGH 19.10.2016, C-582/14 (*Breyer*).

verwendet, um die Datenverarbeitung mit dem Websitebenutzer abzuwickeln[73]. Pseudonyme sind Zeichenfolgen mit Namensersatzfunktion[74]. Einer Pseudonymisierung unterzogene personenbezogene Daten (hier: die IP Adresse), die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine bestimmbare natürliche Person betrachtet werden[75]. Für die Zeit der *session* herrscht eine fixe Zuordnung zwischen dem Pseudonym und der IP Adresse. Fraglich ist allerdings, ob die *SessionID* auch als Pseudonym für den Computer oder gar den Benutzer aufgefasst werden kann. Wie oben bereits dargestellt ist das aber genau nicht der Fall, weil durch das Pseudonym nur die *aktuelle* IP Adresse des Besuchers dargestellt wird. Es gibt keinerlei Beziehung zu seinem vorangegangenen Besuch, auch nicht wenn er über dasselbe Endgerät ausgeführt wurde. Wenn ein Pseudonym aber nicht den Zweck und auch nicht die Fähigkeit hat, eine Person zu referenzieren, dann ist es kein Pseudonym iSv Art 4 Z 5 DSGVO – die Frage nach einer möglichen De-Pseudonymisierung stellt sich somit gar nicht. Im Zwischenergebnis ist die *SessionID* daher kein Pseudonym für den Computer des Benutzers, und damit auch denknotwendigerweise kein Pseudonym für die Person, die den Computer regelmäßig benutzt. **Die Vergabe, Übermittlung und vorübergehende Speicherung der *SessionID* ist daher keine Verarbeitung personenbezogener Daten iSv Art 4 Z 1,2 DSGVO.** Dieses Ergebnis widerspricht auch nicht dem zitierten Wortlaut der *Art-29-Datenschutzgruppe* bzw ErwGr 30 DSGVO.

Im Gegensatz zur *SessionID* wird die *BenutzerID* serverseitig und clientseitig dauerhaft vorgehalten und dient dazu, den Computer (!) des Benutzers beim nächsten Besuch wiederzuerkennen. Da der Computer nicht selbstständig im Internet surft ist die Wiedererkennung letztlich nach ihrer Zweckbestimmung auf den Benutzer ausgerichtet. Die Tatsache, dass die Zuordnung zwischen dem Benutzer und seinem Computer nicht eindeutig ist, ist als technische Unzulänglichkeit und Unschärfe einzustufen, schließt aber den Personenbezug der *BenutzerID* nicht kategorisch aus[76]. Bis auf wenige Spezialfälle führt die Kenntnis über den Computer bzw dessen Standort nämlich zumindest in das familiäre oder berufliche Umfeld[77] der betroffenen Person und ist als solches der erste, ganz wesentliche Schritt zu einer möglichen Bestimmung der Identität der realen Person. Wurde oben die *SessionID* letztlich deshalb nicht als personenbezogenes Datum qualifiziert, weil es keine Relation zwischen zwei getrennten Besuchen desselben Benutzers gibt, wird im Falle der *BenutzerID* aber nun genau diese Relation hergestellt. **Man kann sagen, dass die *BenutzerID* ein Pseudonym für die aktuelle IP Adresse ist, welches bei jedem Besuch aktualisiert wird und somit im Ergebnis immer ein eindeutiges Pseudonym für die tatsächliche IP Adresse des Besuchers ist.** Selbst wenn diese Relation nicht gespeichert

[73] *Dammann* in *Simitis* BDSG § 3 Rn 220c.
[74] AaO Rn 67.
[75] Erwgr 26 DSGVO ; *Härting*, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065 (2067).
[76] andere Ansicht: *Riesz* in *Riesz/Schilchegger* TKG § 96 Rn 27.
[77] *Schleipfer,* ZD 2015, 399 (404).

wird, so wirkt sie dennoch in die Zukunft, da sie beim nächsten Besuch automatisch wiederhergestellt wird. Wenn also die dynamische IP Adresse als personenbezogenes Datum qualifiziert wird, so muss das auch für die *BenutzerID* des Cookies gelten, denn die verarbeitende Stelle – der Websitebetreiber - hat die eindeutige Relation zwischen diesen beiden Elementen bei jedem Kontakt mit dem Nutzer vorliegen. **Auch wenn sich der Websitebetreiber bewusst gegen die dauerhafte Speicherung der IP Adresse entscheidet – sie ist als Datum in seinem Verarbeitungssystem zumindest vorübergehend vorhanden[78] und wird bei jedem weiteren Besuch des Nutzers zwingend erneut verarbeitet[79]. Es kommt daher notwendigerweise zu einer Verkettung eines sogenannten unveränderlichen Rollenpseudonyms**[80]. Die ständige Aktualisierung der Zuweisung zwischen aktueller IP Adresse und *BenutzerID* untergräbt somit auch jene datenschutzfreundlichen Maßnahmen, welche genau diese Art der Zusammenführung von pseudonymisierten Daten vermeiden oder zumindest begrenzen wollen. Solche Maßnahmen sind bspw die automatisierte Löschung von Logfiles nach einem bestimmten Zeitraum, und zwar sowohl auf Seiten des Websitebetreibers als auch auf Seiten des Access-Providers. Die gezielte Löschung ist wirkungslos, wenn der schutzwürdige Personenbezug aller bisher angefallenen Daten bei jeder zukünftigen Verbindungsaufnahme wiederhergestellt werden kann.

Die *BenutzerID* ist serverseitig dauerhaft gespeichert und daher gibt es iSv Art 4 Z 1,2 eine Verarbeitung von personenbezogenen Daten durch einen Verantwortlichen. Diese Erkenntnis ist insofern bemerkenswert, weil sie das faktische Durchführen eines *trackings* im Sinne eines serverseitig persistierten Besucherprofils oder anderer serverseitig gespeicherten benutzerspezifischen Daten, welche einzeln auf ihren Personenbezug untersucht werden müssen, gar nicht voraussetzt.

Die oftmals in der Literatur vertretene Ansicht, dass Cookies nur in Verbindung mit der serverseitigen Speicherung der IP Adresse einen Personenbezug herstellen[81], muss daher ergänzt werden: Aufgrund der unvermeidbaren wiederkehrenden Verknüpfung zwischen Cookie und IP Adresse, wie es bei persistenten Cookies mit einer gespeicherten *BenutzerID* ausnahmslos der Fall ist, ist immer (!) Personenbezug gegeben. Denn: Die *BenutzerID* ist ein Pseudonym für die IP Adresse - Die IP Adresse ist ein Pseudonym für den Benutzer[82]. Diese Argumentationskette soll in weiterer Folge als **„Theorie über die Verkettung der pseudonymisierten IP Adresse“** referenziert werden.

[78] Jedenfalls im TCP/IP Protokollstack.
[79] Der Websitebetreiber hat keinen Einfluss auf die Wiederkehr des Benutzers – diese „droht“ daher ständig und aufgrund des gezielten Vorhalten des serverseitigen *BenutzerID* „rechnet“ der Websitebetreiber schließlich auch mit dem Wiederbesuch.
[80] Vgl *Dammann* in *Simitis* BDSG § 3 Rn 217b & 220d.
[81] Stellvertretend: *Spindler/Nink* in *Spindler/Schuster* (Hrsg), Recht der elektronischen Medien³ (2015) TMG § 11 Rn 21.
[82] *Schleipfer,* ZD 2015, 399 (401).

Den Personenbezug eines Cookie mit eindeutiger *BenutzerID* erkennen auch Betreiber von Werbeplattformen (AdNetworks) vermehrt an, obwohl diese Dienste - laut eigener Aussage - IP Adressen teilweise nur in verkürzter Form speichern[83].

Andere Meinungen in der Literatur, die einen inhärenten Personenbezug der Cookie *BenutzerID* ablehnen oder den Personenbezug dieses Datums nur in Verbindung mit anderen, serverseitig gespeicherten Informationen bejahen[84], sind im Lichte der *Breyer* Entscheidung nicht aufrechtzuerhalten. Fehlt es hingegen am Personenbezug, ist das allgemeine Datenschutzrecht für Cookies nicht einschlägig[85].

3.2.3 Anwendungsbereich beim Einsatz von *device fingerprinting*

An dieser Stelle soll untersucht werden, ob der Einsatz der *device fingerprinting* Technologie serverseitig notwendigerweise mit einer Verarbeitung von personenbezogenen Daten verbunden ist. Im Gegensatz zur Cookie Technologie werden hier clientseitig keine Daten gespeichert - wie beim Cookie gibt es auch hier zunächst nirgendwo eine Zuordnungstabelle zwischen einer bestimmten natürlichen Person und ihres *device fingerprints*[86]. Fraglich ist daher wiederum die Auslegung des Kriteriums der Bestimmbarkeit. Für die weitere Betrachtung soll vorerst zunächst die IP Adresse nicht als Erkennungsattribut mitgeführt werden. Außerdem ist die Analyse zunächst auf den Akt der Wiedererkennung selbst und nicht auf damit verbundene Anwendungsfälle wie zB die Erstellung von Benutzerprofilen (*tracking*) beschränkt.

Ähnlich wie bei Cookies wird streng genommen nur eine Referenz auf das Endgerät des Benutzers hergestellt. Aufgrund der willentlichen Benutzung des Endgeräts durch die Person und einer wie immer gearteten, faktischen und daher potentiell erkennbaren Beziehung zwischen Benutzer und Endgerät bzw zum familiären oder beruflichen Umfeld des Benutzers genügt die Betrachtung des Endgeräts, um einen potentiellen Personenbezug zu bejahen.

Beim *device fingerprinting* wird serverseitig ebenfalls ein Identifier, eine „ID“ erzeugt. Diese ID ist eine Abbildung einer bestimmten Kombination aus Informationselementen, die als kennzeichnende Elemente des Endgeräts des Benutzers zusammengeführt werden. Wie gezeigt ist diese ID per definitionem nur eingeschränkt eindeutig und schon gar nicht eineindeutig. Fehlende Eindeutigkeit führt dazu, dass die ID nicht als Pseudonym für die IP Adresse des Benutzers angesehen werden kann. Theoretisch gibt es beliebig viele Benutzer mit ein und derselben ID – es gibt keine Einschränkung auf eine spezifische Gruppe von

[83] Hier die entsprechende Stellungnahme des Unternehmens: <www.criteo.com/insights/gdpr-need-know-criteo>.
[84] So ausdrücklich: *Heckmann* in *Heckmann* (Hrsg), JurisPK-Internetrecht (2017) Kapitel 9 Rn 131; im Ergebnis ebenfalls: *Spindler/Nink* in *Spindler/Schuster* TMG § 11 Rn 11; *Schmitz* in *Hoeren/Sieber/Holznagel* (Hrsg), Handbuch Multimedia-Recht[46] (2018) Teil 16 Rn 117; *Riesz* in *Riesz/Schilchegger* TKG § 96 Rn 27 f; *Hoeren* in *Kilian/Heussen* (Hrsg), Computerrechts-Handbuch[34] (2018) Teil 14 Kapitel VI Rn 20; andere Ansicht: *Art-29-Datenschutzgruppe*, WP148, 9; *Schmidtmann/Schwierig*, Datenschutzrechtliche Rahmenbedingungen bei Smart-TV, ZD 2014, 448 (453).
[85] *Hoeren* in *Kilian/Heussen,* Teil 14 Kapitel VI Rn 21.
[86] *Alich/Voigt,* CR2012, 344 (346).

Benutzern, bspw diejenigen, die in einem gemeinsamen Haushalt leben. Die Anwendung der *Theorie über die die Verkettung der pseudonymisierten IP Adresse* führt daher hier zu einer Ablehnung des inhärenten Personenbezugs der *fingerprinting* Technologie. Eine jederzeit gültige, ausreichend treffsichere und sich selbstständig aktualisierende Zuordnung zwischen *device fingerprinting* ID und IP Adresse des Benutzers gibt es nicht.

Die *Art-29-Datenschutzgruppe* äußert sich in einer eigenen Opinion zum *device fingerprinting:* Danach soll die Kombination der kennzeichnenden Elemente jedenfalls dann einen Personenbezug haben, wenn diese für den Zweck gesammelt werden, Benutzer Website-übergreifend und über einen bestimmten Zeitraum hinweg zu erkennen[87]. Diese Beschreibung entspricht dem klassischen Anwendungsfall des *tracking*.
Lässt man den Zweck der Sammlung jedoch außen vor und konzentriert sich zunächst nur auf die technischen Aspekte von Identifikation und Wiedererkennung, dann ist zu fragen: Ist die Kombination der kennzeichnenden Elemente für sich alleine bereits ein aussagekräftiges „Profil", welches zumindest ein Teilabbild der Persönlichkeit des Benutzers ist und in wiederkehrender und wiedererkennbarer Art und Weise dem Websitebetreiber mitgeteilt wird?[88]. Die einzelnen Informationselemente, zB die Bildschirmauflösung oder die lokale Spracheinstellung, sind für sich alleine betrachtet jedenfalls keine personenbezogenen Daten[89]. Einige Informationselemente (zB die Spracheinstellung) lassen zwar einen schwach ausgeprägten Schluss auf einzelne Vorlieben des Benutzers zu, haben aber wiederum einen zu geringen Individualisierungsgrad gegenüber anderen Benutzern. Der Großteil der Elemente ist jedenfalls rein technischer Natur und beschreibt das Endgerät, aber nicht die Person des Nutzers. Die Kombination der Elemente hat daher jedenfalls solange keine Aussagekraft über die Persönlichkeit des Nutzers, als diese Kombination nicht ausreichend individuell ist, um einen ausreichend eindeutigen Rückschluss auf die Person zu ermöglichen.
Ist dieser Individualisierungsgrad hingegen erreicht, so wird von *Karg/Kühn* ein Personenbezug bejaht[90]. Dies sei unabhängig davon, ob es eine konkrete Möglichkeit für die tatsächliche Bestimmung der realen Person - im Sinne ihrer tatsächlichen Identität - gibt. Einen ähnlichen Ansatz versucht auch *Pachinger* aus der Intention der Richtlinie 2009/136/EG sowie einzelner Stellungnahmen der *Art-29-Datenschutzgruppe*[91] abzuleiten: Nämlich dass eine erfolgte Individualisierung und eine daraus abgeleitete unterschiedliche Behandlung von Internetbenutzern ausreichend sei, um den Anwendungsbereich des Datenschutzrechts zu eröffnen[92]. Die Motivation dieser argumentativen Bemühungen ergibt sich daraus, dass diese Autoren eine persönlichkeitsrechtliche Schutzlücke glauben erkannt

[87] *Art-29-Datenschutzgruppe,* WP224, 4.
[88] *Spindler/Nink* in *Spindler/Schuster* TMG § 15 Rn 9.
[89] *Karg/Kühn,* ZD 2014, 285 (288).
[90] AaO.
[91] Vgl *Art-29-Datenschutzgruppe*, WP171, Kapitel 3.2.2.
[92] *Pachinger,* Achtung Cookies – Verpflichtung zur Einwilligung beim Online-Targeting, JusIT 2011/10, 20.

zu haben. Diese entstünde dann, wenn Nutzerprofile erstellt werden, obwohl – zumindest nach traditionellem Verständnis – keine personenbezogenen Daten verarbeitet werden[93]. Die Individualisierung alleine kann allerdings nicht ausreichend sein, um einen Datensatz als personenbezogen einzuordnen. Selbst die *Art-29-Datenschutzgruppe* klassifiziert individualisierte, pseudonymisierte, personenbezogene Datensätze ohne faktische Möglichkeit zur De-Pseudonymisierung als „may not be subject to the data privacy directive“[94]. Ein Mittelding zwischen personenbezogenen Daten und nicht personenbezogenen Daten - zB das Konzept der *potentiell personenbezogenen Daten*[95] - ist aber abzulehnen. Zusätzlich problematisch ist beim Ansatz von *Pachinger* und *Karg/Kühn*, dass der mögliche Personenbezug eines Datensatzes davon abhängig gemacht wird, zu welchen Zwecken die Daten verarbeitet werden[96]. Diese Verknüpfung findet allerdings keine Stütze in den Gesetzestexten, namentlich Art 4 Z 1 DSGVO[97] und in den einschlägigen Vorgängerregelungen in BDSG, DSG 2000 und der Richtlinie 95/46/EG[98]: Die B*estimmbarkeit* der Person ist ein unbedingtes, isoliertes Tatbestandsmerkmal. Die im DSGVO Gesetzestext nachfolgende Aufzählung von „*Kennungen* (...) und *besonderen Merkmalen*“ muss aufgrund des vorangestellten Wortes *insbesondere* dahingehend interpretiert werden, dass die genannten Kennungen die Bestimmbarkeit zwar ermöglichen können, aber alleine deren Zuordnung nicht genügen kann. Es gilt weiterhin: Einzelangaben, die sich auf eine einzelne Person beziehen, sind dann keine personenbezogenen Daten, wenn die Person nicht identifizierbar (=bestimmbar) ist[99]. Auch in der *Breyer* Entscheidung konzentriert sich der EuGH auf die Möglichkeiten der Zuordnung eines individualisierten, pseudonymisierten Datensatzes zu einer realen, benennbaren Person. Noch deutlicher ist hier § 1 DSG 2018: Der Betroffene hat kein schutzwürdiges Interesse an der Geheimhaltung von (vermeintlich personenbezogenen) Daten, wenn eine Rückführbarkeit auf den Betroffenen nicht möglich ist. **Die Individualisierung ist demnach eine notwendige, aber keine hinreichende Bedingung für die Annahme des Personenbezugs.**

Das Prinzip des Verbots mit Erlaubnisvorbehalt spricht außerdem für eine isolierte Beurteilung der materiellen Tatbestandsebene (*personenbezogene Daten*) von der Prüfung einer *zweckbezogenen* Rechtfertigung in der *anschließenden* Zulässigkeitsprüfung (Art 6 DSGVO) und damit gegen eine Differenzierung des Kriteriums des Personenbezugs unter Bezugnahme auf den jeweiligen Verarbeitungszweck.

[93] *Dieterich,* Canvas Fingerprinting - Rechtliche Anford. an neue Methoden der Nutzerprofilerstellung, ZD 2015, 199 (203).
[94] *Art-29-Datenschutzgruppe,* WP136, 18; *Dammann* in *Simitis* BDSG § 3 Rn 219a.
[95] Vgl zu diesem Konzept: *Dammann* in *Simitis* BDSG § 3 Rn 36.
[96] *Karg,* Die Rechtsfigur des personenbezogenen Datums - Ein Anachronismus des Datenschutzes?, ZD 2012, 255.
[97] Vgl dazu auch ErwGr 30, 38, 75.
[98] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr, Abl L 1995/281, 31.
[99] *Gola/Klug/Körffer* in *Gola/Schomerus* (Hrsg), Kommentar Bundesdatenschutzgesetz[12] (2015) § 3 Rn 3; *Härting,* NJW 2013, 2065 (2066).

In der Literatur wird daher überwiegend vertreten, dass ein Personenbezug des *device fingerprints* nur dann gegeben ist, wenn der Websitebetreiber über ein personenbezogenes Zusatzwissen verfügt bzw vernünftigerweise verfügen könnte, das die Bestimmbarkeit der Person letztlich ermöglicht[100]. Einen inhärenten Personenbezug der *device fingerprint* ID gäbe es demnach nicht. Nachdem oben bereits aufgrund fehlender Eindeutigkeit die Tauglichkeit der *device fingerprint* ID als Pseudoynm für die IP Adresse abgelehnt wurde, kann dieser Literaturansicht hier zugestimmt werden. Ein geeignetes Zusatzwissen könnte zwar sehr wohl die im Klartext vorhandene, ungekürzte IP Adresse des Benutzers sein, aber nur wenn sie zusätzlich zur *device fingerprint* ID beim Besuch des Benutzers serverseitig gezielt abgespeichert wird – diese Variante soll im Zuge dieser Arbeit als Anwendungsfall noch näher untersucht werden.

Im Ergebnis entstehen daher durch den Einsatz von *device fingerprints* als technische Methode zur Identifikation und Wiedererkennung nicht notwendigerweise personenbezogene Daten. Alleine aus Sicht der technologischen Realisierung, vorbehaltlich der Betrachtung etwaiger zusätzlicher Daten, die sich aus dem konkreten Anwendungsfall ergeben können, ist der sachliche Anwendungsbereich der DSGVO für diese Technologie daher nicht eröffnet.

3.2.4 Anwendungsbereich bei der Identifikation mithilfe des ISP (*MSISDN Forwarding*)

Der entscheidende Unterschied zu den zuvor genannten Technologien ist in datenschutzrechtlicher Hinsicht nun der Umstand, dass beim Akt von Identifikation und Wiedererkennung der Internetprovider des Benutzers (Access-Provider), hier im konkreten Fall der Mobilfunkprovider[101], aktiv eingebunden ist.

Beim *MSISDN forwarding* wird zum Zweck der Identifikation die MSISDN des Benutzers entweder im Klartext oder in pseudonymisierter Form an den Websitebetreiber übermittelt – und zwar direkt beim Aufbau der Kommunikationsverbindung durch Injizieren im sogenannten *HTTP header*. Die MSISDN ist die Telefonnummer des Benutzers und als solche für jedermann als personenbezogenes Datum zu klassifizieren. Das Pseudonym ist jedenfalls für den Access-Provider ein personenbezogenes Datum, denn dieser kann jederzeit in seinem internen Verrechnungssystemen die Verbindung zu den tatsächlichen Stammdaten des Benutzers (genauer: des Teilnehmers) herstellen[102]. Spätestens bei der Zusammenführung von MSISDN bzw Pseudonym mit den tatsächlichen Stammdaten des Benutzers durch die Abfrage der Kundendatenverwaltung des Access-Providers (zB zum Zwecke der Verrechnung einer Drittleistung), findet auch eine *Verarbeitung* von personenbezogenen Daten iSv Art 4 Z 1,2 DSGVO statt. Alleine die *mögliche* Auflösung des

[100] *Alich/Voigt,* CR2012, 344 (346); *Heckmann* in *Heckmann,* Internetrecht, Kapitel 9 Rn 149; *Maisch,* Der Browser Fingerprint als personenbezogenes Datum im Telemedienrecht?, JurisAnwZert ITR 5/2010, Anm 3; Nicht zutreffend hingegen, weil keine Differenzierung hinsichtlich Speicherung der IP Adresse: *Dammann* in *Simitis* BDSG § 3 Rn 65.

[101] Die hier untersuchte technische Identifikationsmethode ist auch bei einem Festnetz-Internetprovider technisch möglich, wird aber – soweit dem Autor durch Recherchen bekannt – derzeit im Festnetzbereich als standardisierte Technologie nicht eingesetzt. Für den Fortgang in dieser Arbeit werden daher die technischen Begriffe aus dem Mobilfunkbereich verwendet.

[102] *Lust* in *Riesz/Schilchegger* TKG § 3 Rn 47.

Pseudonyms durch den Access-Provider erfüllt somit schon das Kriterium der *Bestimmbarkeit.* Jede *vorgelagerte* Verarbeitung des Pseudonyms auf Seiten des Access-Providers ist daher ebenfalls eine Verarbeitung von personenbezogenen Daten und daher ist auch für die initiale Erstellung des Pseudonyms eine Zulässigkeitsprüfung nach geltendem Datenschutzrecht durchzuführen. Ob dies auch für die Verarbeitungsschritte auf Seiten des Websitebetreibers uneingeschränkt gilt, soll in der Folge auf der Ebene des jeweiligen Anwendungsfalls untersucht werden.

3.3 Telekommunikationsgesetz 2003

3.3.1 Allgemeiner, sachlicher und räumlicher Anwendungsbereich TKG

Das Sonderdatenschutzrecht des TKG 2003 (§ 92 ff TKG) ist in seiner Gesamtheit nur auf Betreiber von öffentlichen Kommunikationsnetzen und –diensten anwendbar. Dies ist hier unstrittig der Access-Provider des Internetbenutzers, zB sein Mobilfunkanbieter.

Für den Anbieter eines Dienstes der Informationsgesellschaft, der keinen Kommunikationsdienst iSd TKG anbietet, gibt es lediglich vereinzelte Bestimmungen, zB § 96 Abs 3 TKG[103]. Im Zuge der Diskussion über sogenannte Over-The-Top Services wird erwogen, den Anwendungsbereich des TKG auf Dienstanbieter auszudehnen, die die Übertragung von Signalen über Kommunikationsnetze (§ 3 Z 9 TKG) „qualifiziert veranlassen“[104]. Selbst die Befürworter dieser Argumentation schränken den Erweiterungsbedarf jedoch auf Dienste ein, die eine zentrale Vermittlungsfunktion von Nachrichten bereitstellen (zB Email, WhatsApp). Dies ist bei dem hier untersuchten Websitebetreiber annahmegemäß nicht der Fall – als Dienst der Informationsgesellschaft verarbeitet er demnach auch nicht die spezifischen Datenklassen iSv § 92 Abs 3 TKG (Stammdaten, Verkehrsdaten, Inhaltsdaten, etc.)[105]. Somit ist für den Websitebetreiber der Großteil der spezifischen TKG Datenschutznormen (zB §§ 99, 101 TKG) unanwendbar.

3.3.2 Anwendungsbereich beim Einsatz von *HTTP Cookies*

Für den Websitebetreiber als Anbieter eines Dienstes der Informationsgesellschaft, der auf seiner Website Cookies einsetzt, kommt zunächst die direkte Anwendbarkeit von § 96 Abs 3 TKG in Frage. Mit Bezug auf den Problemaufriss dieser Arbeit bleiben die Sätze 4,5,6 der Vorschrift außerhalb der Betrachtung, denn sie adressieren ein anderes Regelungsziel innerhalb des EU-Einheitsrechtsrahmens zur Telekomunikation.

[103] *Riesz* in *Riesz/Schilchegger* TKG § 92 Rn 19.

[104] *Kühling/Schall,* E-Mail-Dienste sind Telekommunikationsdienste iSd TKG*,* CR 2016, 173; In der Entscheidung VG Köln 11.11.2015, 21 K 450/15 = MMR 2016, 14 wurde mit ähnlicher Argumentation der Dienst *Gmail* als Telekommunikationsdienst qualifiziert. In weiterer Folge wurde vom OVG Nordrhein-Westfalen 26.02.2018, 13 A 17/16 = MMR 2018, 552 (*Schubert*) ein Vorabentscheidungsverfahren (EuGH C-193/18) zu dieser Frage eingeleitet.

[105] *Jahnel,* Datenschutz im Internet - Rechtsgrundlagen, Cookies und Web-Logs, ecolex 2001, 84.

Durch den Einsatz von Cookies werden jedenfalls gemäß § 96 Abs 3 Satz 1 TKG Daten verarbeitet und übermittelt – und zwar sowohl serverseitig als auch clientseitig. Satz 1 schränkt allerdings die Anwendung der gesamten Vorschrift auf personenbezogene Daten ein. Im Hinblick auf *HTTP Cookies* fallen daher nach obiger Analyse *SessionID* Cookies sowie teilweise auch *non-ID Cookies*[106] aus dem sachlichen Anwendungsbereich der Vorschrift. Für Cookies bei denen eine *BenutzerID* serverseitig und clientseitig gespeichert wird, ist hingegen neben Satz 1 auch Satz 2 unproblematisch anwendbar. Dies zum einen, weil ein „Ermitteln" dieser Daten innerhalb der gesamten, zweiseitigen Verarbeitungskette (Setzen, Auslesen, Löschen) eines *HTTP Cookies* notwendigerweise vorkommt, zum anderen, weil die wörtliche Einschränkung auf die „Ermittlung" in Satz 2 sowohl systematisch-teleologisch als auch in richtlinienkonformer Auslegung abzulehnen ist[107]. Satz 3 wiederum kodifiziert eine Ausnahme des generellen Verbots der Verarbeitung und somit eine Ausnahme von der generellen Einwilligungspflicht (Satz 2)[108]. Unter diese Ausnahme kann problemlos die Übertragung der IP Adresse des Endgeräts an den Websitebetreiber im Zuge der eigentlichen Kommunikationsverbindung subsumiert werden. Eine Speicherung der IP Adresse auf Seiten des Websitebetreibers erscheint allerdings alleine aus dieser Ausnahme heraus auf den ersten Blick nicht gerechtfertigt. Für die Verwendung von Cookies mit gespeicherter *BenutzerID* gibt es aufgrund des inhärenten Personenbezugs im Zuge ihrer Verarbeitung zunächst keinen augenfälligen Ausschluss vom Anwendungsbereich von § 96 Abs 3 TKG.

Für die weitere Analyse muss allerdings der europarechtliche Bezug der Vorschrift herangezogen werden. Die Regelung ist das Ergebnis der nationalen Umsetzung von Art 5 Abs 3 der Richtlinie 2009/136/EG. Problematisch ist hier, dass die nationale Umsetzung in mehreren Elementen von der Vorgabe der Richtlinie abweicht:

Der sachliche Anwendungsbereich von Art 5 Abs 3 RL 2009/136/EG ist dem Wortlaut nach nicht auf personenbezogene Daten beschränkt, sondern auf „Informationen". Im Unterschied zur TKG Implementierung sollen allerdings nur Informationen erfasst sein, die auf dem Endgerät des Benutzers gespeichert sind. Letzteres trifft für Cookies unstrittig zu, sodass die Auflösung dieses Konflikts hier unterbleiben kann. Fraglich bleibt danach aber noch das Erfordernis des Personenbezugs. Dazu wörtlich die *Art-29-Datenschutzgruppe*: „Article 5(3) is applicable independently of whether the information stored or accessed in the user's terminal equipment consists personal data or not"[109]. Diese Interpretation stützt sich maßgeblich darauf, dass nach der Unterüberschrift von Artikel 5 und erst recht nach der Bezeichnung der gesamten Richtlinie auch das Schutzziel des Kommunikationsgeheimnisses iSv Art 7 GRC realisiert werden soll und eine Einschränkung

[106] Die Differenzierung nach einem etwaigen Personenbezug von *non-ID Cookies* erfolgt in Kapitel 4.3 dieser Arbeit.
[107] so auch: *Riesz* in *Riesz/Schilchegger* TKG § 96 Rn 8;aA *Geuer/Reinisch*, MR 2018, 123 (134).
[108] AaO Rn 45.
[109] *Art-29-Datenschutzgruppe*, WP188, 8.

von eben jenem nur auf personenbezogene Daten unzulässig ist[110]. Art 5 Abs 3 adressiert dieses Schutzbedürfnis über eine ähnliche Konstruktion wie die Rechtsfortbildung „zum Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme“[111] . Gegenstand dieser Rechtsfortbildung war das Schließen einer Schutzlücke, die verhindert, dass unberechtigte Dritte „Leistungen, Funktionen und Speicherinhalte des Informationssystems nutzen“ - Dies allerdings auch nur dann, wenn dieses System zumindest „persönlichkeitsrelevant“ ist, dh wenn jemand das System als „sein eigenes“ nutzt und daher mit einer hohen Wahrscheinlichkeit Daten vorhanden sind, die zum persönlichen Lebensbereich zu zählen sind[112].

Für eine begriffliche Reduktion auf personenbezogene Daten von Art 5 Abs 3 der Richtlinie spricht wiederum die direkte textuelle Erwähnung der Datenschutzrichtlinie 95/46/EG. Dazu kommt, dass eine Ausdehnung auf alle Informationen, die im Endgerät gespeichert sind oder gespeichert werden, nicht sachgerecht sein kann - **Die schützenswerten Informationen müssen irgendeinen persönlichen Bezug zum Nutzer haben, damit ein Eingriff in die Privatsphäre iSv Art 8 EMRK[113] denkmöglich ist**. Ohne einen solchen Eingriff gibt es keine Rechtfertigung für die Existenz der fraglichen Schutzregelung. Ein Eingriff wäre beim Zugriff auf gespeicherten Kamerafotos oder dem Telefonbuch des Nutzers sicher zu bejahen, aber bei maschinengenerierten Daten, die durch das Ablaufen der Software notwendigerweise entstehen und tw auch gespeichert werden, zu verneinen**. Es erscheint daher zulässig, den in der Richtlinie verwendeten Begriff der „Information“ auf Daten zu reduzieren, die in ihrer semantischen Bedeutung einen Bezug auf die Persönlichkeit des Nutzers herstellen**. Dies kann auch über den Umweg seines Endgeräts passieren, nämlich wenn er eine *ausreichend konkrete* Individualisierung – zB durch eine spezifische Kombination von Konfigurationsoptionen oder die Historie der von ihm besuchten Webseiten - seines Endgeräts vorgenommen hat, sodass diese Individualisierung für sich selbst bereits wieder einen Bezug auf die Persönlichkeit des Nutzers herstellt. Die hier befürwortete Auslegung von „Information“ umfasst auch den explizit adressierten Schutzbereich von ErwGr 65,66 der Richtlinie – hier soll der Benutzer vor Spyware und Schadprogrammen geschützt werden: Eine Überwachung des Benutzers oder ein Unbrauchbarmachen seines Datenbestandes ist jedenfalls ein Eingriff in die Privatsphäre[114].

Mit der in dieser Arbeit vertretenen extensiven Auslegung des Begriffs *personenbezogene Daten* - insbesondere auch mit deren Wechselwirkung zwischen Benutzer und „seinem“ Endgerät - ist jedoch zwischen der nationalen Umsetzung im TKG und der Auslegung des Begriffs „Information“ in der Richtlinienvorgabe kein substanzieller Unterschied mehr erkennbar. Zumindest nicht in dem Umfang, welcher eine Abkehr von dem Wortlaut des TKG

[110] So auch *Alich/Voigt,* CR 2012, 344 (345).
[111] BVerfG 27.2.2008 , 1 BvR 370/07 = MMR 2008, 315 (*Bär*) = JA 2008, 475 (*Kudlich*).
[112] *Kutscha,* Mehr Schutz von Computerdaten durch ein neues Grundrecht, NJW 2008, 1042 (1043).
[113] Vgl Art 1 Abs 3 RL 2009/136/EG sowie ErwGr 3 der Vorgängerrichtlinie 2002/58/EG.
[114] Vgl Fußnote 111.

als unmittelbar anwendbares Gesetz rechtfertigen könnte[115]. Eine Festlegung, ob Art 5 Abs 3 der Richtlinie auf personenbezogene Daten einzuschränken ist[116], braucht an dieser Stelle daher nicht zu erfolgen[117].

Der detaillierten Analyse des Einwilligungserfordernisses, konkret bezogen auf unterschiedliche Anwendungsfälle in Kapitel 4.3 dieser Arbeit, soll hier nicht vorgegriffen werden. Auf der Ebene der Gesetzesauslegung fehlt allerdings noch ein Maßstab für die Beurteilung, ob die Verarbeitung von personenbezogenen Daten *unbedingt erforderlich ist um den angeforderten Dienst für den Benutzer zu erbringen* (§ 96 Abs 3 Satz 3 TKG) – diese Erforderlichkeit führt letztendlich zu einer Ablehnung des Einwilligungserfordernisses und ist daher maßgeblich für die Beurteilung der einzelnen Anwendungsfälle. Die Ausnahmebestimmung vom generellen Einwilligungsvorbehalt ist wörtlich aus der Richtlinie übernommen. Auf deren Basis hat die Art-*29-Datenschutzgruppe* eine umfassende Analyse publiziert, zu welchem Zweck und in welcher Form Cookies von dem Einwilligungserfordernis ausgenommen sein sollen. Dazu wurden 7 Kategorien von Cookies als Ausnahme zum Einwilligungserfordernis sowie 3 Kategorien von Cookies mit aufrechtem Einwilligungserfordernis ausgearbeitet[118]. Die Einteilung erfolgte hinsichtlich der Verarbeitungszwecke des Cookies. Ein Abgleich mit den hier gefundenen Ergebnissen, die ausschließlich auf die technische Minimalimplementierung und den damit verbundenen Personenbezug der Daten abstellen, bietet sich für eine Positionsbestimmung zur „unbedingten Erforderlichkeit der Verarbeitung“ an - soll aber der detaillierten Analyse der Anwendungsfälle in den späteren Kapiteln nur indikativ vorgreifen:

- Alle von der *Art-29-Datenschutzgruppe* gelisteten *Session Cookies* erfordern keine Einwilligung → Übereinstimmung zum hier gefundenen Ergebnis, da kein Personenbezug der Cookie Daten.
- persistent gespeicherte *non-ID Cookies* werden von der *Art-29-Datenschutzgruppe* in Kapitel 3.6 als „nicht unbedingt erforderlich“ und daher als einwilligungspflichtig beurteilt. Die Begründung: *Non-ID Cookies* sind eine Komfortfunktion für den Benutzer und nicht unbedingt für die Erbringung des angeforderten Dienstes notwendig[119] → tw Abweichung zum hier gefunden Ergebnis, falls Personenbezug

[115] *Riesz* in *Riesz/Schilchegger* TKG § 96 Rn 16-25 (unter anderem auch mit dem Argument der europarechtlichen Mindestharmonisierung); zur Möglichkeit der richtlinienkonformen Rechtsfortbildung von RL 2009/136/EG auf Grundlage des TMG: *Schmitz* in *Hoeren/Sieber/Holznagel* Teil 16 Rn 277; *Moos,* Unmittelbare Anwendbarkeit der Cookie-Richtlinie - Mythos oder Wirklichkeit?, K&R 2012, 637. Vgl generell zur Grenze der richtlinienkonformen Auslegung: EuGH 4.7.2006, C-212/04 (*Adeneler uA*).

[116] Stellvertretend für diese Einschränkung: *Jahnel*, Spamming, Cookies, Logfiles und Location Based Services im TKG 2003, ÖJZ 9/2004, 336 Kapitel C.1. Für diese Einschränkung spricht auch der Rechtsvergleich mit Deutschland, wo eine inhaltlich mit dem öTKG vergleichbare Regelung (nämlich § 15 TMG) in genau diesem Aspekt als Richtlinienkonform eingestuft wurde (Quelle: <www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html>). Die hM spricht sich allerdings gegen diese Einschränkung aus: *Schirmbacher,* Online-Marketing und Social-Media-Recht² (2017) Kapitel 6.1; *Art-29-Datenschutzgruppe,* WP171, 10; *Dieterich,* ZD 2015, 199 (200).

[117] Ein EuGH Vorabentscheidungsverfahren zu dieser Fragestellung ist unter C-673/17 (*Planet 49*) anhängig.

[118] *Art-29-Datenschutzgruppe*, WP194, Kapitel 3 & 4.

[119] Aus den Erläuterungen zur dieser Begründung geht hervor, dass die *Art-29-Datenschutzgruppe* hier eine Ausnahme von der Ausnahme vermeiden wollte und diese Art von Cookies als minimalinvasiv einschätzt, vgl aaO.

der Cookie Daten abgelehnt wird. Diese Abweichung wird in Kapitel 4.3 noch einmal thematisiert.

- *BenutzerID* basierte Cookies werden von der *Art-29-Datenschutzgruppe* fast ausschließlich als einwilligungspflichtig klassifiziert und dieses Ergebnis entspricht daher in einem großem Umfang der hier aufgestellten, abstrakt-generellen Regel: „Wenn Personenbezug und kein unbedingtes, technisches Erfordernis der Verarbeitung, dann Einwilligungspflicht". Einzelne Abweichungen von den hier gefundenen Ergebnissen werden in Kapitel 4.3 noch einmal thematisiert.

3.3.3 Anwendungsbereich beim Einsatz von *device fingerprinting*

Unter Bezugnahme auf die Ergebnisse aus Kapitel 3.2.3 und den Wortlaut von § 96 Abs 3 Satz 1,2 TKG gibt es aufgrund des fehlenden Personenbezugs keine Anknüpfung an die Vorschrift. Dies steht wiederum im Widerspruch zu einer Stellungnahme der *Art-29-Datenschutzgruppe*, die die Technologie des *device fingerprinting* unter Art 5 Abs 3 der Richtlinie 2009/136/EG als einwilligungspflichtig klassifiziert[120]. Fraglich ist an dieser Stelle, ob das Festhalten am Wortlaut des TKG hier ebenfalls sachgerecht ist. Andernfalls könnte der Anwendungsfall *device fingerprinting* eine Indikation für eine richtlinienkonforme Ausdehnung des TKG Anwendungsbereichs liefern:

Im Gegensatz zur Cookie Technologie werden hier keine Daten auf dem Endgerät gespeichert - allerdings sehr wohl von dem Endgerät ausgelesen. Der Lesezugriff auf im Endgerät vorliegende Informationen ist in Art 5 Abs 3 RL 2009/136/EG beschrieben als „gaining access to information already stored", bzw auf deutsch: „der Zugriff auf Informationen die bereits im Endgerät (..) gespeichert sind (...) ist nur gestattet, wenn (...)". Der Wortlaut der Richtlinie lässt vermuten, dass nur der nachgelagerte Zugriff auf Informationen umfasst ist, welche zuvor auch durch einen Dienstanbieter abgespeichert wurden. ErwGr 66 spricht in demselben Zusammenhang allerdings von „bereits gespeicherten Informationen" und lässt somit den Schluss zu, den auch die *Art-29-Datenschutzgruppe* vollzieht: „*It is not correct to interpret Article 5 Abs 3 as meaning that the third-party does not require consent to access information on that device simply because he did not store it".*

Der Schutzbereich von Art 5 Abs 3, wie oben dargestellt, soll die Vertraulichkeit der Daten im Endgerät schützen. Dieser Schutzbereich kann sich nicht auf Informationen erstrecken, welche das Endgerät im Zuge einer bewusst durch den Nutzer gesetzten Handlung zum Abruf eines Informationsdienstes gegenüber dem Kommunikationsziel preisgibt. Erst recht nicht, wenn diese Informationen keinen Ansatzpunkt für eine Bestimmbarkeit der Person

[120] *Art-29-Datenschutzgruppe*, WP224, 7 f.

liefern. „Gaining information“[121] deutet auf einen aktiven Prozess des Dienstanbieters hin, der gezielt das Auslesen von Informationen aus dem Endgerät anstößt. Aber genau dies ist beim *passive fingerprinting* nicht der Fall, wonach dieses daher auch im Hinblick auf die Richtlinie 2009/136/EG kein Einwilligungserfordernis begründet.

Auf den ersten Blick problematischer erscheint allerdings das *active fingerprinting,* da hier der Dienstanbieter praktisch gezielt „Spähsoftware“ einsetzt, um Informationen aus dem Benutzerendgerät auszulesen. Da diese Spähsoftware allerdings letztendlich nur in der Umgebung des Webbrowsers abläuft und auch nur im Moment der durch den Benutzer verursachten Übertragung der Webinhalte aktiv ist, ist eine Abgrenzung zum *passive fingerprinting* im Hinblick auf Telos und Wortlaut der Richtlinie nicht leicht herstellbar. Außerdem bleibt es dabei, dass die ausgelesenen, technischen Informationen iA keinen unmittelbaren Bezug zur Privatsphäre des Nutzers haben (vgl Kapitel 3.3.2). Letztlich ist also die Unsicherheit in der Auslegung von Art 5 Abs 3 der Richtlinie zu groß, um eine Abkehr vom klaren Wortlaut des TKG (*personenbezogene Daten*) zu vertreten.

Obwohl der persönliche Anwendungsbereich von § 99 TKG und § 96 Abs 1,2 TKG für den Websitebetreiber nicht eröffnet ist, liefern auch diese Vorschriften eine Stütze für obige Argumentation: Die Eingangsdaten für den *device fingerprint* werden vom Webbrowser des Nutzers erhoben bzw versendet – Eine Einordnung als Verkehrsdaten iSd EU-Einheitsrechtsrahmens bietet sich in analoger Betrachtungsweise an. Für die Einordnung als Verkehrsdaten wäre per se kein Personenbezug nötig, jedoch adressiert die Richtlinie 2009/136/EG in Art 6 ausdrücklich nur „Verkehrsdaten, die sich auf Teilnehmer und[122] Nutzer beziehen“. Dieser Schutzumfang wurde dann auch in §§ 99, 96 Abs 1,2 TKG implementiert, ohne dass die Klarstellung zur Voraussetzung eines Personenbezugs in die nationale Vorschrift Einzug gefunden hat[123]. Für Verkehrsdaten ohne Personenbezug gibt es folglich weder im TKG noch in der Richtlinie anwendbare Vorschriften.

Im Ergebnis bleibt es demnach weiterhin bei der Voraussetzung des Personenbezugs für die Anwendbarkeit von § 96 Abs 3 TKG und damit einhergehend ist der Anwendungsbereich der Vorschrift beim Einsatz der *device fingerprinting* Technologie generell nicht eröffnet.

3.3.4 Anwendungsbereich bei der Identifikation mithilfe des ISP (*MSISDN forwarding*)

Der Anwendungsfall des *Direct Carrier Billing* ist dem TKG Gesetzgeber bekannt – vgl dazu die Definition des „Drittanbieters“ in § 3 Z 4a TKG. Das Charakteristikum dieser mehrgliedrigen Definition ist dabei lit e, wodurch einerseits die notwendige Abgrenzung zu

[121] Der aktuelle Entwurf der ePrivacy VO, welche Art 5 Abs 3 RL 2009/136/EG komplett ersetzen wird, spricht in diesem Regelungszusammenhang von „Collection (...) of data“ und unterstützt somit die hier dargelegte Interpretation der aktuell gültigen Richtlinie in teleologischer Hinsicht.

[122] Das Wort „und“ sowie die Bezeichnung der beteiligten Personen erscheint ist in diesem Zusammenhang verwirrend. Für die Betrachtung an dieser Stelle genügt jedenfalls der Bezug zum „Benutzer des Endgeräts“.

[123] *Riesz* in *Riesz/Schilchegger* TKG § 99 Rn 4.

normalen Bezahlvorgängen im Internet – zB über Kreditkarte – vorgenommen wird[124] und andererseits klargestellt wird, dass der fragliche Dienst von einem Drittanbieter und nicht von dem Mobilfunkbetreiber selbst angeboten wird. Die derzeitigen Regelungen im TKG haben allerdings ausschließlich den Konsumentenschutz zum Ziel (vgl § 29 Abs 2a TKG) und gehen nicht auf eventuelle Datenschutzprobleme ein[125]. Von der in § 24 Abs 2 TKG zugewiesenen Verordnungskompetenz für die „Drittanbieterproblematik" hat die Regulierungsbehörde stand heute keinen Gebrauch gemacht. Die Regulierungsbehörde kommuniziert dahingehend – rein informell - die Möglichkeit, die Bezahlung von Drittanbieterdiensten über die Telefonrechnung beim jeweiligen Mobilfunkprovider pauschal sperren zu lassen[126]. Dies entspricht einer Opt-Out Lösung, deren datenschutzrechtliche Zulässigkeit noch zu prüfen ist.

Für den Access-Provider ist das gesamte Sonderdatenschutzrecht des TKG (§ 92 ff TKG) anzuwenden und daher muss bei der Verarbeitung personenbezogener Daten nach der jeweiligen Datenklasse unterschieden werden. Beim Einsatz von *MSISDN forwarding* findet auf Seiten des Access-Providers jedenfalls einer Verarbeitung der IP Adresse (= Verkehrsdaten[127], Zugangsdaten[128]) und eine Verarbeitung der MSISDN (=Stammdaten, Verkehrsdaten[129], Zugangsdaten[130]) statt. Wird für die Datenübermittlung eine pseudonymisierte MSISDN eingesetzt, sind jedenfalls die Regelungen für Verkehrsdaten und Zugangsdaten einschlägig. Mithilfe einer weiten Auslegung der Begriffsdefinition Stammdaten in § 92 Abs 3 Z 3 TKG, insbesondere nach dem Kriterium „personenbezug" sowie „notwendig für die Abwicklung der Rechtsbeziehung", kann auf Seiten des Access-Providers auch die pseudonymisierte MSISDN als Teil der Stammdaten aufgefasst werden.

Im Sinne einer lex specialis Beziehung zur DSGVO (vgl dazu ausführlich Kapitel 3.4) sind daher für den Access-Provider primär die spezialisierten Zulässigkeitstatbestände §§ 97, 99 TKG sowie, als allgemeinere Bestimmung, § 96 TKG heranzuziehen. Zu beachten ist, dass Zugangsdaten eine Untermenge von Verkehrsdaten sind[131].

Für den Websitebetreiber, er ist der Drittanbieter sowie Betreiber eines Dienstes der Informationsgesellschaft iSd TKG, ist wiederum nur § 96 Abs 3 TKG für die Beurteilung der Zulässigkeit der Datenverarbeitung einschlägig.

---

[124] *Lust* in *Riesz/Schilchegger* TKG § 3 Rn 51.
[125] *Lust,* VbR 2016/6, 18.
[126] Siehe Website der RTR: <www.rtr.at/de/tk/TKKS_BezahlenmitdemHandy>.
[127] *Riesz* in *Riesz/Schilchegger* TKG § 99 Rn 9.
[128] OGH 14.07.2009, 4 Ob 41/09x Gliederungspunkt 5.3.2. = MR 2009, 247 (*Daum*) = JusIT 2009/103, 206 (*Zyklan*) = ecolex 2009/421, 1072 (*Horak*) = ÖBl 2010/15, 85 (*Büchele*).
[129] Die MSISDN ist Teil des *HTTP* headers. Der *HTTP header* ist – so wie der *Email header* – als Verkehrsdatum einzustufen (vgl *Riesz* in *Riesz/Schilchegger* TKG § 101 Rn 5).
[130] Im betrachteten Anwendungsfall dient die MSISDN – ähnlich wie die IP Adresse – dazu, eine bestimmte (iA in der Vergangenheit liegende) Kommunikationsverbindung einem bestimmten Teilnehmer des Mobilfunkbetreibers, referenziert durch seine Stammdaten, zuzuordnen. Somit ergibt sich eine Subsumption der MSISDN unter der Definition der Zugangsdaten in § 92 Abs 3 Z 4a TKG. Unterstützend für diese Einordung auch der Ausschussbericht (Seite 3) zur entsprechenden TKG Novelle (184 BlgNR XXII. GP 3): „(...) Zugangsdaten, welche jenen Teil von Verkehrsdaten darstellen, die zur Identifikation eines Teilnehmers an einer Internetkommunikation notwendig sind."
[131] *Riesz* in *Riesz/Schilchegger* TKG § 99 Rn 10.

Kurz soll an dieser Stelle darauf eingegangen werden, ob *MSISDN forwarding* in der hier beschrieben Realisierung nicht einen Verstoß gegen die Netzneutralitätsbestimmungen in Art 3 TSM-VO (VO (EU) 2015/2120) darstellen könnte. Art 3 Abs 3 TSM-VO schreibt vor, dass der Access-Provider den gesamten Internetverkehr, unabhängig von den jeweils durch den Kunden abgerufenen Diensten, gleich zu behandeln hat. Insbesondere sind hier auch Ungleichbehandlungen, welche von der Auswahl des Kommunikationspartners durch den Internetbenutzer ausgelöst werden, untersagt. Beim Einsatz von *MSISDN Forwarding* wird die Manipulation des *HTTP headers* jedoch im Allgemeinen auf bestimmte Ziel-IP Adressen beschränkt - somit gibt es auf der Ebene der Datenübertragung hier eine Ungleichbehandlung des Internetverkehrs iSv Art 3 Abs 3 UAbs 1 TSM-VO. Je nach Zieladresse wird der *HTTP header* verändert oder eben nicht. Diese Ungleichbehandlung wirkt sich allerdings nicht auf die Diensterbringung aus. Insbesondere gibt es keine Diskriminierung, Beschränkung oder Störung der vom Endbenutzer abgerufenen Dienste.

Unter Art 3 Abs 3 UAbs 2,3 TSM-VO werden dann „Verkehrsmanagementmaßnahmen", sofern sie nicht durch die angeführten Ausnahmebestimmungen erlaubt sind, als unzulässig festgeschrieben. Verkehrsmanagementmaßnahmen sind manipulative Eingriffe in die Datenströme der Endnutzer die vom *best-effort*[132] Prinzip abweichen[133]. Das Injizieren von einzelnen, zusätzlichen Feldern im *HTTP header* ist für sich selbst genommen keine Maßnahme zur Steuerung des Verkehrs iSd der Servicequalität der Internetverbindung (konkret: Bandbreite, Jitter, Packet loss, Latency)[134] und wirkt sich auch nicht auf diese aus. Die Methode des *MSISDN forwarding* verursacht keine Abweichung vom *best-effort* Prinzip und ist daher keine Verkehrsmanagementmaßnahme im Sinne der TSM-VO.

Die Vorschriften zur Netzneutralität in Art 3 TSM-VO sollen auch die Netzneutralität für den jeweiligen Dienstanbieter sicherstellen[135]. Daraus lässt sich ableiten, dass der Access-Provider im Umfang seiner Privatautonomie die Funktion *MSISDN forwarding* diskriminierungsfrei an interessierte Drittanbieter – zB AdNetworks, kostenpflichtige Endkundendienste - anbieten muss. Dies sei annahmegemäß hier der Fall.

3.4 Verhältnis TKG/DSGVO mit dem Rechtsstand *vor* Inkrafttreten der ePrivacy VO

Zu klären ist nun in einem finalen Schritt das Verhältnis der unmittelbar anwendbaren Datenschutzgesetze DSGVO und § 92 ff TKG. In Deutschland wurde und wird teilweise noch vertreten, dass das Sonderdatenschutzrecht des Telemediengesetzes seit dem 25.5.2018 *vollständig* verdrängt wird[136]. Auch wenn diese strikte Sichtweise mittlerweile in der

[132] In paketvermittelnden Netzen bedeutet „best-effort", dass alle eintreffenden Pakete unverzögert weitergeleitet werden, solange im Netz noch freie Übertragungskapazität vorhanden ist.
[133] TKK 18.12.2017, R 5/17-11, 17.
[134] Vgl BEREC, Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, BoR (16) 127.
[135] TKK 18.12.2017, R 5/17-11, 14.
[136] *Roggenkamp* in *Plath* (Hrsg), DSGVO/BDSG/ TMG³ (2018) TMG Einleitung Rn 13; *Keppeler*, Was bleibt vom TMG-Datenschutz nach der DS-GVO?, MMR 2015, 779; *Keber* in *Schwartmann* (Hrsg), Praxishandbuch Medien, IT- und Urheberrecht[4] (2018) Kapitel 3.3 Rn 48; *Nebel/Richter,* Datenschutz bei Internetdiensten nach der DS-GVO, ZD 2012, 407;

deutschen Literatur eine Relativierung erlebt hat[137], so ist die Situation in Österreich von vornherein anders zu bewerten: Im Gegensatz zu den entsprechenden Regelungen in Deutschland[138] entstammt § 96 Abs 3 TKG direkt aus der Umsetzung der ePrivacy Richtlinien 2002/58/EG[139] und 2009/136/EG. Anders als im Verhältnis zu RL 95/46/EG, welche ausdrücklich aufgehoben wird, gilt daher: Art 95 DSGVO iVm ErwGr 173 zum Anwendungsvorrang muss nach dem Wortlaut[140] so interpretiert werden, dass die nationalen datenschutzrechtlichen Umsetzungen der RL 2002/58/EG[141] iA weiter Gültigkeit haben[142].

Andererseits kann an dieser Stelle schon jetzt festgehalten werden, dass ein Rückgriff auf die DSGVO für jene datenschutzrechtlichen Themen, die nicht im TKG normiert sind, unproblematisch ist. Dafür spricht in aller Klarheit § 92 Abs 1 Satz 2 TKG, der in der aktuellen Fassung BGBl I 29/2018 die subsidiäre Gültigkeit des DSG 2000 anordnet und seit dem 25.5.2018 somit sinngemäß auf die DSGVO verweist. Seit der Umsetzung der ePrivacy Richtlinie 2009/136/EG Art 5 Abs 3 in nationale Gesetze wurde immer wieder kritisiert, dass die Richtlinie keine Vorgaben zur konkreten Ausgestaltung der Einwilligung (zB Opt-in vs. Opt-Out, ausdrücklich vs. konkludent) macht und es daher zu vielen unterschiedlichen nationalen Umsetzungen kam. Dies erweist sich im Hinblick auf die Situation in Österreich nun als Vorteil, denn mangels konkreter Bestimmungen im TKG wird man nun ausnahmslos die entsprechenden Vorschriften der DSGVO bezüglich den Anforderungen an eine rechtmäßige Einwilligung heranziehen müssen. Dasselbe gilt für die Ausgestaltung der Informationspflichten, die nun ebenfalls in der DSGVO konkretisiert wurden und jedenfalls für den Anbieter eines Dienstes der Informationsgesellschaft im TKG nicht genauer definiert wurden.

Aus dem Wortlaut von Art 95 DSGVO wird man unproblematisch schließen können, dass eine Datenverarbeitung im genannten Kontext, die beurteilt am Maßstab einer (richtlinienkonformen!) nationalen Umsetzung von 2002/58/EG vor dem 25.5.2018 rechtmäßig war, auch nach dem 25.5.2018 rechtmäßig ist[143]. Die Abweichung in der Umsetzung von 2002/58/EG in § 96 Abs 3 TKG ist hier weitgehend unbeachtlich, weil die DSGVO ohnehin nur auf personenbezogene Daten Anwendung findet und daher hier keine Widersprüchlichkeit entstehen kann. Allerdings wird man in § 96 Abs 3 Satz 2 TKG das Wort

---

„Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26.4.2018“ <www.datenschutz-berlin.de/pdf/publikationen/DSK/2018/2018-DSK-Positionsbestimmung_TMG.pdf>.

[137] Zusammenfassend: *Kremer,* Wer braucht warum das neue BDSG?, CR 2017, 367 (371).

[138] *Keppeler,* MMR 2015, 779 (781).

[139] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Abl L 2002/201, 37.

[140] Der Volltext dazu lautet: „Es sollen keine *zusätzlichen* Verpflichtungen auferlegt werden“.

[141] RL 2009/136/EG ist eine Änderung von RL 2002/58/EG und somit von dieser Aufzählung mitumfasst.

[142] So auch *Geuer/Reinisch*, MR 2018, 123 (123).

[143] *Kremer,* CR 2017, 370 (371).

„Ermittlung“ auf das Wort „Verarbeitung“ ausdehnen müssen – diese Interpretation war aber auch schon vor Inkrafttreten der DSGVO die hM[144].

Art 95 referenziert zwar nur auf *Betreiber von Kommunikationsdiensten* iSd TKG. Aus der allgemeinen Zielsetzung der RL 2002/58/EG und unter Einbeziehung des Hinweises in Art 21 Abs 5 DSGVO muss man aber davon ausgehen, dass eine Ausdehnung auf Dienste der Informationsgesellschaft kein Hindernis für den Ausschluss vom Anwendungsvorrang darstellen kann.

Wesentlich problematischer ist die Frage, ob man aufgrund der spezifischen und ausdrücklichen Anordnung des Einwilligungserfordernisses in § 96 Abs 3 TKG den Schluss ziehen muss, dass der Erlaubnistatbestand des berechtigten Interesses aus Art 6 Abs 1 lit f DSGVO als Rechtfertigungsgrund für die Verarbeitung von personenbezogenen Daten durch den Websitebetreiber keinesfalls in Frage kommt. Art 95 DSGVO[145] soll so interpretiert werden, dass diejenigen nationalen Umsetzungsvorschriften aus 2002/58/EG, die den Schutz von personenbezogenen Daten als Ziel haben, vom generellen Anwendungsvorrang der DSGVO ausgeschlossen sind[146]. § 96 Abs 3 TKG entstand aus der direkten Umsetzung von RL 2002/58/EG, 2009/136/EG[147] welche wiederum eine Spezialisierung des allgemeinen Einwilligungserfordernisses aus der Datenschutzrichtlinie 95/46/EG ist[148]. Es gibt keinen Hinweis darauf, dass der Unionsgesetzgeber an Ziel, Zweck und Rechtsfolge des Spezialitätsverhältnisses zwischen RL 95/46/EG und 2002/58/EG bzw 2009/136/EG im Zuge der Einführung der DSGVO etwas ändern wollte. Zur Beurteilung des Anwendungsvorrangs ist nun an dieser Stelle hilfreich, dass § 96 Abs 3 TKG auf den Geltungsbereich *personenbezogene Daten* eingeschränkt ist, denn dadurch ergibt sich die volle Überdeckung zur DSGVO und ein starkes Argument für die Verdrängung eben dieser. Problematisch ist an dieser Stelle nun allerdings die fehlende Einschränkung des TKG auf Daten, die im Endgerät gespeichert sind (vgl Richtlinie Art 5 Abs 3). Durch die Ausdehnung des sachlichen Anwendungsbereichs auf personenbezogene Daten *außerhalb* des Benutzerendgeräts erfolgte von österreichischer Seite eine überschießende Umsetzung der Richtlinie im TKG. Die Annahme eines Vorrangs des *überschießenden* Teils der Umsetzung würde dem anerkannten Rangverhältnis zwischen Unions- und nationalem Recht widersprechen[149]. **Für die Verarbeitung von personenbezogenen Daten *außerhalb* des Endgeräts ist daher**

[144] *Pachinger,* Der neue „Cookie-Paragraph“ – Erste Gedanken zur Umsetzung des Art 5 Abs 3 E-Privacy-RL in § 96 Abs 3 TKG 2003 idF BGBl I 2011/102, jusIT 2012/8, 20; *Riesz* in *Riesz/Schilchegger* TKG § 96 Rn 26; Vgl dazu auch EBRV 138 BlgNR XXIV. GP 25.

[145] Vgl auch Art 21 Abs 5 DSGVO.

[146] *Holländer* in *Brink/Wolff* (Hrsg), Beck Online-Kommentar Datenschutzrecht[24] (2018) DSGVO Art 95 Rn 5; *Feiler/Forgó*, EU-DSGVO (2016) Art 95.

[147] *Pachinger,* JusIT 2012/8, 16.

[148] *Art-29-Datenschutzgruppe*, WP187, 13.

[149] OGH 23.05.2013, 4 Ob 29/13p Gliederungspunkt 1.2.c. = ecolex 2013/335, 80 (*Tonninger*) = ZfRV-LS 2013/56 (*Ofner*) = JusIT 2013/76, 161 (*Haybäck*) = ÖBl 2013/64, 266 (*Melcher*) = MR 2013, 293 (*Heidinger*) = ZfRV 2014/25, 219 (*Cach*);Vgl Stellungnahme 29/2017 des Deutschen Anwaltvereins durch die Ausschüsse Informationsrecht und Gefahrenabwehrrecht zum ePrivacy VO Kommissionsentwurf (Berlin 2013), 7, <www.computerundrecht.de/DAV-SN_29-17.pdf>.

die angeordnete Ausnahme vom Anwendungsvorrang nur eingeschränkt gültig. Das heißt: Für eine Datenverarbeitung außerhalb des Endgeräts des Benutzers kann uU auf die Rechtfertigungsgründe der DSGVO zurückgegriffen werden. Insbesondere auf das berechtigte Interesse gemäß Art 6 Abs 1 lit f DSGVO.

Im Ergebnis ist daher davon auszugehen, dass der lex specialis Grundsatz generell weiterhin anzuwenden ist. Für eine Datenverarbeitung ohne Benutzereinwilligung bleibt daher die Beurteilung nach § 96 Abs 3 Satz 3 Halbsatz 2 TKG maßgeblich: Das *unbedingte Verarbeitungserfordernis* verursacht durch die technische Zurverfügungstellung des Dienstes auf ausdrücklichen Wunsch des Benutzers. Die Argumentation im vorangegangen Absatz öffnet (vorsichtig) ein Einfallstor für ein berechtigtes Interesse des Websitebetreibers in das strenge Einwilligungserfordernis von 96 Abs 3 TKG. Vieles spricht aber dafür, dass die Interessensabwägung iSd generellen Intention des TKG Sonderdatenschutzrechts auf technische Belange einzuengen ist. Für die Verarbeitung von personenbezogenen Daten auf dem Endgerät selbst ist ein noch strengerer Maßstab anzulegen. Ob dieses Ergebnis ohne Einschränkung in allen Anwendungsfällen sachgerecht ist, soll im Zuge dieser Arbeit noch untersucht werden.

3.5 Möglicher Lückenschluss über allgemeines Persönlichkeitsrecht

Wie bereits im Kapitel 3.2.2 bei der Analyse von Art 5 Abs 3 RL 2009/136/EG angedeutet, könnte sich bei einer alleinigen Konzentration auf das Datenschutzrecht (TKG, DSGVO) eine Schutzlücke ergeben. Dies nämlich dann, wenn sich durch eine Datenverarbeitung ein Eingriff in die Privatsphäre ergibt, obwohl keine personenbezogenen Daten verarbeitet werden[150]. Dass dies möglich sein muss, ergibt sich rechtsdogmatisch schon durch die Aufspaltung des Art 8 EMRK in die Art 7 und Art 8 GRC. Art 5 Abs 3 RL 2009/136/EG gibt in diesem Zusammenhang auch die richtigen Denkanstöße, nämlich durch die Verwendung des Begriffs *Information* anstatt des Begriffs *personenbezogene Daten*. Vor dem Hintergrund von Art 7,8 GRC und Art 8 EMRK muss es sich dabei jedenfalls um Informationen handeln, die einen persönlichen Bezug zu einer Person haben und deren Offenlegung oder Mitteilung in schutzwürdige Interessen dieser Person eingreifen. Im Gegensatz zu Art 5 Abs 3 RL 2009/136/EG ist es für den Grundrechtseingriff allerdings irrelevant, ob die Daten auf dem Endgerät gespeichert werden oder nicht.

Auch wenn in der österreichischen Literatur zur generellen Anerkennung eines allgemeinen Persönlichkeitsrechts kein Konsens besteht, so ist der Schutz der Privatsphäre im Sinne von Art 8 EMRK unter § 16 ABGB unstrittig[151]. Außerdem muss es für diese Art des Grundrechtseingriffs die Möglichkeit einer Interessensabwägung zwischen den Beteiligten geben[152].

Als Gegengewicht zur tendenziell strengen Einschränkung auf den Wortlaut des § 96 Abs 3 TKG soll daher bei der Einzelprüfung der Anwendungsfälle darauf geachtet werden, ob trotz fehlender Verarbeitung personenbezogener Daten nicht doch ein Eingriff in das Persönlichkeitsrecht des Datensubjekts stattfindet.

Das Erfordernis zur Einwilligung in so einen Eingriff kann sich daher auch außerhalb des Datenschutzrechts aus den allgemeinen Bestimmungen des Persönlichkeitsrechts § 16 ABGB bzw § 1328a ABGB ergeben. Letzteres ist die Ausführungsbestimmung von § 16 ABGB[153], steht jedoch gemäß § 1328a Abs 2 ABGB in einem Subsidiaritätsverhältnis zu den jeweils spezielleren Schutzvorschriften im Persönlichkeitsrecht. Zu diesen zählt auch das Datenschutzrecht[154], welches allerdings im Gegensatz zum ausdrücklich genannten MedG nicht vom Subsidiaritätsgrundsatz ausgeschlossen ist[155]. Zwar gilt eine Website als Medium iSd MedG, wenn allerdings die Datenverarbeitung nicht in Verbindung mit der Veröffentlichungsfunktion der Website steht, soll diese Datenverarbeitung nicht nach den

[150] *Art-29-Datenschutzgruppe,* WP136, 24; *Dieterich* ZD 2015, 199 (203).
[151] *Schmädel*, Persönlichkeitsrechte im österreichischen und deutschen Filmrecht unter besonderer Beachtung der Rechte des Filmschauspielers (2009), 27.
[152] *Koch* in *Koziol/Bydlinski/Bollenberger* (Hrsg), ABGB[5] (2017) § 16 Rn 4.
[153] *Danzl* in *Koziol/Bydlinski/Bollenberger* ABGB § 1328a Rn 2.
[154] EBRV 173 BlgNR 22. GP 19 f.
[155] *Helmich*, Schadenersatz bei Eingriffen in die Privatsphäre, ecolex 2003, 888 (890).

Grundsätzen des MedG beurteilt werden. Der subsidiäre Schutz über § 1328a ABGB steht daher prinzipiell offen.

3.6 Ausblick auf die ePrivacy VO[156]

3.6.1 Allgemeiner, sachlicher und räumlicher Anwendungsbereich Art 1,2,3 ePrivacy VO

Die ePrivacy VO setzt, wie schon die ePrivacy Richtlinie (2002/58/EG, 2009/136/EG), auf den Art 7,8 der EU Grundrechte Charta auf und wird die genannte Richtlinie komplett ersetzen. Erklärtes Ziel des Gesetzgebungsverfahrens ist es, die vielen unterschiedlichen nationalen Implementierungen der ePrivacy Richtlinie über das Rechtsinstrument der unmittelbaren Anwendbarkeit der Verordnung komplett zu harmonisieren – insbesondere auch im Hinblick auf Regelungen zu Cookies und ähnlichen Technologien[157]. Der Websitebetreiber ist als Dienst der Informationsgesellschaft namentlich als Normadressat in Art 8 Abs 1 lit c ePrivacy VO genannt. Die Anwendbarkeit für den Access-Provider ergibt sich direkt aus Art 2 - der Access-Provider ist der Bereitsteller des elektronischen Kommunikationsdienstes.

Während in Art 5 Abs 3 RL 2009/136/EG Umfang und Bedeutung des Wortes *Information* noch strittig ist (vgl Kapitel 3.3.2), bleibt in der ePrivacy VO kein Raum für diesen Streit. Mit dem Zusatz „including about its software and hardware..."[158] wird unzweifelhaft ausgedrückt, dass für den Zugriffsschutz auf Informationen, die auf dem Endgerät gespeichert sind, kein Personenbezug iSd Datenschutzrechts erforderlich ist[159]. Auch die hier vertretene Auslegung von Art 5 Abs 3 RL 2009/136/EG (siehe Kapitel 3.3.2) kann für die ePrivacy VO nicht aufrechterhalten werden: Zwar geht es weiterhin um *Informationen*, also zumindest interpretierbare Daten mit einer entsprechenden Semantik[160], allerdings ist ein ausreichendes Maß an *Individualisierung* nicht mehr erforderlich. Zu den geschützten Informationen gehören demnach nicht nur Daten, die der Benutzer selbst abspeichert (zB seine Musiksammlung), sondern bspw auch Konfigurationsdaten der Software, die der Benutzer verändert hat oder die weiterhin in ihrer Standardeinstellung vorliegen. Die aktuelle Bildschirmauflösung, auch wenn sie für eine Vielzahl von Benutzern identisch ist, wäre bereits eine derart geschützte Information und darf daher gemäß Art 8 Abs 1 ePrivacy VO

[156] Stellvertretend für jede Referenz auf die geplante Verordnung: Berücksichtigt wird primär der Entwurf der EU Kommission vom 10.1.2017. Teilweise wird der Kommissionsentwurf ergänzt durch die Änderungsvorschläge des EU Parlaments vom 23.10.2017 sowie durch Diskussionsvorschläge der eingesetzten Arbeitsgruppe „WP TELE" des EU Rates. Für die wörtliche Auslegung wird, im Gegensatz zu bereits verabschiedeten Gesetzesmaterialen, auf die englische Version des Textes referenziert.

[157] *Roßnagel* , Entwurf einer E-Privacy-Verordnung – Licht und Schatten, ZRP 2017, 33.

[158] Im Volltext von Art 8 Abs 1: „The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (...)".

[159] Vgl *Rauer/Ettig,* Rechtskonformer Einsatz von Cookies, ZD 2018, 255 (256); *Schleipfer,* Datenschutzkonformes Webtracking nach Wegfall des TMG, ZD 2017, 460 (464); Differenzierend: *Engeler*, Die ePrivacy-Verordnung zwischen Trilog und Ungewissheit, ZD 2017, 549.

[160] *Specht,* Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2016, 288 (290).

ohne technische Notwendigkeit nicht ausgelesen werden. Genauso dürfen nach dieser Vorschrift nicht ohne weiteres Daten auf dem Endgerät gespeichert werden bzw die Rechenleistung des Geräts benutzt werden.

Im Hinblick auf das Endgerät besteht somit ein zum klassischen Datenschutz komplett paralleles Schutzregime, nämlich die Umsetzung der Schutzziele aus der Informationssicherheit: *Confidentiality* und *Integrity.* Und zwar, wie oben gezeigt, unabhängig von einem konkreten Personenbezug der betroffenen Daten. Der Umfang des Schutzes geht dabei augenscheinlich über die Grundrechtsgewährleistung aus Art 7,8 GRC hinaus[161]. Das Aufziehen dieses parallelen Schutzregimes könnte aber auch so interpretiert werden, dass der Gesetzgeber einer zu ausschweifenden Interpretation von „was sind personenbezogenen Daten?“ entgegentreten möchte. Denn es gilt andererseits: Bei einem weiten Verständnis des Personenbezugs, wie bspw durch die *absolute Theorie* vertreten, könnte man die fraglichen Schutzziele zumindest teilweise auch im Datenschutzrecht abbilden.

Der datenschutzrechtlichen Analyse auf Basis des Entwurfs zur ePrivacy VO liegt zugrunde, dass § 96 Abs 3 TKG durch die Regelungen der ePrivacy VO vollständig verdrängt werden, und dass die ePrivacy VO als lex specialis zur DSGVO[162] primär Anwendung finden wird. Da die ePrivacy VO in ihrem derzeitigen Entwurfsstadium die Rechtskonstruktion des *berechtigten Interesses* an einer Datenverarbeitung innerhalb ihres materiellen Anwendungsbereichs nicht vorsieht[163], ergibt sich daher unmittelbar, dass dieser Rechtfertigungsgrund - obwohl in der DSGVO vorgesehen - für den Websitebetreiber und den Access-Provider iA nicht zur Verfügung stehen wird.

3.6.2 Anwendungsbereich beim Einsatz von *HTTP Cookies*

Weder das Kriterium des Personenbezugs noch die Notwendigkeit eines potentiell persönlichkeitsrechtlichen Eingriffs sind Voraussetzungen für die Eröffnung des Schutzbereichs. Sowohl das Setzen des Cookies als auch das Auslesen des Cookies[164], unabhängig von dessen Inhalt, unabhängig von der zugrundeliegenden Semantik der Daten und unabhängig von deren Zweckbestimmung, ist daher gemäß Art 8 Abs 1 ePrivacy VO nur zulässig, wenn einer der folgenden Sachverhalte zutrifft:

- Wenn es für die Bereitstellung eines vom Endnutzer gewünschten Dienstes der Informationsgesellschaft *nötig*[165] ist.

[161] *Engeler/Felber,* Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis, ZD 2017, 251 (252).
[162] AaO.
[163] Das ist einer der umstrittensten Punkte im Gesetzgebungsverfahren.
[164] Art 8 Abs 1 wörtlich: „The use of processing and storage capabilities (...)“.
[165] Art 8 Abs 1 lit c.

- Der Benutzer eingewilligt[166] hat, wobei die Einwilligung den in der DSGVO gesetzten Maßstäben genügen muss. Zusätzlich ist die Möglichkeit vorgesehen, eine „Generaleinwilligung“ über die Cookie-Einstellung im Webbrowser abzugeben[167].
- Spezialfall: Webtraffic Analyse (siehe Kapitel 4.8,4.9).

Im Vergleich zum Wortlaut von Art 5 Abs 3 RL 2009/136/EG ergibt sich für das Kriterium „nötig“ hier eine Abweichung. Die Richtlinie statuiert „*strictly* necessary to provide the service“ sowie „*explicitly* requested by the user” - der Kommissionsentwurf der ePrivacy VO enthält diese beiden Steigerungsbegriffe nicht. Allerdings: Die Ergänzungen zum Gesetzesentwurf durch das EU Parlament[168] sehen wiederum diese beiden Steigerungsformen vor. An dieser Stelle soll daher angenommen werden, dass für die ePrivacy VO eine ähnliche Auslegung des Kriteriums der *technischen Notwendigkeit* zu erfolgen hat, wie es bei der Richtlinie der Fall war. Das hat den Vorteil, zumindest in Bezug auf Cookies, dass die detaillierte Ausarbeitung der *Art-29-Datenschutzgruppe*[169] für dieses Kriterium unverändert herangezogen werden kann.

3.6.3 Anwendungsbereich beim Einsatz von *device fingerprints*

Die Technologie des *device fingerprinting* wird von der ePrivacy VO adressiert, wie man ErwGr 20 entnehmen kann. Das Verbot für nicht zweckgerichtete und nicht technisch notwendige clientseitige Verarbeitungen gemäß Art 8 Abs 1 ePrivacy VO umfasst jedenfalls das *active fingerprinting,* sofern letzteres nicht für Kompatibilitätsverbesserungen zwischen Webserver und Browser eingesetzt wird und daher, in enger Auslegung, als technische Notwendigkeit iSv Art 8 Abs 1 lit c ePrivacy VO gerechtfertigt ist.

Hinsichtlich des *passive fingerprinting* ist allerdings eine Klarstellung notwendig: Die prägenden Elemente des *passive device fingerprints* werden heute entweder aufgrund von Compliance-Anforderungen mit den anwendbaren technischen Standards gesendet[170], oder von den Webbrowser Herstellern – im Sinne einer jahrelangen Entwicklung – freiwillig und zusätzlich zu den Vorgaben der Standards, mitgesendet. Das Ziel dieser tw proprietären Erweiterungen war eine Profilierung und Abgrenzung der unterschiedlichen, untereinander im Wettbewerb stehenden Produkte, verbunden mit der Anforderung, eine möglichst große Minimalkompatibilität im Internet herzustellen. Diese herstellerspezifischen Erweiterungen erscheinen heute mit den Privacy by Design Prinzipien schwer in Einklang zu bringen, müssen aber letztlich als technische Realität des Internets akzeptiert werden. Einseitige Änderungen würden zu schweren Störungen im Internetverkehr führen. Websitebetreiber nutzen je nach Programmierung ihrer Web-Applikation einige der mitgesendeten Elemente

[166] Art 8 Abs 1 lit b.
[167] Das ist ebenfalls ein strittiger Punkt im Gesetzgebungsverfahren.
[168] Änderungsvorschläge des EU Parlaments vom 23.10.2017.
[169] *Art-29-Datenschutzgruppe,* WP194, Kapitel 3 & 4.
[170] ZB: Protokollspezifikation HTTP.

um die Usability zu verbessern oder um überhaupt die notwendige Kompatibilität zur Diensterbringung herzustellen – zumindest letzteres müsste man sinnvollerweise unter Art 8 Abs 1 lit c ePrivacy VO als zulässig erachten, um nicht mit einem Tag auf den anderen einen Großteil des Internetverkehrs für unrechtmäßig erklären zu müssen[171]. Eine vom Websitebetreiber verursachte, zusätzliche clientseitige Datenverarbeitung gibt es beim *passive fingerprinting* daher nicht. Hingegeben gibt es notwendigerweise, und eventuell auch gegen den Willen des Websitebetreibers, ein „Auslesen" und Übermitteln von für die Computeridentifikation geeigneten Informationselementen. Falls der Websitebetreiber einige der übermittelten Elemente serverseitig gar nicht benötigt bzw in seiner Applikation nicht berücksichtigt, fehlt iSe Einzelfallbetrachtung sogar die technische Notwendigkeit des Auslesens per se. In diesem Sinne muss Art 8 Abs 1 ePrivacy VO so zu verstehen sein, dass hinsichtlich jener Daten die ohnehin von den Webbrowsern übermittelt werden, lediglich die zweckfremde Weiterverarbeitung, nicht jedoch die Ersterhebung verboten ist[172]. Darauf deutet auch die englische Formulierung der Regelung hin: „*collection* of information". Nach dieser Leseart ist somit auch das *passive fingerprinting,* nämlich als zweckfremde Weiterverarbeitung der fraglichen Informationselemente ohne technische Notwendigkeit, vom Einwilligungsvorbehalt des Art 8 ePrivacy VO umfasst.

3.6.4 Anwendungsbereich bei der Identifikation mithilfe des ISP (*MSISDN forwarding*)

Bei der technischen Realisierung des *MSISDN forwarding* ist das Endgerät des Benutzers nicht involviert. Weder werden Daten vom Endgerät ausgelesen, noch wird Rechenleistung oder Speicherplatz des Endgeräts verwendet. Art 8 ePrivacy VO kommt daher hier nicht zur Anwendung. Die Beurteilung erfolgt somit auf Basis der allgemeineren Bestimmung, Art 6 ePrivacy VO. Diese Bestimmung statuiert unterschiedliche Erlaubnistatbestände für Inhaltsdaten[173] und Metadaten[174], wobei der *HTTP header* unter den Metadaten einzuordnen ist. Eine Analyse dieser Erlaubnistatbestände erfolgt anwendungsfallbezogen in Kapitel 4.6 und Kapitel 4.7.

[171] *Schleipfer,* ZD 2017,460 (464).
[172] *Engeler/Felber,* ZD 2017, 251 (252).
[173] Die Definition in Art 4 lit b ePrivacy VO lautet: „ 'electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound.".
[174] Die Definition in Art 4 lit c ePrivacy VO lautet: „ ' electronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication.

4. Einwilligungserfordernis für ausgewählte Anwendungsfälle

Nach der Ermittlung des abstrakten-generellen datenschutzrechtlichen Prüfmaßstabs sollen nun typische Anwendungsfälle der einzelnen Identifikations- und Wiedererkennungstechnologien näher beleuchtet werden. In Kapitel 3 wurde die datenschutzrechtliche Einordnung der einzelnen Technologien einzig anhand eines möglichen Personenbezugs des jeweiligen Identifikators bewertet. Diese Konzentration auf IP Adressen, Cookies und *device fingerprints* ist nur gerechtfertigt, wenn es genau diese technischen Details sind, von denen die Datenschutzkonformität des jeweiligen Anwendungsfalls entscheidend abhängt[175]. Im Zuge der konkreten Anwendung entstehen nämlich zusätzliche, zweckbezogene Daten die wiederum separat auf ihre datenschutzrechtliche Relevanz zu prüfen sind. Dazu kommt, dass die Rechtfertigung einer Verarbeitung von personenbezogenen Daten, basierend auf einer Einwilligung oder eines anderen Erlaubnistatbestands, anhand des konkreten Verarbeitungszwecks zu prüfen ist. Die Identifikation und Wiedererkennung des Benutzers ist für die folgenden Anwendungsfälle aber nicht der eigentliche Zweck der Verarbeitung, sondern nur ein technisches Hilfsmittel um diesen Zweck zu erreichen.

4.1 Allgemein gültige Gemeinsamkeiten und Erläuterungen

Bevor auf die einzelnen Anwendungsfälle im Detail eingegangen wird, sollen noch allgemein gültige Festlegungen getroffen werden.

4.1.1 Führung des *HTTP access logfile* auf Seiten des Websitebetreibers

Allen Anwendungsfällen liegt annahmegemäß zugrunde, dass der Websitebetreiber ein sogenanntes *HTTP access logfile*[176] führt. Selbst wenn der Websitebetreiber ein reiner Content-Provider ist und sich zur Erfüllung seines Dienste eines Host-Providers iSv § 16 ECG bedient, muss dem Websitebetreiber die Führung des *HTTP access logfile* zugerechnet werden, denn er ist Verantwortlicher iSd Datenschutzgesetze.

Im *HTTP access logfile* werden die IP Adressen und die Zugriffszeitpunkte der Websitebesucher gespeichert[177]. Die Aufbewahrung dieser Daten erfolgt im Allgemeinen über den Zeitraum des aktuellen Besuchs des Nutzers hinaus – dabei kann es sich um mehrere Tage bzw Wochen handeln. Wie oben gezeigt, ergibt sich die Prüfung der datenschutzrechtlichen Zulässigkeit am Maßstab von § 96 Abs 3 TKG – diese Norm ist der maßgebliche, spezialgesetzliche Prüfmaßstab für ein etwaiges Einwilligungserfordernis zur Datenverarbeitung innerhalb des *HTTP access logfile* des Websitebetreibers[178], da die IP

[175] *Schleipfer,* ZD 2015, 399.
[176] In der juristischen Literatur auch als „Web-Log" bekannt.
[177] *Stiemerling/Lachenmann,* Erhebung personenbezogener Daten beim Aufruf von Webseiten - Notwendige Informationen in Datenschutzerklärungen, ZD 2014, 133.
[178] AA *Schenk(Stratil),* Zugriffsanalyse, Online-Targeting und Social Media-Plug-ins - bereichsspezifischer Datenschutz im DSG 2000 und TKG 2003 (2013), 19.

Adresse als personenbezogenes Datum einzuordnen ist. Die Ausnahmeregelung vom Einwilligungserfordernis § 96 Abs 3 Satz 3 TKG fordert aus einer technischen Perspektive die „unbedingte Erforderlichkeit für die Bereitstellung des angeforderten Dienstes". Streng nach dem Wortlaut schließt diese Regelung eine Speicherung der IP Adressen im *HTTP access logfile* über mehrere Tage oder gar Wochen hinweg aus, denn eine unbedingte Erforderlichkeit für diese Speicherung ist für die Erbringung des Dienstes unmittelbar nicht gegeben. Ein berechtigtes Interesse des Websitebetreibers kann, wie oben hergleitet, nicht ohne weiteres berücksichtigt werden.

Allerdings: Für diese serverseitige, vorübergehende Speicherung von IP Adressen im *HTTP access logfile* des Websitebetreibers wurde im Zuge der *Breyer*[179] Entscheidung eine Zulässigkeit der Datenverarbeitung ohne Einwilligung des Benutzers bejaht. Die Entscheidung erfolgte auf Basis von § 15 Abs 1 Satz 1 TMG iVm Art 7 lit f RL 95/46/EG[180]. Dazu wörtlich der EuGH: „Art 7 Buchstabe f der Richtlinie 95/46 ist dahin auszulegen, dass er einer Regelung eines Mitgliedstaats entgegensteht, nach der ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung *erforderlich* sind"[181]. Dies wird im damit begründet, dass der Dienstanbieter ein berechtigtes Interesse daran haben könnte, seine Systeme gegenüber Cyber-Angriffen zu schützen und einige Angriffsmuster nur unter Zuhilfenahme von aussagekräftigen Logfiles erkennbar sind. Ähnliches gilt für drohende und tatsächlich stattfindende technische Gebrechen, deren Vermeidung, Analyse und Behebung ebenfalls das Abspeichern von Quell-IP Adressen erforderlich machen kann. § 15 Abs 1 Satz 1 TMG adressiert denselben Regelungszweck wie § 96 Abs 3 TKG - Eine Übertragung auf die aktuelle österreichische Rechtslage unter Berücksichtigung der neuen Gesetzeslage seit dem 25.5.2018 bietet sich daher an. Der Regelungsgehalt Art 6 Abs 1 lit f DSGVO und Art 7 lit f RL 95/46/EG ist identisch – hier ergeben sich also keine Hindernisse für die Übertragung auf die neue Rechtslage. Sowohl § 15 Abs 1 Satz 1 TMG als auch § 96 Abs 3 Satz 1,2,3 TKG 2003 fordern für die Eröffnung ihres Anwendungsbereichs - im Gegensatz zur Vorgabe durch die Richtlinie - keine Speicherung der Daten auf dem Endgerät des Benutzers.

Das TKG fordert dem Wortlaut folgend eine „unbedingte Erforderlichkeit", wo hingegen das TMG nur von einer schlichten „Erforderlichkeit" spricht. Allerdings ist § 96 Abs 3 direkt aus einem Richtlinienumsetzungsakt hervorgegangen und eine europarechtliche Auslegung des Wortlauts ist daher erst recht zutreffend. Der Klarheit der *Breyer* Entscheidung ist hier Folge zu leisten: Mangels eines alternativen Einfallstors im TKG muss § 96 Abs 3 Satz 3 daher so interpretiert werden, dass auch eine vorübergehende Speicherung der Quell-IP Adresse im *HTTP access logfile* ohne Einwilligung des Benutzers zulässig ist. Dieses Ergebnis deckt

[179] EuGH 19.10.2016, C-582/14 *(Breyer)* iVm BGH 16.5.17, VI ZR 135/13.
[180] Vgl Leitsatz der BGH Entscheidung aaO.
[181] EuGH 19.10.2016, C-582/14 (*Breyer*) Rn 64.

sich erfreulicherweise mit der dogmatischen europarechtlichen Herleitung aus Kapitel 3.4, wo ein Durschlagen des berechtigten Interesses iSd DSGVO auf die spezielle Regelung des TKG - jedenfalls für Daten außerhalb des Endgeräts - vorsichtig befürwortet wurde.

Ergänzend sei noch angemerkt, dass das *HTTP access logfile* weitere, benutzerspezifische Daten abspeichert. Da wäre zunächst der sogenannte *Referrer*[182]*.* In Verbindung mit der IP Adresse des Benutzers reichert dieses Datum den benutzerspezifischen, personenbezogenen Datensatz nicht unwesentlich an. Der *Referrer* enthält die Web-Adresse, von welcher der Benutzer einem Link folgend auf das Angebot des Websitebetreibers gelangt ist (zB via Treffer in einer Suchmaschine)[183]. Das kritische Datum hinsichtlich des Personenbezugs bleibt aber weiterhin die IP Adresse – der *Referrer* ist nur ein zusätzliches personenbezogenes Datum, erhöht aber iA nicht die Bestimmbarkeit der natürlichen Person. Die Speicherung des *Referrers* kann jedenfalls auch mit derselben Argumentation („Aufrechterhaltung des technischen Betriebs“) gerechtfertigt werden wie die IP Adresse selbst.

Das *HTTP access logfile* speichert außerdem uU auch Eingaben des Benutzers, welche dieser auf den entsprechenden Web-Eingabemasken der Website durchführt. Diese Eingaben werden uU[184] über die URL an die nächste Unterseite übergeben und können daher auch Teil des *HTTP Access Logs* sein*.* Diese Eingaben tätigt der Benutzer allerdings freiwillig und bewusst. Selbst wenn er nicht mit einer vorübergehenden Speicherung seiner Eingaben rechnet, wird im Sinne einer Interessensabwägung der obigen Argumentation („Aufrechterhaltung des technischen Betriebs“) folgend eine vorübergehende Speicherung auf Seiten des Websitebetreibers zuzustehen sein.

Im Ergebnis löst das alleinige Führen des *HTTP access logfile* noch kein Einwilligungserfordernis seitens des Websitebenutzers aus. Allerdings muss das Logfile mit einer automatischen Löschung[185] versehen werden und die im Logfile abgespeicherten Daten dürfen ohne Anonymisierung keinem weiterführenden Zweck, zB einer Besucherstatistik, zugeführt werden. Abgesehen von diesen Vorgaben sei ergänzend noch auf die Vorschriften zur Informationspflicht gemäß Art 13,14 DSGVO und im speziellen § 96 Abs 3 Satz 1 TKG verwiesen, welche jedenfalls eingehalten werden müssen.

4.1.2 Freiwillige Registrierung zu einem geschlossenen Bereich einer Website

Eine freiwillige Registrierung zu einem geschlossenen Bereich einer Website („Login-Area“) ist eine klassische Methode, um einen Websitebenutzer wiederzuerkennen. Jedoch wird auf

[182] Quelle Wikipedia: <en.wikipedia.org/wiki/*HTTP*_referer>
[183] *Feiler/Horn,* DSGVO Praxis, 98.
[184] Dies ist abhängig von der Programmierung der Webseiten und der Konfiguration der Webserversoftware. Vgl POST vs GET Methode: <developer.mozilla.org/en-US/docs/Learn/HTML/Forms/Sending_and_retrieving_form_data>
[185] Die Angemessenheit der Löschfrist soll an dieser Stelle nicht konkretisiert werden. Eine untere Grenze könnte sich ergeben aus BGH 3.7.2014, III ZR 391/13 = ZD 2014, 461 (*Eckhardt*): „Die Speicherung von bis zu sieben Tagen ist zulässig“. Eine obere Grenze könnte sein: „bis zu 3 Monate“ (vgl *Feiler/Horn,* DSGVO Praxis*,* 98).

diesen Anwendungsfall im Rahmen dieser Arbeit nicht im Detail eingegangen, da der Vorgang für den Benutzer weitgehend transparent ist, der Benutzer annahmegemäß freiwillig diese Eingaben tätigt und im Zuge der Eingabe seiner persönlichen Daten oder der Wahl seines Login Namens mit einer entsprechenden Einwilligungserklärung konfrontiert werden kann bzw muss - je nach dem Zweck der Verarbeitung. Unter Einhaltung der Informationspflichten gemäß Art 13,14 DSGVO wird man eine einfache Registrierung zu einem geschlossenen Bereich einer Website, wo der Benutzer seinen *username* und sein *password* frei wählen kann, bereits als konkludente, freiwillig erteilte, ausreichend informierte und unmissverständliche Einwilligungshandlung zur Verarbeitung des als Pseudonyms einzustufenden *username* ansehen können. Dem Websiteanbieter wird oftmalig auch zuzustehen sein, dass er die einzelnen Benutzer dazu zwingt, eine gültige Email Adresse einzugeben. Das kann eine erforderliche Maßnahme zur Missbrauchsbekämpfung sein. Für die Datenschutzkonformität des Internetangebotes ist es zusätzlich notwendig, dem Benutzer die Möglichkeit zur Löschung seines Accounts zu geben (Art 17 DSGVO).

4.2 Vorhalten von benutzerspezifischen Einstellungen und Eingaben für den Zeitraum des aktuellen Besuchs der Website

4.2.1 Kurzbeschreibung des Anwendungsfalls

Wie in Kapitel 1.1.2 angesprochen, findet auch in diesem Szenario streng genommen bereits eine Identifikation und Wiedererkennung des Benutzers statt – und zwar bei jedem einzelnen Zugriff auf eine Unterseite der Website. Dies erfolgt zu dem Zweck dem Benutzer über mehrere Unterseiten hinweg den angeforderten Workflow zur Verfügung zu stellen. Es werden benutzerspezifische Einstellungen und Eingaben des Benutzers für die Dauer der aktuellen Sitzung gespeichert. Beispielhaft: Die Sprache der Webseite, Positionen von Anzeigeelementen, zuletzt eingegebene Suchbegriffe, Authentifizierungsinformationen, Warenkörbe, etc. Sämtliche Einstellungen und Eingaben werden vom Benutzer annahmegemäß freiwillig mittgeteilt und der Benutzer rechnet auch damit, dass diese Eingaben und Einstellungen zumindest für den Zeitraum seines Besuchs erhalten bleiben.

4.2.2 Datenschutzrechtliche Rollenzuteilung

Der Websitebetreiber ist Verantwortlicher und wäre als solcher der Verpflichtete zur Einholung der Einwilligung. Falls er sich eines Hosting-Providers bedient, ist letzterer Auftragsverarbeiter[186] und eine erteilte Einwilligung gegenüber dem Verantwortlichen würde ebenfalls die Datenverarbeitung durch den Auftragsverarbeiter rechtfertigen. Der Internetbenutzer ist Betroffener iSd DSGVO und somit derjenige, der die Einwilligung zu erteilen hätte.

[186] *Funke/Wittmann*, Cloud Computing – ein klassischer Fall der Auftragsdatenverarbeitung?, ZD 2013, 221.

Im Zuge der technischen Verarbeitungsvorgänge (Cookie setzen, auslesen, übermitteln, löschen) findet keine datenschutzrechtlich relevante Änderung in der Rollenzuteilung statt.

4.2.3 Datenschutzrechtliche Einordnung der technischen Verarbeitungsvorgänge

Sollen benutzerspezifische Einstellungen oder Eingaben des Benutzers für die Dauer der aktuellen Sitzung erhalten bleiben, werden üblicherweise *Session Cookies* mit einer *SessionID* eingesetzt. Wie in Kapitel 2.1.1 iVm Kapitel 3.3.2 ausgearbeitet, ist diese ID nicht als personenbezogenes Datum einzuordnen. Eine Verarbeitung von personenbezogenen Daten findet zwar im *HTTP access log* statt (siehe Kapitel 4.1.1) – die Verarbeitung der *SessionID* führt allerdings nicht zu einer zusätzlichen Verarbeitung von personenbezogenen Daten. Eine Speicherung der *SessionID* über den einzelnen Besuch hinaus findet annahmegemäß nicht statt[187] und daher ergibt sich auch keine Möglichkeit für eine nachgelagerte Anreichung der Daten, die eventuell doch zu einem Personenbezug führen könnten. Die *SessionID* liefert in Kombination zum *HTTP Access Log* keine **zusätzlichen** Identifizierungsmöglichkeiten und trägt für sich genommen keinerlei persönlichkeitsrelevante Aussagen **über** den Benutzer.

Authentifizierungsinformationen (*username*, *password*) werden für die Dauer der Sitzung iA nicht über die Cookie Technologie, sondern über rein serverseitige Mechanismen vorgehalten[188]. Dabei kommt es somit iA zu keiner Speicherung von Informationen auf dem Endgerät des Benutzers und außer den in Kapitel 4.1.2 bereits genannten Daten zu keiner zusätzlichen Verarbeitung personenbezogener Daten.

4.2.4 Einwilligungserfordernis (de lege lata)

Das Einwilligungserfordernis zur Führung des *HTTP access logs* wurde in Kapitel 4.1.1 verneint. Annahmegemäß wird ansonsten nicht über die Dauer der Sitzung hinaus festgehalten, welche Unterseiten der Benutzer besucht hat und wie lange er auf diesen verweilt hat. Aus der Perspektive des *tracking* ergibt sich daher keine Verarbeitung von personenbezogenen Daten, die eine Einwilligung erforderlich machen würden.

Mit Verweis auf Kapitel 2.1.1 iVm Kapitel 3.3.2: Unter Verwendung von *Session Cookies* findet keine *zusätzliche* Verarbeitung von personenbezogenen Daten statt. Unter der Annahme, dass es für das serverseitige *HTTP Access Log* ein berechtigtes Interesse zur Verarbeitung gibt, ergibt sich somit bei der Verwendung von *Session Cookies* kein eigenes Einwilligungserfordernis nach dem TKG und der DSGVO.

[187] Dies kann zwar vorübergehend für Zwecke der Fehlerbehebung notwendig sein, ist aber für den Dauerbetrieb des Webservice nicht erforderlich.
[188] ZB: Beim *Apache* Webserver: <www.htaccess-guide.com/password-protection> .

Eine Beurteilung nach dem Regelungsgehalt der Richtlinie 2009/136/EG Art 5 Abs 3 sowie nach der Interpretation der *Art-29-Datenschutzgruppe*[189] kommt zum selben Ergebnis[190].

4.2.5 Einwilligungserfordernis (beurteilt anhand der ePrivacy VO)

Das Einwilligungserfordernis wird anhand von Art 8 ePrivacy VO beurteilt, denn auch wenn der *Session Cookie* nach einer engen Definition nicht am Endgerät „gespeichert" wird, so findet dennoch eine clientseitige Verarbeitung von Daten statt – insbesondere auch eine *Erhebung von Informationen* bei jedem Zugriff auf eine Unterseite des Webangebots. Daher werden die Interpretationen der *Art-29-Datenschutzgruppe* (vgl Kapitel 3.6.2) zu Art 5 Abs 3 RL 2009/136/EG für die Beurteilung herangezogen. Die hier betrachteten *Session Cookies* können unter Art 8 Abs 1 lit c ePrivacy VO als „strictly necessary to provide the requested service"[191] subsumiert werden und sind daher nicht einwilligungspflichtig[192]. Somit ergibt sich kein anderes Ergebnis als in der de lege lata Betrachtung.

4.3 Vorhalten von benutzerspezifischen Einstellungen und Eingaben für die nachfolgenden Besuche auf der Website

4.3.1 Kurzbeschreibung des Anwendungsfalls

Im Gegensatz zum vorherigen Anwendungsfall werden die Einstellungen und Eingaben des Benutzers nun über den einzelnen Besuch des Benutzers hinaus aufbewahrt. Der Zweck der Speicherung ist nun nicht mehr, die angeforderten Eingaben und Einstellungen für den eigentlichen Benutzungsvorgang bereitzuhalten, sondern dem Nutzer diese Eingaben und Einstellungen bei seinem nächsten Besuch wieder zur Verfügung zu stellen. Sofern es sich nicht um eine Registrierung und einen geschlossen Login-Bereich[193] handelt, muss der Nutzer iA nicht damit rechnen, dass er beim nächsten Besuch der Website die von ihm getätigten Eingaben und Einstellungen (zB die Sprachauswahl, letzte eingegebene Suchbegriffe) erneut vorfindet.

Wichtig für die Unterscheidung zu anderen Anwendungsfällen, insbesondere zu *behavioral targeting* (Kapitel 4.7), ist festzuhalten: Der Zweck des gegenständlichen Anwendungsfalls impliziert, dass der Benutzer bei seiner Wiederkehr die Personalisierung der Inhalte selbst wahrnimmt, bspw indem er in einer Drop-Down Box seine vorangegangen Eingaben sieht. Das kann sogar so weit gehen, dass er im Sinne einer Komfortfunktion auf die von ihm zuletzt besuchten Unterseiten hingewiesen wird – das gezielte „anklicken" von Unterseiten soll in diesem Zusammenhang nämlich ebenfalls unter „Eingabe" subsumiert werden. Wie

[189] Vgl Kapitel 3.3.2 iVm Fußnote 119.
[190] Vgl Kapitel 3.3.2; sowie *Art-29-Datenschutzgruppe,* WP194, Kapitel 3.1 „User-input cookies" & Kapitel 3.6 „UI customization cookies".
[191] *Art-29-Datenschutzgruppe*, WP194, Kapitel 2.2 „Criterion B".
[192] So auch: *Schleipfer,* ZD 2017, 460 (464).
[193] Vgl Kapitel 4.1.2.

bisher soll angenommen werden, dass unabhängig vom Zweck des vorliegenden Anwendungsfalls jede vom Benutzer abgerufene Unterseite für beschränkte Zeit ohnehin auch im *HTTP Access Log* gespeichert wird.

4.3.2 Datenschutzrechtliche Rollenzuteilung

Identisch mit vorherigem Anwendungsfall, siehe Kapitel 4.2.2.

4.3.3 Datenschutzrechtliche Einordnung der technischen Verarbeitungsvorgänge

Zur Realisierung dieses Anwendungsfalls werden entweder persistente Cookies mit einem Benutzeridentifikator (=*BenutzerID*) und/oder persistente *non-ID Cookies* eingesetzt. Die Dauer der Speicherung bestimmt der Websitebetreiber in seiner Anwendungsprogrammierung.

4.3.4 Einwilligungserfordernis (de lege lata)

Im Einklang mit den Ergebnissen aus Kapitel 3.2.2 findet beim Einsatz von dauerhaften benutzerspezifischen bzw computerspezifischen Identifikatoren eine Verarbeitung personenbezogener Daten statt. Das Vorhalten der *BenutzerID* liefert eine *zusätzliche Möglichkeit* für die Bestimmbarkeit der realen Person, insbesondere iVm mit dem *HTTP Access Log*. Auch nach der Löschfrist des *HTTP Access Log* kann die Zuordnung zur aktuellen IP Adresse bei jedem nachfolgenden Besuch wiederhergestellt werden. Auch wenn die *BenutzerID* als Zufallsdatum, als Pseudonym, keine persönlichkeitsrelevante Information *über* den Benutzer trägt, so führt deren Verarbeitung aufgrund der zusätzlichen Bestimmbarkeit dennoch zu erhöhten Risiken für die Privatsphäre des Benutzers[194]. Für das Führen des *HTTP Access Log* sind die Verarbeitung der *BenutzerID* und die serverseitige Speicherung von benutzerspezifischen Eingaben und Einstellungen nicht notwendig. Die Zulässigkeit der Verarbeitung der *BenutzerID* kann somit nicht von der Rechtfertigung zur Führung des *HTTP Access Log* gedeckt sein.

Gemäß Kapitel 3.4 iVm Kapitel 4.1.1 ist nur eine sehr eingeschränkte Berücksichtigung eines berechtigten Interesses des Websitebetreibers bei der Anwendung von § 96 Abs 3 TKG möglich, und dieses soll noch dazu auf technisch motivierte Rechtfertigungsgründe eingeengt werden. Einen spezialgesetzlichen Erlaubnistatbestand für diesen Fall, wie bspw in § 15 Abs 3 TMG[195], gibt es in Österreich nicht. Einwänden von Websitebetreibern, welche durch die Speicherung von benutzerspezifischen Eingaben und Einstellungen ihr Produkt verbessern und dadurch die Benutzerakzeptanz erhöhen wollen, wird man entgegenhalten, dass diese Zwecke auch mit anonymisierten Daten zu erreichen sind[196]. Alternativ kann dem Benutzer auch eine entsprechende Auswahlmöglichkeit zur Verfügung gestellt werden, ob er

[194] Vgl „Theorie über die Verkettung der pseudonymisierten IP Adresse".
[195] Es ist - wie bereits dargelegt - umstritten, ob § 15 Abs 3 TMG nach dem 25.5.2018 noch angewendet werden kann.
[196] Ähnlich argumentieren für Fahrzeugdaten: *Kunnert,* Die datenschutzkonforme Vernetzung des Automobils, CR 2016, 509 (512); *Roßnagel,* Fahrzeugdaten – wer darf über sie entscheiden, Straßenverkehrsrecht 8/2014, 281 (285).

die Speicherung seiner Einstellungen und Eingaben wünscht. Genau diese Auswahlmöglichkeit wäre, bei entsprechender Formulierung und Ausgestaltung, eine datenschutzrechtliche Einwilligungserklärung und muss als solche mangels anderer berücksichtigungswerter Interessen auf Seiten des Websitebetreibers hier verlangt werden. Der inhärente Personenbezug der *BenutzerID* führt daher ohne weitere Analyse der konkret verarbeitenden Inhaltsdaten (!), welche allenfalls noch zusätzlich zur *BenutzerID* gespeichert werden[197], zu diesem Ergebnis.

Der genannte Anwendungsfall ist jedoch auch durch den Einsatz von *non-ID Cookies* realisierbar. Hier ist eine differenzierte Betrachtungsweise erforderlich: Wie in den Kapiteln 3.2.2, 3.3.2 erläutert, findet hier uU für sich alleine betrachtet nicht notwendigerweise eine Verarbeitung von personenbezogenen Daten statt.
Einer generellen Ablehnung des Einwilligungserfordernisses steht zunächst die Argumentation und die Beurteilung der *Art-29-Datenschutzgruppe* auf Basis der Richtlinie 2009/136/EG Art 5 Abs 3 entgegen (vgl Kapitel 3.3.2). Aus den Erläuterungen in Kapitel 3.6 von WP194 geht hervor, dass die *Art-29-Datenschutzgruppe* diese Art von Cookies als minimalinvasiv einschätzt, aber trotzdem das Einwilligungserfordernis aufrechterhalten möchte. Hier erweist sich die strikte, technische Sichtweise der Richtlinie mit dem hinreichenden (!) Kriterium der „lokalen Datenspeicherung“ und die darauf aufbauende (ebenfalls technische) Argumentation der *Art-29-Datenschutzgruppe* offenbar als zu einschränkend. Zielführender ist es hier, die gespeicherten Daten im Cookie auf deren persönlichkeitsrechtlichen Gehalt zu analysieren. Der Inhalt des Cookies wird bei jeder Kontaktaufnahme mit der Website an den Websitebetreiber übermittelt – demnach gibt es auch auf Seiten des Websitebetreibers eine *Verarbeitung* iSd Datenschutzgesetze.

Danach sollen für die datenschutzrechtliche Analyse von *non-ID Cookies* fünf Fälle unterschieden werden, und zwar nach dem konkreten Inhalt der gespeicherten Daten:

1. Fall: Die im *non-ID Cookie* gespeicherten Daten könnten *systemimmanent* eindeutig für jeden unterschiedlichen Benutzer sein, zB wenn Authentifizierungsinformationen (*username*[198] und/oder verschlüsseltes *password*) für den Login gespeichert werden. Diese Cookies sind aufgrund der zusätzlichen Bestimmbarkeit des realen Benutzers über die Konstruktion der *Theorie über die Verkettung der pseudonymisierten IP Adresse* identisch zu behandeln wie jene mit einer serverseitig eindeutig vergebenen *BenutzerID*. Über die zwingende Verbindung mit der IP Adresse des Benutzers erfahren somit auch die im Cookie gespeicherten Inhaltsdaten einen Personenbezug – sie können aus technischen Gründen nicht ohne Herstellung des Personenbezugs verarbeitet werden. Es findet daher eine *zusätzliche* Verarbeitung von personenbezogenen Daten statt, die iA nicht ohne weiteres von

[197] ZB: die gewählte Spracheinstellung des Benutzers.
[198] Annahmegemäß vergibt der Benutzer hier selbst einen *Username* und ist nicht gezwungen, ein unmittelbares personenbezogenes Datum (zB: seine Email Adresse) anzugeben.

einer eventuell konkludenten oder auch ausdrücklichen[199] Einwilligung wie beschrieben in Kapitel 4.1.2 („Registrierung“) gedeckt ist. Auch die Rechtfertigung aus Kapitel 4.1.1 („*HTTP Access Log*“) greift nicht.

2. Fall: Die im *non-ID Cookie* gespeicherten Daten könnten *nicht systemimmanent* eindeutig für jeden unterschiedlichen Benutzer sein. Sie *könnten* aber im Laufe der Zeit eindeutig werden (Bspw gespeicherte Suchanfragen, Speicherung des Verlaufs der besuchten Unterseiten). Hier muss mit Verweis auf Kapitel 3.2.3 berücksichtigt werden: Im Vergleich zum *device fingerprint*, welcher den Grad an Individualität über die fortschreitende Zeit verliert, ist es hier genau umgekehrt – bei einer Speicherung von historischen Benutzereingaben wird der Datensatz über die fortschreitende Zeit immer eindeutiger. Der Argumentation in Kapitel 3.2.3 folgend, greift die *Theorie über die Verkettung der pseudonymisierten IP Adresse* hier aber aufgrund der fehlenden systemimmanenten Eindeutigkeit trotzdem nicht. Daher ergibt sich hier auch iVm dem *HTTP Access Log vorerst* keine zusätzliche Verarbeitung personenbezogener Daten und keine Einwilligungsverpflichtung.

3. Fall: Die im *non-ID Cookie* gespeicherten Daten könnten für sich alleine betrachtet bereits personenbezogene Daten im Sinne eines zentralen Identifikationselements der Person sein, zB Name, email-Adresse oder ähnliche Stammdaten. Diese Daten können auch im Nachhinein in die Datenbasis des Cookie gelangen, zB indem sich ein Benutzer bei der Website registriert und dort seine Stammdaten eingibt. Der Personenbezug ergibt sich hier gemäß Art 4 Z 1 DSGVO bereits über das Kriterium der *Bestimmtheit.* Durch die lokale Speicherung am Endgerät und das Versenden des kompletten Datensatzes an den Server findet eine *zusätzliche* Verarbeitung von personenbezogenen Daten statt, die iA nicht ohne weiteres von einer eventuell konkludenten oder auch ausdrücklichen Einwilligung wie beschrieben in Kapitel 4.1.2 („Registrierung“) gedeckt ist. Auch die Rechtfertigung aus Kapitel 4.1.1 („*HTTP Access Log*“) greift nicht.

4. Fall: Die im *non-ID Cookie* gespeicherten Daten könnten für sich alleine Identifizierungsmerkmale liefern, die zur *Bestimmbarkeit* der realen Person im Sinne eines *besonderen Merkmales* gemäß Art 4 Z 1 DSGVO führen. Ein plakatives Beispiel wäre der Fall, wo eine Website mit einem Online-Routenplaner bei jeder Benutzung den Start- und Endpunkt einer Route speichert. Nach einigen wenigen wiederkehrenden Besuchen kann mit hoher Wahrscheinlichkeit auf ein zentrales Bestimmbarkeitsmerkmal des Benutzers, seine Wohnadresse, geschlossen werden. Durch die lokale Speicherung am Endgerät und das Versenden des kompletten Datensatzes an den Server findet eine *zusätzliche* Verarbeitung von personenbezogenen Daten statt, die nicht vom Erlaubnistatbestand Kapitel 4.1.1 („*HTTP Access Log*“) umfasst ist.

[199] Je nach der konkreten Ausgestaltung der Abfrage.

5. Fall: Angenommen, die im *non-ID Cookie* gespeicherten Daten liefern für sich alleine iA *keine* Identifizierungsmerkmale, die zur *Bestimmbarkeit* der realen Person führen. Ein plakatives Beispiel wäre der Fall, wo ein *non-ID Cookie* dafür verwendet wird, einzig die vom Benutzer getätigte Spracheinstellung auf einer Website abzuspeichern. Schwieriger in der Beurteilung sind jene Fälle, in denen der *non-ID* Cookie ein *Nutzungsprofil*[200] des Benutzers enthält - bspw gespeicherte Suchanfragen oder die Speicherung des Verlaufs der besuchten Unterseiten, sogenannter *clickstream*[201]. Unter der Annahme, dass auch die *Summe* aller vorhandenen Daten kein *besonderes* Merkmal gemäß Art 4 Z 1 DSGVO ist, welches zu einer unmittelbaren Bestimmbarkeit der Person führt, so kann das Nutzungsprofil dennoch Aufschlüsse über Hobbys, Interessen, Kaufverhalten, Bedürfnisse, Vorlieben und daraus resultierend Rückschlüsse auf zentrale Persönlichkeitsmerkmale der Person ermöglichen. Dadurch erfolgt zumindest ein Teilabbild der Persönlichkeit des Nutzers[202]. Dem steht auch nicht die begrenzte Speichergröße des *HTTP Cookies* entgegen, denn diese kann einerseits durch technologische Erweiterungen erhöht werden und andererseits ist eine ausreichende Aussagekraft der gespeicherten Informationen auch in einem 4kByte[203] Datenraum denkbar. Aus datenschutzrechtlicher Sicht kommt erschwerend hinzu, dass der Inhalt des Cookie in seiner Gesamtheit bei jedem Besuch der Website an den Websitebetreiber übermittelt wird und letzterer daher auch ohne eine serverseitige Speicherung regelmäßig Kenntnis von dem kompletten Datensatz erlangt. Die Daten *können* sogar eindeutig sein – da sie aber nicht *systemimmanent* eindeutig (siehe oben, 2. Fall) sind, greift die Argumentation über die *Theorie über die Verkettung der pseudonymisierten IP Adresse* hier nicht.

Beurteilt man die in dem Nutzungsprofil enthaltenen Daten letztlich als Teilabbild der Persönlichkeit des Nutzers[204], so handelt es sich dabei zweifellos um *Daten über eine Person*, und diese sind auch, bezogen auf den Einzelnutzer des Endgeräts, individualisiert. Aber: Einzelangaben, die sich auf eine einzelne Person beziehen, sind dann keine personenbezogenen Daten, wenn die Person nicht bestimmbar ist[205]. Für eine Bestimmbarkeit der realen Person anhand des Nutzungsprofils müssten weitere Verknüpfungsmöglichkeiten zur realen Person in anderen, zumindest theoretisch verfügbaren Datenquellen, vorliegen. Ansonsten bleibt es schlicht bei einem *Wissen* über eine *unbekannte* Person. Darauf findet das Datenschutzrecht keine Anwendung. Dafür spricht auch die Definition des *Profiling* Art 4 Z 4 DSGVO: Unter *Profiling* versteht die DSGVO eine spezifische Verarbeitung *personenbezogener Daten* und regelt für diese

[200] Der Begriff *Nutz**ung**sprofil* ist hier absichtlich gewählt. Die DSGVO spricht hingegen von Nutz**er**profilen bzw Persönlichkeitsprofilen (ErwGr 30, 38). Eine Abgrenzung dieser drei Begriffe ist schwierig, aber: Der gegenständliche Anwendungsfall ist jedenfalls darauf beschränkt, dass die vom Benutzer übergebenen Informationen nicht durch, wie auch immer ausgestaltete, Profiling-Mechanismen angereichert werden. Vgl dazu auch „persönliche Aspekte" (Art 4 Z 4 DSGVO).
[201] In der Praxis wird dieser Anwendungsfall oft mit *BenutzerID*-Cookies realisiert. In diesem Fall ergibt sich das Einwilligungserfordernis wie oben bereits dargestellt.
[202] *Spindler/Nink* in *Spindler/Schuster* § 15 TMG Rn 9.
[203] Quelle Wikipeida: <en.wikipedia.org/wiki/HTTP_cookie>
[204] Dies ist eine Einzelfallentscheidung die konkreten Bezug auf die Art und den Umfang der gesammelten Daten nehmen muss. Die Schwelle wird man eher niedrig ansetzen – Eine oftmalige Suche nach „veganen Kochrezepten" könnte genügen.
[205] *Gola/Klug/Körffer* in *Gola/Schomerus* BDSG § 3 Rn 3.

spezifische Verarbeitung besondere Rechte und Pflichten[206]. Aus diesen Regelungen kann man aber nicht den Umkehrschluss ziehen, dass alleine die Existenz eines Nutzungsprofils über eine Person den Personenbezug dieses Profils impliziert. Die Bestimmbarkeit der realen Person ist weiterhin Voraussetzung für den Personenbezug des Nutzungsprofils, zB durch die Auflösung eines mit dem Datensatz verbundenen Pseudonyms oder durch andere Zusammenführungsmethoden. Zu berücksichtigen ist dabei auch, dass das Nutzungsprofil weiterhin auf eine Website begrenzt ist und vorerst kein Austausch von Nutzungsprofilen zwischen verschiedenen Websitebetreibern angenommen wird. Die DSGVO ist nicht auf anonymisierte Datensätze anzuwenden (ErwGr 21). Auch aus einer historischen Betrachtung des Datenschutzrechts ging es, vereinfacht gesagt, immer um den Schutz von Daten, die einer Personen „mit Namen und Gesicht" zugeordnet sind[207].

Nun könnte aber als Gegenargument angeführt werden, dass im Moment der Kontaktaufnahme das Nutzungsprofil des Benutzers gemeinsam mit seiner aktuellen IP Adresse dem Websitebetreiber *mitgeteilt* wird und letzterer daher wie gezeigt sehr wohl eine Zuordnungsmöglichkeit zwischen der realen Person und dem übermittelten Profil herstellen könnte. Diese *Mitteilung* würde für sich alleine bereits zu einer *Datenverarbeitung* als Voraussetzung für eine Eröffnung des Datenschutzrechts führen, auch ohne dass der Websitebetreiber selbst eine Speicherung der Daten vornimmt. Die Zuordnung zur realen Person kann der Websitebetreiber aber nicht durch eigenes Wissen tun, sondern annahmegemäß nur durch eine Abfrage über den Access-Provider. Diese Abfragemöglichkeit steht nicht in Echtzeit zur Verfügung, sondern ist ein langwieriger, manueller Prozess – teilweise unter Mitwirkung der Behörden. Sofern das Nutzungsprofil und dessen Zuordnung zu einer IP Adresse serverseitig nicht gespeichert wird[208], steht dieser Weg der retrograden Bestimmung der realen Person somit nicht offen.

Die Speicherung des Nutzungsprofils auf dem Endgerät selbst eröffnet nicht den Anwendungsbereich des Datenschutzes, da diese Speicherung im geschützten, privaten Lebensbereich des Benutzers stattfindet. Es gilt nämlich: Der Betroffene, der nur Daten über sich selbst verarbeitet, ist weder Auftraggeber noch Verantwortlicher iSd DSGVO[209].

Fraglich ist daher letztlich, ob die hier erfolgte Auslegung des Begriffs *Bestimmbarkeit* im Sinne einer möglichen Zusammenführung mit der realen, benennbaren Person in diesem Anwendungsfall sachgerecht ist. Durch den neuerlichen Besuch des Benutzers auf der Website findet, wenn auch keine Verknüpfung mit der realen Identität, jedenfalls eine eindeutige Wiedererkennung statt und anhand dieser Wiedererkennung iVm mit dem vorgehaltenen Nutzungsprofil wird dem Benutzer ein individualisiertes Benutzungserlebnis geboten. Man könnte demnach sagen, dass die Online-Identität (auch genannt: virtuelle

[206] *Schleipfer,* ZD 2017, 460 (462).
[207] *Härting,* NJW 2013, 2065 (2069).
[208] Das ist annahmegemäß nicht der Fall. Auch das *HTTP Access Log* liefert hier iA keine verknüpfungsfähige Information.
[209] *Häberle* (Hrsg), Erbs/Kohlhaas - Strafrechtliche Nebengesetze[219] (2018) BDSG § 3 Rn 33.

Identität[210]) des Benutzers festgestellt und zugewiesen wird, aber eben nicht seine reale Identität[211]. Die heimliche Ausspähung der eigenen Aktivitäten, auch wenn sie anonym erfolgt, wird von vielen Benutzern als Eingriff in die Privatsphäre empfunden[212]. Im Hinblick darauf erscheint ein kompletter Ausschluss aus einem persönlichkeitsrechtlichen Schutzbereich problematisch. Eine dogmatisch vertretbare Subsumption unter das zentrale Kriterium V*erarbeitung personenbezogener Daten* ist aber aufgrund der fehlenden Bestimmbarkeit der Person - zumindest außerhalb weniger Spezialfälle[213] - weiterhin nicht möglich[214].

Einen Ausweg bietet der Denkansatz, den auch die EU in ihrer ePrivacy Gesetzgebung verfolgt. Unter Berufung auf Art 7 GRC bzw Art 8 EMRK sind Eingriffe in die Privatsphäre von Benutzern von Kommunikationsendgeräten auch dann denkmöglich, wenn keine Verarbeitung von personenbezogenen Daten stattfindet (vgl Kapitel 3.3.2, 3.5). Die Beurteilung, ob ein Eingriff vorliegt, erfolgt dann allerdings außerhalb des Datenschutzrechts.

Als deliktrechtliches Einfallstor in das Privatrechtsverhältnis zwischen Websitebetreiber und Internetnutzer kommt das allgemeine Persönlichkeitsrecht gemäß § 16 ABGB, bzw in einer noch spezielleren Ausprägung, § 1328a ABGB in Betracht. Das allgemeine Persönlichkeitsrecht schützt den Nutzer „hinter" der Online-Identität, aber nicht die Online-Identität selbst – letztere ist kein Rechtsträger des Persönlichkeitsrechts[215]. Der Schutz ist unabhängig davon zu gewähren, ob die natürliche Person „hinter" der Online-identität bekannt ist oder nicht[216]. Spezifische Interessen, Neigungen und Gewohnheiten dieser Person liegen im Schutzbereich von § 1328a ABGB[217]. Es ist nicht ausgeschlossen, dass die gespeicherten Daten – zB ein Nutzungsprofil - eine entsprechende Aussagekraft haben.

Im Gegensatz zu anderen Persönlichkeitsschutznormen ist bei § 1328a ABGB die *Veröffentlichung* keine Bedingung für den Eingriff in den Schutzbereich. Es genügt die *Verwertung*, und zwar im Sinne des Ziehens eines wirtschaftlichen Nutzens[218]. Ausgeschlossen ist der Schutz, wenn die in Frage stehenden Informationen selbst veröffentlicht oder preisgegeben wurden[219] - mit einer unwissentlichen Speicherung auf Seiten des Kommunikationspartners muss der Preisgebende hingegen nicht rechnen. Inwieweit diese Speicherung eine Persönlichkeitsverletzung darstellen kann, ist Gegenstand einer umfassenden Interessensabwägung und somit nur einer Einzelfallbeurteilung zugänglich. Falls der Websitebetreiber aber seinerseits nur wirtschaftliche Interessen geltend

[210] Eine mögliche Definition von „Online-Identität" nach *Meyer*, Identität und virtuelle Identität natürlicher Personen im Internet (2011) 133: „Ein Nutzerprofil einer Person, das auf Dauer angelegt ist, konsistent genutzt wird und daher für andere Nutzer wiedererkennbar ist, ohne dass die dahinterstehende natürliche Person erkennbar ist.".
[211] *Pachinger,* JusIT 2011/10, 20.
[212] *Härting,* NJW 2013, 2065 (2071).
[213] Vgl 4. Fall.
[214] Stellvertretend: *Dieterich,* ZD 2015, 199 (203).
[215] *Meyer*, Identität und virtuelle Identität, 134.
[216] Vgl aaO Kapitel II.1.
[217] *Danzl* in *Koziol/Bydlinski/Bollenberger* ABGB § 1328a Rn 4.
[218] *Helmich,* ecolex 2003, 888.
[219] *Danzl* in *Koziol/Bydlinski/Bollenberger* ABGB § 1328a Rn 4.

machen kann, so wird eine zeitlich unlimitierte oder zumindest sehr großzügige, systematische und umfassende Speicherung von Nutzungsprofilen die Voraussetzungen eines Verstoßes gegen § 1328a ABGB erfüllen können.

Im Ergebnis zu 5. Fall bleibt daher festzuhalten, dass im Falle der umfassenden Speicherung von Eingaben, Einstellungen oder *clickstreams*, welche einen nicht unwesentlichen persönlichen Bezug zu einem nicht bestimmbaren - aber im Zuge seines Wiedererscheinens dennoch ausgesonderten und iA auch anders behandelten[220] - Nutzer herstellen, eine Einwilligung zu fordern ist[221]. Allerdings ergeben sich die Ausgestaltungsanforderungen dieser Einwilligung nicht durch das Datenschutzrecht, sondern über das allgemeine Persönlichkeitsrecht. Insofern könnte eine – informierte[222] und unmissverständliche – Opt-Out Lösung ausreichend sein. Doch das soll an dieser Stelle nicht weiter vertieft werden.

4.3.5 Einwilligungserfordernis (beurteilt anhand der ePrivacy VO)

Das Einwilligungserfordernis wird anhand von Art 8 ePrivacy VO beurteilt und zwar unter Anwendung der Interpretationen der *Art-29-Datenschutzgruppe* (vgl Kapitel 3.6.2) zu Art 5 Abs 3 RL 2009/136/EG. Eine Differenzierung nach dem Personenbezug der verarbeitenden Daten ist danach nicht erforderlich. Keiner der Erlaubnistatbestände von Art 8 Abs 1 lit a bis lit d ePrivacy VO ist erfüllt, insbesondere auch nicht die *technische Notwendigkeit*. Beurteilt nach der ePrivacy VO ergibt sich demnach ein unbedingtes Einwilligungserfordernis für die Realisierung dieses Anwendungsfalls mittels *HTTP Cookies*.

4.4 „Auto-Login“ zu einem geschlossenen Benutzerbereich

4.4.1 Kurzbeschreibung des Anwendungsfalls

Hierbei handelt es sich um einen Spezialfall zum Anwendungsfall aus Kapitel 4.3. Es geht darum, dass dem Benutzer ein „Auto-Login“ zu einem abgeschlossenen Benutzerbereich angeboten wird. Abweichend von Kapitel 4.3. ist für diesen Fall aber eine vorherige Registrierung (vgl Kapitel 4.1.2) erforderlich – die Authentifizierungsdaten (*username*, *password*) sind demnach serverseitig gespeichert.

4.4.2 Datenschutzrechtliche Rollenzuteilung

Identisch zu den vorherigen Anwendungsfällen, siehe Kapitel 4.2.2.

---

[220] Der Benutzer wird insofern unterschiedlich behandelt, weil er letztlich eine unterschiedliche Darstellung auf den Webseiten bekommt. Die Darstellung wird aufgrund seines vorangegangenen Verhaltens für ihn personalisiert.

[221] **Wichtig:** Das hier abgeleitete Schutzkonzept ist darauf aufgebaut, dass der fragliche Datensatz des Cookies eine *aktive* Aussonderung des Benutzers verursacht. Dies erfolgt im behandelten Anwendungsfall durch die lokale Speicherung und somit fixierte Beziehung zum Computer des Benutzers und das anschließende Absenden des Datensatzes zum Websitebetreiber bei jedem einzelnen Besuch. Würde der Datensatz von dem Computer getrennt, zB durch das Abspeichern auf einem USB Stick oder durch das Einspielen in eine (passive bzw offline) BigData Analyse, so ist die hier dargelegte Argumentation des Persönlichkeitsrechtseingriffs nicht mehr haltbar.

[222] Die Informationspflichten aus der DSGVO könnten hier analog herangezogen werden.

4.4.3 Datenschutzrechtliche Einordnung der technischen Verarbeitungsvorgänge

Die folgenden Technologien können zum Einsatz kommen:

a) *HTTP Cookie* mit clientseitig gespeichertem Pseudonym (*BenutzerID*)
b) *HTTP Cookie* mit clientseitig gespeicherten Authentifizierungsdaten (*Username*, *password*)[223]

Aufgrund der fehlenden Eindeutigkeit kommt die Technologie *device fingerprinting* hier in der Praxis nicht zum Einsatz.

Die dargestellten Identifikationsmethoden erlauben lediglich die Wiedererkennung des Endgeräts, aber nicht des Benutzers selbst. Dies erfordert iA einen Schutz des Benutzers vor der unberechtigten Benutzung seines Endgeräts. Je nach Ausgestaltung des Webangebots kommt in der Praxis daher oftmals ein zweistufiger Login-Prozess zur Anwendung. Hierbei gelangt der Nutzer durch den Auto-Login nur zu „unkritischen" Dienstleistungen, wie zB das streaming von Videos im Rahmen seines Vertrags. Sobald der Benutzer Einstellungen ändert oder kostenpflichtige Bestellungen macht wird oftmals zusätzlich eine manuelle Authentifizierung durchgeführt (zB durch die Eingabe von *username*, *password*).

4.4.4 Einwilligungserfordernis (de lege lata)

Mit Verweis auf die Ergebnisse aus Kapitel 4.3.4: Bei beiden technischen Realisierungen kommt es zur Verarbeitung von personenbezogenen Daten. Bei a) aufgrund der Verarbeitung des eindeutigen Pseudonyms *BenutzerID*, bei b) aufgrund der Verarbeitung der *systemimmanent* eindeutigen Authentifizierungsdaten im Cookie. Für die zusätzliche (!) Verarbeitung von personenbezogenen Daten gibt es gemäß § 96 Abs 3 TKG keine technische Notwendigkeit. Das Auto-Login ist demnach eine einwilligungspflichtige, zusätzliche Komfortfunktion. Die notwendige Einwilligung, sofern sie die Anforderungen an Informiertheit und Unmissverständlichkeit erfüllt und zusätzlich die Informationspflichten gemäß Art 13,14 DSGVO eingehalten werden, kann im Zuge der Erstregistrierung des Benutzers abgefragt werden. Da es auf Seiten des Websitebetreibers keine Rechtfertigung für die Verarbeitung gibt und durch die Nutzung der Funktion iA ein erhöhtes Identifizierungsrisiko der realen Person entsteht, muss dem Benutzer jedenfalls die Wahlmöglichkeit gegeben werden, den Dienst auch ohne der Auto-Login Funktion zu nutzen. Der Benutzer kann das jederzeit durch Widerruf einer zuvor erteilten Einwilligung gemäß Art 7 Abs 3 DSGVO ausdrücken.

[223] Aus sicherheitstechnischen Gründen ist diese technische Realisierung nicht optimal, vgl Fußnote 14.

4.4.5 Einwilligungserfordernis (beurteilt anhand der ePrivacy VO)

Zur Realisierung dieses Anwendungsfalls mittels *HTTP Cookies* ist kein Erlaubnistatbestand aus Art 8 lit a bis d ePrivacy VO einschlägig. Siehe dazu auch die Ausführungen des vorangegangen Kapitels 4.3.5. Somit ergibt sich für das Einwilligungserfordernis kein anderes Ergebnis als in der de lege lata Betrachtung.

4.5 Zusätzliche Sicherheitsüberprüfung bei Authentifizierung zu Login-Area

4.5.1 Kurzbeschreibung des Anwendungsfalls

Der Anwendungsfall ist ähnlich zum Anwendungsfall aus Kapitel 4.4 („Auto-Login“), jedoch erfolgt hier kein automatischer Login zum abgeschlossenen Bereich der Website, sondern eine zusätzliche Überprüfung des manuell durchgeführten Authentifizierungsergebnisses. Falls sich ein Benutzer in der Vergangenheit regelmäßig von ein und demselben Endgerät in den geschlossenen Bereich der Website eingeloggt hat, so soll ein neuerlicher Login[224] von einem anderen/unbekannten Endgerät zu einer zusätzlichen Sicherheitsabfrage führen. Wahlweise auch zu einer Notifikation des Benutzers per email über den versuchten Login-Versuch. Geraten *username* und *password* in die falschen Hände, so ist auf diese Art und Weise ein effektiver zusätzlicher Schutz vor Identitätsdiebstahl realisiert.

4.5.2 Datenschutzrechtliche Rollenzuteilung

Identisch zu den vorherigen Anwendungsfällen, siehe Kapitel 4.2.2.

4.5.3 Datenschutzrechtliche Einordnung der technischen Verarbeitungsvorgänge

Die folgenden Technologien können zum Einsatz kommen:

a) *HTTP Cookie* mit clientseitig gespeichertem Pseudonym (*BenutzerID*)
b) Wiedererkennung des Endgeräts mittels *device fingerprint*

4.5.4 Einwilligungserfordernis (de lege lata)

zu a) Aufgrund der Verarbeitung der *BenutzerID* findet eine Verarbeitung von personenbezogenen Daten statt, für welche auf den ersten Blick kein Rechtfertigungsgrund ersichtlich ist. Gemäß Kapitel 3.4 iVm Kapitel 4.1.1 ist nur eine sehr eingeschränkte Berücksichtigung eines berechtigten Interesses des Websitebetreibers bei der Anwendung von § 96 Abs 3 TKG möglich, und dieses soll noch dazu auf technisch motivierte Rechtfertigungsgründe eingeengt werden. Gegenstand der Interessensabwägung wäre hier: Auf der einen Seite der Schutz vor Identitätsdiebstahl – dieser liegt im beiderseitigen Interesse. Auf der anderen Seite ein zusätzlicher Eingriff in die Privatsphäre des Nutzers, der

[224] Voraussetzung: Die eingegebenen Authentifizierungsinformationen (*username, password*) sind korrekt.

bereits durch die zusätzliche Verarbeitung von personenbezogenen Daten erfolgt und iA auch das Risiko für die Verknüpfung mit der realen Identität des Benutzers erhöht.

Es soll davon ausgegangen werden, dass der Websitebetreiber die *reale* Identität der Person bereits kennt, also eine Registrierung des Benutzers mit seinen tatsächlichen Stammdaten (zB Name, Adresse) bereits stattgefunden hat. Nur diese reale Identität soll vor Identitätsdiebstahl geschützt werden, aber keine etwaige *Fake-Identität*. Die zusätzliche Verarbeitung von personenbezogenen Daten durch den Cookie erhöht daher für den Benutzer nicht das Risiko der Verknüpfung mit seiner realen Identität – letztere ist nämlich annahmegemäß bereits bekannt. Die zusätzliche Datenverarbeitung, die durch Abspeichern und Auslesen des Cookies verursacht wird, ist daher mit Bezug auf die geforderte Interessensabwägung nur gegen das Minimalprinzip des Datenschutzes „aufzurechnen". Dabei muss auch Berücksichtigt werden, dass auf Seiten des Benutzers ebenfalls ein unmittelbarer Nutzen entsteht, nämlich der Schutz vor Identitätsdiebstahl. Das Risiko der Bestimmbarkeit des realen Benutzers steigt hingegen nicht. Der Websitebetreiber hat jedenfalls ein Interesse daran, sich selbst vor den negativen Folgen eines Identitätsdiebstahles seiner Benutzer zu schützen. Dieses Interesse ist berechtigt und es gibt kein überwiegendes, entgegenstehendes Interesse auf Seiten der Benutzer. Der Websitebetreiber verfolgt hier einen nachvollziehbaren Zweck und setzt eine verhältnismäßige Maßnahme zu dessen Erreichung. Somit ist sein berechtigtes Interesse ein Rechtfertigungsgrund, der gegen den Wortlaut von § 96 Abs 3 TKG zu berücksichtigen ist.

Zusätzlich gilt: Der Schutz des Webangebots vor Identitätsdiebstahl ist eine „Notwendigkeit zur Vertragserfüllung", jedenfalls im Hinblick auf die Nebenpflichten, die den Benutzern geschuldet werden. Aus dieser vertraglichen Notwendigkeit ergibt sich über den Umweg der Cookie Technologie - als geeignetes, technisches Verfahren - auch eine technische Notwendigkeit der Datenverarbeitung für die Zurverfügungstellung des Dienstes und somit eine direkte Subsumption unter den Ausnahmetatbestand § 96 Abs 3 Satz 3 TKG[225]. Die Anerkennung als Notwendigkeit zur Vertragserfüllung hat den folgenden Vorteil: Sofern der Websitebetreiber in seinen Nutzungsbedingungen auf die gegenständliche Identifikationsmethode hinweist, kann er sich auf diese Vertragserfüllung berufen und damit einem Nutzer, der dieser Identifikationsmethode nicht zustimmt, das komplette Webangebot verweigern. Diese Schlussfolgerung geht aus § 96 Abs 3 Satz 2,3 TKG nicht direkt hervor, entspricht aber einem allgemeinen Gedanken des Datenschutzrechts: Die Einordnung der Datenverarbeitung unter den gesetzlichen Rechtfertigungstatbestand der „Vertragserfüllung" schließt nämlich das Betroffenenrecht des Widerspruchs iSv Art 21 DSGVO aus.

Im Ergebnis gibt es somit einen gesetzlichen Erlaubnistatbestand für den Einsatz des Cookies zum oben genannten Zweck und somit kein Einwilligungserfordernis für den gegenständlichen Anwendungsfall.

[225] Im Volltext: „Die Datenverarbeitung ist unbedingt erforderlich für die Zurverfügungstellung eines Dienstes der vom Benutzer ausdrücklich gewünscht wurde".

zu b) Das Ergebnis der rein technischen Betrachtung aus Kapitel 3.2.3 war, dass der Einsatz von *device fingerprinting* nur dann zu einer Verarbeitung personenbezogener Daten führt und daher potentiell einer Einwilligungspflicht unterliegt, wenn zusätzliche Elemente abgespeichert werden, welche Rückschlüsse auf die reale Identität des Benutzers erlauben. Dies könnte sich dadurch ergeben, dass serverseitig gemeinsam mit der *device fingerprint* ID auch die IP Adresse des Nutzers abgespeichert wird[226]. Sobald serverseitig eine Verbindung dieser beiden Datensätze fix existiert oder nach allgemeinem Ermessen die Verbindung wahrscheinlich hergestellt werden wird – zB im Zuge von manuellen Recherchen durch den Systemadministrator – muss man die *device fingerprint* ID als zusätzliche Information über den durch die IP Adresse bestimmbaren Benutzer ansehen. Alleine das Führen des *HTTP Access Log* genügt dafür aber nicht – Der Betreiber könnte über technische und organisatorische Maßnahmen sicherstellen, dass eine Verbindung dieser beiden Datensätze nicht möglich bzw nicht mit vertretbarem Aufwand möglich ist. Für eine effiziente Abwehr von Hackingangriffen im Rahmen des hier beschriebenen Anwendungsfalles wird man serverseitig aber nicht auf das zusätzliche Identifikationselement IP Adresse verzichten wollen. Diese liefert unter Berücksichtigung der historischen Zugriffe wichtige Hinweise darauf, ob ein unautorisierter Zugriff auf den Benutzeraccount gerade versucht wird, zB über die geographische Aussagekraft der IP Adresse oder durch die relative Häufigkeit von Zugriffen von einer und derselben Quell-IP Adresse. Im Gegensatz zu anderen Anwendungsfällen würde die Wirksamkeit dieser Schutzmaßnahme beeinträchtigt werden, falls die IP Adresse in verkürzter – und damit wirksam anonymisierter – Darstellung abgespeichert wird. Im Vergleich zur Betrachtung unter a) muss aber festgehalten werden, dass die IP Adresse ein deutlich kritischeres, weil direkter verknüpftes Datum mit dem jeweiligen Benutzer ist als die serverseitig vergebene *BenutzerID* im Rahmen des Cookies. Für die Erstellung eines aussagekräftigen Profils von (unverdächtigen) Quell-IP Adressen wird man eine jahrelange Speicherung aller Zugriffe weder benötigen noch rechtfertigen können. Im Sinne der Datensparsamkeit ist die Anzahl der historischen Daten daher zu begrenzen. Unter dieser Voraussetzung und unter Beachtung der Informationspflichten kann dennoch auf die Argumentation der Rechtfertigungsgründe unter a) zurückgegriffen werden, also sowohl „berechtigtes Interesse“ als auch „Vertragserfüllung“. Dies gilt jedenfalls solange die Schutzmaßnahme auf den Schutz der einzelnen Benutzeraccounts ausgerichtet ist und nicht der generelle Schutz der Verfügbarkeit des Systems das Ziel der Maßnahme ist.

4.5.5 Einwilligungserfordernis (beurteilt anhand der ePrivacy VO)

Das Einwilligungserfordernis wird anhand von Art 8 ePrivacy VO beurteilt und zwar unter Anwendung der Interpretationen der *Art-29-Datenschutzgruppe* (vgl Kapitel 3.6.2) zu

[226] Vgl Kapitel 2.2.

Art 5 Abs 3 RL 2009/136/EG. In dieser Interpretation werden „User centric security cookies", welche die Sicherheit des vom Benutzer angeforderten Webservices erhöhen, ähnlich den Argumentationen im vorangegangenen Kapitel, als technische Notwendigkeit zur Vertragserfüllung eingestuft und mit dieser Begründung ein Einwilligungserfordernis verneint. Eine Unterscheidung zwischen den Technologien *HTTP Cookie* und *device fingerprinting* ist auf Basis der ePrivacy VO nicht mehr erforderlich (vgl Kapitel 3.6.3). Im Zuge des Gesetzgebungsprozesses der ePrivacy VO wird eine auf diesen Anwendungsfall gerichtete ausdrückliche Ausnahmeregelung in Art 8 Abs 1 ePrivacy VO diskutiert[227].

4.6 Direct Carrier Billing mittels MSISDN Forwarding

4.6.1 Kurzbeschreibung des Anwendungsfalls

Verglichen mit den vorherigen Anwendungsfällen wird nun ein 3-Parteien Verhältnis betrachtet, denn der Access-Provider des Benutzers – hier annahmegemäß ein Mobilfunkprovider – übernimmt nun ebenfalls eine funktionale Rolle im Prozess der Identifikation und Wiedererkennung. In diesem Anwendungsfalls soll dem Kunden die Möglichkeit geboten werden, per „1-Click" eine Zahlung bei einem Websitebetreiber zu leisten, welche letztlich dann vom Access-Provider gegenüber dem Kunden über dessen Telefonrechnung eingehoben wird (vgl technische Beschreibung zum *MSISDN Forwarding* in Kapitel 2.3). Annahmegemäß wird die MSISDN des Anschlussinhabers im *HTTP header* der Kommunikation in Form eines Pseudonyms an ausgewählte Partnerwebsites, mit welchen der Mobilfunkbetreiber entsprechende Verträge abgeschlossen hat, übermittelt. Der Mobilfunkbetreiber verwendet iA für ein und denselben Kunden unterschiedliche Pseudonyme für unterschiedliche Partnerwebsites.

4.6.2 Datenschutzrechtliche Rollenzuteilung

Ein Auftragsverarbeitungsverhältnis zwischen Mobilfunkanbieter und Websitebetreiber kann nicht angenommen werden. Dagegen spricht schon die Einteilung des Websitebetreibers als Drittanbieter gemäß § 3 Z 4a TKG. Der Kunde fordert einen vom Mobilfunkbetreiber augenscheinlich unabhängigen Dienst des Drittanbieters an. Die Zahlung wickelt zwar der Mobilfunkbetreiber „im Auftrag" des Drittanbieters ab, da aber der Mobilfunkbetreiber das zur Identifikation notwendige Pseudonym erstellt, verwaltet, in den Datenstrom eingefügt und letztlich gegen die Kundendatenbank auflöst, ist er Verantwortlicher gemäß den Datenschutzgesetzen. Beim *Direct Carrier Billing* ist im Moment der Rechnungsstellung immer eine De-Pseudonymisierung, also die Auflösung des Pseudonyms gegen die tatsächlichen Stammdaten des Anschlussinhabers, notwendig.

[227] Diskussionspapier 10975/18 der EU Rat Arbeitsgruppe WP TELE vom 10. Juli 2018 , <www.parlament.gv.at/PAKT/EU/DIR/index.shtml?FART=INT&FZAHL=0003&JAHR=2017&TYP=COD>.

Die dargestellte Konstellation könnte allerdings auf eine „gemeinsame Verantwortung“ gemäß Art 26 DSGVO hinweisen. Eine gemeinsame Verantwortung muss nicht notwendigerweise bereits bei der Erhebung der Daten begründet werden. Auch eine *nachträgliche* Begründung der gemeinsamen Verantwortlichkeit ist möglich[228] und wäre aus einer technischen Sichtweise hier eher zutreffend. Die Konstruktion der gemeinsamen Verantwortlichkeit erfordert jedenfalls, dass die in Art 26 DSGVO normierten Minimalvereinbarungen zwischen den beiden Entitäten – im speziellen mit Bezug auf die Betroffenenrechte – vertraglich festgehalten sind. Dies wäre nur anhand einer Einzelfallbeurteilung zu beurteilen und kann hier ohne Kenntnis der Verträge nicht durchgeführt werden. Für die folgende Beurteilung kann die Klassifikation der „gemeinsamen Verantwortung“ aber gegebenenfalls offen bleiben. Das ist dann der Fall, wenn kein Zweifel daran besteht, dass beide Entitäten personenbezogene Daten verarbeiten und somit die entsprechenden, zweckbezogenen Interessensabwägungen für beide Entitäten getrennt durchgeführt werden können.

Zum derzeitigen Stand der Untersuchung wurde noch nicht die Frage beantwortet, ob die pseudonymisierte MSISDN auch für den Drittanbieter ein personenbezogenes Datum darstellt oder nicht. Diese Antwort ist jedoch einfach zu geben, und zwar mit zwei Begründungen. {Erstens}: Nach der oben ausgearbeiteten *Theorie über die Verkettung der pseudonymisierten IP Adresse* ergibt sich hier kein anderes Ergebnis als bei der *HTTP Cookie* Technologie unter Einsatz eindeutiger *BenutzerIDs*. Und außerdem, {zweitens}, gibt es in der hier besprochenen Realisierung nun sehr wohl eine jeweils aktuelle Zuordnung in Form einer Liste, welche die De-Pseudonymisierung der MSISDN und damit die Zuordnung zu den tatsächlichen Stammdaten des Benutzers bzw des Anschlussinhabers erlaubt. Diese Liste wird vom Access-Provider und nicht vom Websitebetreiber („der Dritte“) geführt, jedoch gibt es zwischen diesen beiden Entitäten ein aufrechtes Vertragsverhältnis über die Nutzung des Pseudonyms. Selbst wenn in diesem Vertrag die De-Pseudonymisierung durch den Dritten per Vereinbarung ausgeschlossen wird, so gibt es dennoch ein Naheverhältnis zwischen den beiden Unternehmen, welches in besonderen Situationen (Man denke an Vertragsstreitigkeiten, gerichtliche Verfahren, technische Notsituationen, Insolvenzfälle, uÄ) möglicherweise zu besonderen Maßnahmen führt, die eine – wenn auch nur teilweise – De-Pseudonymisierung ermöglichen. Streng genommen müssten hier auch die technischen Möglichkeiten erörtert werden, ob der Websitebetreiber eigenständig die Rückrechnung der Pseudonyme auf die jeweilige MSISDN vornehmen kann, zB durch eine *Brute-Force-Attacke* auf die Hashfunktion der übermittelten Pseudonyme[229]. Eine endgültige Entscheidung zur Argumentation {zweitens} soll der Einzelfallbeurteilung vorbehalten bleiben. Jedenfalls ist über die Argumentation {erstens} ein Personenbezug des Pseudonyms auf Seiten des

[228] *Spoerr* in *Brink/Wolff* DSGVO Art 26 Rn 24.
[229] VG Bayreuth 8.5.2018, B 1 S 18.105 = BeckRS 2018, 9586 Rn 8.

Dritten gegeben. Auf eine mögliche Konstruktion einer gemeinsamen Verantwortung muss nicht eingegangen werden.

4.6.3 Datenschutzrechtliche Einordnung der technischen Verarbeitungsvorgänge

Bei der erstmaligen Erstellung der partnerspezifischen Pseudonyme findet ein sequentieller Lesezugriff auf die Stammdaten aller Kunden des Access-Providers statt. Ebenso erfolgt bei der Auflösung des Pseudonyms im Zuge der Rechnungsausstellung ein Zugriff auf den jeweiligen Stammdatensatz des Kunden. Das Pseudonym ist im Zuge der Übermittlung an den Websitebetreiber als Verkehrs- und Zugangsdatum einzustufen – und zwar für beide Beteiligte. Somit gibt es im Prozess mehrere Verarbeitungsschritte von personenbezogenen Daten, für die eine Zulässigkeitsprüfung zu erfolgen hat.

4.6.4 Einwilligungserfordernis (de lege lata)

Beurteilt für den Access-Provider: Weder für das Erzeugen des Pseudonyms noch für dessen Auflösen ist ein Rechtfertigungsgrund aus § 97 Abs 1 TKG (Stammdaten) ableitbar. Insbesondere betrifft der Erlaubnistatbestand von Z 2 dieser Regelung nur die *Entgelte*, die zur Bereitstellung des Kommunikationsdienstes anfallen, aber nicht Entgelte aus darüberhinausgehenden Drittleistungen. Für das Pseudonym als Verkehrsdatum ergibt sich eine ähnliche Situation, denn hier ist der spezielle Erlaubnistatbestand in § 99 Abs 2 TKG noch eindeutiger formuliert: Nur die Speicherung von „Verkehrsdaten die zur Verrechnung von Endkundenentgelten erforderlich sind“ ist erlaubt. Eine anonymisierte Speicherung wäre zwar erlaubt, jedoch ist das Pseudonym kein anonymes Datum.
Bezogen auf den Access-Provider liegt es nahe, *Direct Carrier Billing* als einen „Dienst mit Zusatznutzen“ gemäß § 92 Abs 3 Z 9 TKG einzuordnen. Charakteristisch dafür ist die Verarbeitung von Verkehrsdaten über die Notwendigkeit zur Kommunikationsdiensterbringung hinaus. Problematisch erscheint hier jedoch, dass aus diesem Dienst kein direkter Nutzen gezogen wird, sondern lediglich die Abrechnung eines anderen Dienstes bereitgestellt wird. Insbesondere ist die Bezahlung der Drittleistung auch nicht der „vom Benutzer ausdrücklich angeforderte Dienst“, denn die Bezahlung kann nach der allgemeinen Zivilrechtsdogmatik nicht als das identitätsstiftende Element des Leistungsaustausches angesehen werden. Fraglich ist, ob die Einordnung als „Dienst mit Zusatznutzen“ überhaupt zu einer unterschiedlichen Beurteilung des Einwilligungserfordernisses führt. § 99 Abs 4 TKG statuiert dazu, dass eine „Zustimmung“ des Teilnehmers zur Verarbeitung der betroffenen Verkehrsdaten für die Erbringung des Dienstes mit Zusatznutzen ausreichend ist. Da der Begriff *Zustimmung* im Gesetz nicht näher ausgeführt ist, könnte man von einer erleichterten Zustimmung, zB auch in AGBs des Access-Providers ausgehen[230]. Da es sich bei den hier verarbeiteten Daten allerdings um

[230] *Riesz* in *Riesz/Schilchegger* TKG § 99 Rn 37.

personenbezogene Daten handelt, und da es – konkret auf unionsrechtlicher Ebene - keine Hinweise auf eine Erleichterung des Einwilligungserfordernisses in diesem konkreten Fall gibt[231], führt die Einordnung von *Direct Carrier Billing* als „Dienst mit Zusatznutzen" zu keiner Abweichung bei der Beurteilung des datenschutzrechtlichen Einwilligungserfordernisses.
Auch aus § 96 Abs 1,2,3 TKG ergibt sich keine Zulässigkeit für die Verarbeitung des Pseudonyms als Verkehrs- bzw Stammdatum, und zwar aus folgender Begründung: Es gibt keine erkennbare technische Notwendigkeit für die Erbringung eines vom Benutzer explizit angeforderten Dienstes. Auch die Rechtfertigung der Vertragserfüllung greift nicht – geschuldet wird nur die Erbringung des Kommunikationsdienstes. Daher ist letztlich von einem Einwilligungserfordernis für den gegenständlichen Anwendungsfall auszugehen. Die Einwilligung kann beispielsweise auf dem self-service Portal des Mobilfunkproviders erteilt werden. Eine Opt-Out Lösung, wie sie heute zT praktiziert wird[232], kann hingegen nicht ausreichend sein! Um die Informationspflichten der Datenschutzgesetzgebung zu erfüllen muss für den Benutzer jedenfalls ersichtlich sein, an welche Partner-Websites das Pseudonym nach seiner Einwilligung übermittelt wird. Einzeleinwilligungen zur Übermittlung an jede einzelne Partner-Website sind nicht einzufordern, da der Benutzer erst durch den gezielten und von ihm selbst hervorgerufenen Besuch der jeweiligen Partner-Website die Übermittlung des Pseudonyms verursacht.

Beurteilt für den Drittanbieter: Falls die Anforderungen an die Informiertheit der Einwilligung im Zuge der Abgabe gegenüber dem Mobilfunkanbieter eingehalten werden, ist davon auszugehen, dass die erteilte Einwilligung auch die Zulässigkeit der Datenverarbeitung auf Seiten des Drittanbieters mitumfasst. Dies könnte auch, je nach vertraglicher Ausgestaltung, letztlich in Form einer *gemeinsamen Verantwortlichkeit* gesehen werden. Wichtig ist allerdings, dass die Einwilligung *vor* der eigentlichen Nutzung des Bezahldienstes abgefragt wird: Dies ist insofern wichtig, da das *MSISDN Forwarding* iA bei jedem Besuch der Partner-Website stattfindet und nicht erst im Moment des Bezahlungsvorganges. Aus diesem Grund ist eine „on demand" Einwilligung gegenüber dem Websitebetreiber, die während des Bezahlvorganges eingeholt wird und die Datenübermittlung ex post rechtfertigt, iA als unzulässig einzustufen. Das liegt auch daran, dass die Erstellung der Pseudonyme auf Seiten des Access-Providers ein technisch komplexer Prozess ist, der iA aus technischen Gründen bereits vor der ersten Kontaktaufnahme des Benutzers mit der Partner-Website erfolgt.

Durch Recherche im Internet sowie nach persönlichen Gesprächen mit Vertretern aus den technischen Abteilungen von zwei Mobilfunkanbietern kann festgehalten werden, dass der Einsatz dieser Technologie ihren Höhepunkt überschritten hat und mehr und mehr Mobilfunkanbieter diese Praxis beenden bzw beenden wollen. Neben den

[231] AaO.
[232] Quelle: <www.rtr.at/de/tk/TKKS_BezahlenmitdemHandy>

datenschutzrechtlichen Problematiken, wie sie in dieser Arbeit dargestellt wurden, gibt es auch technische Schwierigkeiten in Verbindung mit dem Trend zu verschlüsselten Kommunikationsverbindungen im WWW. *Direct Carrier Billing* wird vermehrt durch andere Technologien realisiert, bei denen durch eine tiefere Integration zwischen dem Websitebetreiber und dem Mobilfunkanbieter im Moment des Bezahlvorgangs über *SessionIDs* und sogenannte *tokens* eine Verbesserung in datenschutzrechtlicher Hinsicht erzielt werden soll[233]. Damit einher geht der Trend, den Benutzer besser zu informieren und in erhöhtem Maße persönliche Einwilligungen für die Benutzung solcher Zusatzdienste einzufordern.

4.6.5 Einwilligungserfordernis (beurteilt anhand der ePrivacy VO)

Der Kommissionsentwurf sieht nur wenige Möglichkeiten vor, in denen Metadaten welche nicht für die unmittelbare Zurverfügungstellung des abgerufenen Dienstes technisch notwendig sind, verarbeitet werden dürfen. In Art 6 Abs 2 lit b ePrivacy VO gibt es einen Erlaubnistatbestand für die Verarbeitung von Metadaten zum Zwecke der Verrechnung. Doch auch diese Regelung muss auf die Verrechnung von Kommunikationsdienstleistungen beschränkt bleiben und kann nicht ohne weiteres auf die Verrechnung von Drittleistungen ausgedehnt werden. Auch die Ausnahmebestimmungen für TSM-VO konforme Verkehrsmanagementmaßnahmen (siehe Kapitel 3.3.4) in Art 6 Abs 2 lit a führen hier zu keiner Ausnahme vom generellen Einwilligungsvorbehalt, da es sich nicht um eine Verkehrsmanagementmaßnahme handelt.

4.7 Personalisierte Online Werbung mithilfe von *behavioral targeting*

4.7.1 Kurzbeschreibung des Anwendungsfalls

Verglichen mit den zuvor behandelten Anwendungsfällen kommt nun eine komplett neue Drittpartei ins Spiel, und zwar der Betreiber des sogenannten AdNetworks[234]. In bestimmten Ausprägungsformen sind nun sogar vier Parteien involviert, nämlich dann, wenn der Access-Provider des Benutzers ebenfalls Teil der zweckgerichteten Datenverarbeitungskette ist.
Beim *behavioral targeting* werden bei der Darstellung der einzelnen Webseiten für den Benutzer personalisierte Werbebotschaften (sogenannte Werbebanner) eingeblendet, die sich thematisch auf die Inhalte bzw Websites beziehen, die der Benutzer in der Vergangenheit besucht hat. Teilweise werden auch die vom Benutzer getätigten Interaktionen mit diesen Websites (zB eingegebene Suchbegriffe, *clickstreams*, gekaufte Produkte) miteinbezogen[235]. Eine spezifische Ausprägung dieser Werbeform ist das

[233] Eine neuere, von der Mobilfunkindustrie weltweit getriebene Authentifizierungslösung ist bspw *Mobileconnect* <www.mobileconnect.io>.
[234] Einige bekannte Unternehmen/Produkte auf diesem Gebiet sind: *Criteo, AdRoll, Google Adsense, Clicksor, nugg.ad, ClickAd, DoubleClick, Yahoo Publisher Network, Adobe Advertising Cloud,* etc.
[235] Vgl *Schirmbacher,* Online-Marketing, Kapitel 7.3.5.

sogenannte *retargeting*: Dabei wird ein einmal betrachtetes aber nicht gekauftes Produkt über mehrere Stunden und Tage hinweg auf besonders vielen - von der ursprünglichen Website unabhängigen – anderen Websites individuell als Werbebotschaft eingeblendet[236]. Es geht beim *retargeting* also darum, den einzelnen Internetbenutzer mit einer bestimmten Werbebotschaft zu „verfolgen". Ein solches Ausspielverhalten von Werbung ist nur möglich, wenn ein Datenaustausch zwischen den unterschiedlichen Websites stattfindet. Genau dafür sorgt das AdNetwork.

4.7.2 Datenschutzrechtliche Rollenzuteilung

Die Rollenverteilung zwischen dem Websitebetreiber und dem AdNetwork im Hinblick auf die Verarbeitung der personenbezogenen Daten wurde in der rechtswissenschaftlichen Literatur kontroversiell diskutiert. Weitgehend unstrittig war dabei, dass das AdNetwork, sofern es über personenbezogene Daten verfügt, als Verantwortlicher im Sinne der Datenschutzgesetzgebung anzusehen ist[237]. Das AdNetwork markiert nämlich den Benutzer, zB über einen *Third-Party* Cookie mit einer *BenutzerID,* und speichert die darauf folgenden Internetaktivitäten des Benutzers serverseitig als Liste ab (sogenanntes *tracking)*. Strittig war hingegen die Rolle des Websitebetreibers – er wurde vereinzelt von Autoren als datenschutzneutral qualifiziert[238]. Begründet wurde dies mit der fehlenden Einflussnahme auf die übertragenen Daten sowie der grundlegenden Definition des *Verantwortlichen* – er müsse Daten für sich selbst erheben oder verarbeiten. Demgegenüber vertrat die *Art-29-Datenschutzgruppe* schon im Jahr 2010 in der beschriebenen Konstellation das Konzept einer *geteilten Verantwortung*, und zwar mit folgender Begründung: Es gibt eine kausale Verursachung der Datenübertragung zwischen dem Benutzer und dem AdNetwork durch den Websitebetreiber, indem letzterer die dynamische Umleitung des Endgeräts in Richtung des AdNetworks willentlich durch die Programmierung seiner Website herbeiführt - Für den Benutzer ist diese Umleitung weder transparent noch gewollt[239]. Diese Begründung ist technisch nicht zu beanstanden, erscheint aber im Hinblick auf die wörtliche Definition des *Verantwortlichen* nur bedingt überzeugend. Erst in einer Gesamtbetrachtung des Zusammenspiels zwischen dem Websitebetreiber und dem AdNetwork ist die Annahme der *geteilten Verantwortung* in vertretbarer Weise zu argumentieren: Da wäre zum einen der Vertrag zwischen Websitebetreiber und AdNetwork, der eine klare Aufteilung der Verantwortlichkeiten vorsieht[240]. Verstärkend kommt noch die Tatsache hinzu, dass der Websitebetreiber in seiner Programmierung sehr wohl auch direkten Einfluss darauf nimmt, mit welchen Daten (zB Produktbezeichnungen und andere spezifische

[236] *Venzke-Caprarese,* DuD 9/2017, 577 (577).
[237] AaO; *Forgó/Helfrich/Schneider*, Betrieblicher Datenschutz² (2014) Teil VIII Kap 4 Rn 94 f.
[238] Stellvertretend: *Voigt/Alich,* Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber, NJW 2011, 3541 (3542).
[239] *Art-29-Datenschutzgruppe*, WP171, 11.
[240] Stellvertretend hierzu das entsprechende Vertragswerk von *Google Adsense:* <www.google.com/adsense/new/localized-terms?hl=de>.

Erkennungsmerkmale) die personenbezogenen Daten des Benutzers auf Seiten des AdNetworks verknüpft werden[241]. Mittlerweile haben auch die Anbieter von AdNetworks das Konzept der *gemeinsamen Verantwortung* angenommen[242] und die Rechtsfigur fand auch Einzug in die DSGVO (Artikel 26). Derzeit ist ein EuGH Vorabentscheidungsverfahren anhängig, welches in dieser Frage eine endgültige Aussage erwarten lässt[243]. In diesem Verfahren gibt es zwar noch kein Ergebnis, jedoch kann die Entscheidung *Wirtschaftsakademie Schleswig-Holstein*[244] bereits stand heute als Indikator für die Etablierung des Konzepts *geteilte Verantwortung* in der vorliegenden technischen Realisierungen gesehen werden – Generalanwalt *Yves Bot* hat in seinem Schlussantrag zu C-210/16 auch schon die Gemeinsamkeiten beider Verfahren herausgestrichen.

In der Praxis vereinbaren der Websitebetreiber und das AdNetwork eine Aufteilung der Pflichten, vor allen der Informationspflichten und der Betroffenenrechte – dies geht soweit, dass der AdNetwork-Betreiber auch konkrete Vorgaben für die Datenschutzhinweisseite des Websitebetreibers macht. Das AdNetwork ist ebenfalls ein Dienst der Informationsgesellschaft gemäß Art 3 Z 1 ECG und damit ist § 96 Abs 3 TKG der maßgebliche Beurteilungsmaßstab für die datenschutzrechtlichen Aspekte de lege lata.

Falls bei der Umsetzung dieses Anwendungsfalles auch noch der Access-Provider involviert ist, zB im Zuge des Einsatzes von *MSISDN forwarding*, gilt mit Verweis auf Kapitel 4.6: Der Access-Provider verarbeitet jedenfalls personenbezogene Daten und ist nicht als Auftragsverarbeiter einzustufen.

4.7.3 Datenschutzrechtliche Einordnung der technischen Verarbeitungsvorgänge

Die folgenden Technologien zur Identifikation und Wiedererkennung des Endgeräts können zum Einsatz kommen:

a) *Third-Party HTTP Cookie* mit clientseitig gespeicherter Referenznummer (*BenutzerID*), gesetzt und verwaltet durch das AdNetwork
b) *Third-Party HTTP Cookie* ohne clientseitig gespeicherte Referenznummer
c) *Device fingerprinting*
d) *MSISDN forwarding*

Die Wiedererkennung wird einerseits dazu benutzt, um das bereits vorhandene Nutzerprofil durch weitere Informationen aus der aktuellen Benutzerinteraktion anzureichern. Der Hauptzweck ist allerdings, in Echtzeit die einzublendende Werbebotschaft passend zu dem Nutzerprofil auszuwählen. Zusätzlich wird iA auch festgehalten, ob ein Benutzer auf eine konkrete Werbebotschaft geklickt hat und über das sogenannte *frequency capping* wird

[241] AA *Martini* in *Paal/Pauly* DSGVO Art 26 Rn 19.
[242] Stellvertretend: aaO; *Criteo* <www.criteo.com/insights/gdpr-need-know-criteo>.
[243] EuGH C-40/17 (*Fashion ID*).
[244] EuGH 5.06.2018, C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*).

protokoliert, wie oft ein und derselbe Benutzer ein und dieselbe Werbungeinblendung zugeteilt bekommen hat.

4.7.4 Einwilligungserfordernis (de lege lata)

zu a) Ob *behavioral targeting* eine Direktwerbung iSd DSGVO ist[245], muss nicht entschieden werden, denn die Rechtfertigung über ErwgGr 47[246] DSGVO iVm Art 6 Abs 1 lit f DSGVO steht wegen der vorrangigen Anwendung des TKG ohnehin nicht unmittelbar offen. Gemäß Kapitel 3.4 iVm Kapitel 4.1.1 ist nur eine sehr eingeschränkte Berücksichtigung eines berechtigten Interesses des Websitebetreibers bei der Anwendung von § 96 Abs 3 TKG möglich, und dieses soll noch dazu auf technisch motivierte Rechtfertigungsgründe eingeengt werden. § 96 Abs 3 TKG fordert für eine Ausnahme zum Einwilligungserfordernis wörtlich: „unbedingt erforderlich für die Zurverfügungstellung eines Dienstes, den der Benutzer ausdrücklich gewünscht hat". Teile der österreichischen Literatur[247] verweisen nun auf die Auslegung zur Richtlinie 2009/136/EG durch die *Art-29-Datenschutzgruppe*[248], aber auch eine direkte Wortinterpretation von § 96 Abs 3 TKG kann zu keinem anderen Ergebnis kommen: Der vom Benutzer ausdrücklich aufgerufene Dienst ist die Darstellung der Website des Websitebetreibers. Selbst wann man die eingebundene Werbung als Teil der Webseite auffasst, so ist für deren Darstellung dennoch keine Verarbeitung von personenbezogenen Daten *unbedingt erforderlich*. Für eine Erweiterung der Ausnahmebestimmung über ihren Wortlaut hinaus gibt es hinsichtlich des Zwecks *behavioral targeting* keine Notwendigkeit. Somit ergibt sich ein Einwilligungserfordernis für die Realisierung dieses Anwendungsfalls mit der *HTTP Cookie* Technologie. Das Einwilligungserfordernis ist auch unabhängig davon, ob das AdNetwork Quell-IP Adressen in Klartext bzw in verkürzter/anonymisierter Form speichert[249] oder nicht.

Die Konstruktion der gemeinsamen Verantwortlichkeit von AdNetwork und Websitebetreiber führt dazu, dass bei den heute in der Praxis auftretenden Webangeboten im Zweifelsfall folgendes anzunehmen ist: Die Einwilligungserklärung eines Benutzers gilt nur für die konkrete Kombination der beiden Erklärungsadressaten, also demnach nur für das Sammeln und Auswerten des Nutzerprofils auf der vom Benutzer aufgerufenen Website. Solange der AdNetwork Betreiber nicht direkter und transparenter mit dem Internetbenutzer in Interaktion tritt – zB über seine eigene Website oder über zentralisierte Consentmanagement-

[245] Dagegen: *Feiler/Horn,* DSGVO Praxis, 188; Dafür: *Schleipfer,* ZD 2017, 460. Der Kommissionsentwurf Art 4Abs 13 lit f ePrivacy VO iVm ErwGr 32 klassifiziert *Online Behavioral Targeting* als Direktwerbung, allerdings nach dem Wortlaut nur dann, wenn das Ziel für die Werbebotschaft eine *identifizierte* oder *identifizierbare* Person ist.

[246] Aus dem Volltext: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden".

[247] *Riesz* in *Riesz/Schilchegger* TKG § 96 Rn 48 ff; *Pachinger,* Aktuelles zur datenschutzrechtlichen Zustimmung beim Online-Targeting, jusIT 2012/84, 175.

[248] *Art-29-Datenschutzgruppe*, WP194, Kapitel 3 & 4.

[249] Vgl Fußnote 83.

Platformen[250] - wird man eine generelle, Website-übergreifende Einwilligung für das *tracking* des Internetbenutzers über alle am Werbenetzwerk teilnehmenden Websites kaum annehmen können[251]. Zukünftig erscheint es aber durchaus denkbar, dass sich bei einer höheren Standardisierung, sowohl auf der technischen als auch auf der vertraglichen Ebene, verbunden mit mehr Transparenz in Richtung der Internetbenutzer, diese Möglichkeit eröffnet.

zu b) Das Ausspielen von personalisierter Werbung ist auch über *non-ID Cookies* möglich. Es gibt auch Anbieter von AdNetworks, zB das Unternehmen *Nugg.ad*, die diese Methode nutzen[252]. *Nugg.Ad* hat ca. 10 diskrete Interessensgebiete (zB Auto, Fashion, Gesundheit) und in diesen Gebieten noch 5-10 weitere Unterklassifizierungen definiert. Bei jedem Besuch einer Website, die mit der Technologie von *Nugg.ad* ausgestattet ist, wird das betroffene Themengebiet in einem clientseitig gespeicherten *non-ID Cookie* hinterlegt. Über einen bestimmten Beobachtungszeitraum ergibt sich somit über die Auswertung der jeweils besuchten Themengebiete und der entsprechenden Häufigkeiten des Besuchs ein Interessensprofil des Nutzers. Dieses verbleibt lokal auf seinem Endgerät gespeichert, wird aber bei jedem Besuch einer entsprechenden Website in Echtzeit ausgelesen und dafür benutzt, eine spezifische Werbeanzeige einzublenden. Laut eigener Aussage speichert *Nugg.ad* serverseitig keine IP Adressen ab und verwendet bereits für die Entscheidung, ob eine Werbung an einen bestimmten Benutzer einer Zielregion auszuspielen ist, verkürzte IP Adressen. Durch technische und organisatorische Maßnahmen wird sichergestellt, dass beim Vorgang des Anonymisierens der IP Adressen, welcher für sich genommen eine Verarbeitung von personenbezogenen Daten wäre, keine Rückführbarkeit möglich ist. Der Anonymisierungsdienst wird von einem anderen Unternehmen betrieben. Der Argumentation von Kapitel 3.2.2 folgend, erscheint es auch hier sachgerecht, diese Art der Verarbeitung von IP Adressen nicht als Verarbeitung personenbezogener Daten zu klassifizieren, denn lediglich das Empfangen und die Auswertung des Inhalts von TCP/IP Paketen ohne Speicherung der IP Adresse soll nicht automatisch zu einem Personenbezug führen. Nach den bisherigen Ergebnissen und Erläuterungen (vgl Kapitel 4.3.4 „Vorhalten von Eingaben/Einstellungen“ – 5. Fall) findet bei dieser Methodik mit Verweis auf die im Cookie gespeicherten Daten aufgrund der fehlenden Bestimmbarkeit der realen Person keine Verarbeitung personenbezogener Daten statt.
Fraglich ist auch hier, ob die komplette Verneinung eines Persönlichkeitsschutzes letztlich sachgerecht ist. Insbesondere im Hinblick darauf, dass die *Art-29-Datenschutzgruppe* den Anwendungsfall von *HTTP Cookies* im Zusammenhang mit personalisierter Werbung explizit

[250] Auf dieser Web-Plattform können Einwilligungen zum *tracking* durch eine Vielzahl von AdNetworks direkt abgegeben und widerrufen werden: <www.youronlinechoices.com/at/praferenzmanagement>.
[251] Vgl dazu diesen Online Beitrag: <digiday.com/marketing/ad-retargeters-trying-work-around-gdpr-apple>.
[252] Unternehmenswebsite: <mtm.nuggad.net/en>.

als zustimmungspflichtig ausweist[253]. Die *Art-29-Datenschutzgruppe* verfolgt dabei eine zweckorientierte Argumentation und erkennt den fehlenden Personenbezug der verarbeitenden Daten als Ausschlussgrund für das Einwilligungserfordernis zur Cookie Verarbeitung nicht an[254]. Das Ergebnis des – zumindest aus technischer Sicht – vergleichbaren Anwendungsfalls aus Kapitel 4.3.4 (5. Fall) war, dass außerhalb des Datenschutzregimes DSGVO/TKG eine Interessensabwägung zwischen den Beteiligten auf Basis des allgemeinen Persönlichkeitsrechts durchgeführt werden kann. Dabei müssen selbstbeschränkende Maßnahmen, wie die eingeschränkte Zahl von Interessensgebieten, die zeitlich eingeschränkte Speicherdauer, sowie technische und organisatorische Maßnahmen zur Verhinderung der Rückführbarkeit in die Interessensabwägung miteinfließen. Die Interessensabwägung muss sich allerdings auf den Websitebetreiber beziehen und nicht auf das AdNetwork. Das liegt daran, dass der Websitebetreiber ursächlich dafür verantwortlich ist, das AdNetwork auf seiner Website einzubinden und er letztlich dem Benutzer gegenüber den Eingriff in dessen Persönlichkeitsrechte rechtfertigen muss. Das AdNetwork hat zwar ein wirtschaftliches Interesse auf möglichst vielen Seiten eingebunden zu werden um seine Datenbasis zu verbessen und damit für andere Websitebetreiber attraktiver zu werden. Es fehlt aber an der Unmittelbarkeit des Aufeinandertreffens zwischen diesem Interesse und dem einzelnen Internetbenutzer und seinem singulär zu beurteilenden Besuch.

Der Websitebetreiber hat jedenfalls ein Interesse, personifizierte Werbung zur Finanzierung seiner Website anzubieten und die gewählte Methodik ist auch geeignet, bessere Click-Raten auf seiner Website zu generieren[255] und somit höhere Werbeerlöse zu erzielen. Auch wenn die technische Sichtweise der Datenverarbeitung und die Art der gespeicherten Daten, zumindest auf den ersten Blick, starke Ähnlichkeiten mit der Analyse aus Kapitel 4.3.4 (5. Fall)[256] haben, so ist die Einschränkung der Persönlichkeitsrechte des Benutzers hier dennoch anders zu bewerten. Und zwar aus folgenden Gründen:

Zunächst ist die Datenerhebung unterschiedlich. Im referenzierten Anwendungsfall aus Kapitel 4.3.4 gibt der Benutzer willentlich und wissentlich sämtliche Daten selbst preis[257] und nur die - für ihn unvorhersehbare - Speicherung in Kombination mit der wiederholten Übermittlung an den Websitebetreiber und daraus resultierender, individualisierter Darstellung ist der Ansatzpunkt für den persönlichkeitsrechtlichen Eingriff. Im referenzierten Anwendungsfall ist die Datenspeicherung als Komfortfunktion des Benutzers aufzufassen, denn bei seiner Wiederkehr sieht der Benutzer die gespeicherten Daten auch wieder – zB

[253] *Art-29-Datenschutzgruppe,* WP171, Kapitel 3.2.2; *Art-29-Datenschutzgruppe,* WP194, Kapitel 4.2.
[254] Vgl Kapitel 3.3.2.
[255] *Nugg.ad* veröffentlicht hier entsprechende Auswertungen: <www.nugg.ad/tl_files/media/w15/Cases/EN/cs_toyota_en.pdf>.
[256] Zu Erinnerung, das Ergebnis aus Kapitel 4.3.4 (5.Fall) war: Im Falle der umfassenden Speicherung von Eingaben, Einstellungen oder *Clickstreams*, welche einen nicht unwesentlichen persönlichen Bezug zu einem nicht bestimmbaren, aber im Zuge seines Wiedererscheinens dennoch ausgesonderten und iA auch anders behandelten Nutzers herstellen, ist eine persönlichkeitsrechtliche Einwilligung auf Basis von §§ 16, 1328a ABGB zu fordern.
[257] Dies gilt streng genommen auch für den sogenannten *clickstream* als Nutzungsprofil.

als Eingabevorschlag in einer Drop-Down Box. Das ist für ihn zwar überraschend, aber zumindest bei seiner Wiederkehr ersichtlich und erkennbar. Im gegenständlichen Anwendungsfall findet hingegen eine versteckte, langwierige „Beobachtung" statt und aus dieser Beobachtung heraus werden gezielt Teilabbilder der Persönlichkeit, nämlich spezifische Interessen, bereits bei der Erhebung zugeordnet. Diese „Beobachtung" findet noch dazu Website-übergreifend statt. Tatsächlich handelt es sich bereits um ein Persönlichkeitsprofil und nicht mehr bloß um ein Nutzungsprofil bzw Nutzerprofil[258]. Im Hinblick auf die Interessen, Neigungen und Gewohnheiten ist die Datenbasis in diesem Anwendungsfall bereits mittels Profiling-Mechanismen vorverarbeitet und angereichert. Das ist potentiell eine stärkere Persönlichkeitsrechteinschränkung iSv §§ 16, 1328a ABGB, und zwar bereits im Zeitpunkt der Speicherung, sowie nochmal verstärkt durch den Akt der Aufbewahrung.

Im Schutzbereich von § 16 ABGB ist das Recht auf freie Selbstbestimmung umfasst. Es umfasst auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden[259]. Bei der hier vorliegenden Methode hat der Benutzer jedoch keinerlei Kenntnis, welche Aspekte seiner Persönlichkeit gesammelt werden und wann und an wen sie übermittelt werden.

Stärker wiegt jedoch, dass im gegenständlichen Anwendungsfall die gespeicherten Daten im Cookie hier für eine im Hintergrund stattfindende, automatisierte Entscheidung benutzt werden, und zwar: „Welchen Werbe-Banner bekommt der Benutzer zu sehen?". Für den Benutzer ist dieser Vorgang überhaupt nicht transparent. Die Entscheidung, welche Werbung angezeigt wird, ist zwar für den Benutzer im Sinne eines Wertungsmaßtabes in analoger Betrachtung zur entsprechenden Regelung in Art 22 DSGVO keine *erhebliche* Beeinträchtigung[260], fließt aber dennoch in die Interessensabwägung mit ein. Die Abwehr gegen bewusste Manipulationen ist in der freien Willensbildung und damit im Schutzbereich von § 16 ABGB[261] enthalten. Dies geht allerdings nicht soweit, dass dem Einzelnen ein Schutz vor unerwünschten, aber wohlmeinenden Ratschlägen bis hin zur Beeinflussung durch fahrlässige Fehlinformationen zugestanden wird[262].

Es darf nicht vergessen werden, dass personifizierte Werbung ja auch zu personifizierten Angeboten führt, indem ein Benutzer spezifische Produktangebote oder auch Rabatte bekommt, die einem anderen nicht zugänglich werden. Dies ist aus dem Gesichtspunkt der Privatautonomie zwar per se unproblematisch, der Idee von Art 22 DSGVO liegt jedoch auch ein Transparenzgebot zugrunde: Die Unkenntnis über die Eingangs- und Beurteilungskriterien, die zu einer spezifischen Entscheidung führen, werden als

[258] Vgl ErwGr 30 gegenüber ErwGr 38 DSGVO.
[259] BVerfG 15.12.1983, 1 BvR 209/83 = NJW 1984, 419 (421).
[260] *Feiler/Forgó* DSGVO Art 22 Rn 4.
[261] *Koch* in *Koziol/Bydlinski/Bollenberger* ABGB § 16 Rn 7.
[262] *Baston-Vogt,* Der sachliche Schutzbereich des zivilrechtlichen allgemeinen Persönlichkeitsrechts (1997) 466.

persönlichkeitsrechtliche Einschränkung eingeordnet. Diese Argumentation ist genauso für den Schutzbereich von § 16 ABGB gültig.

Eine Persönlichkeitsrechtverletzung wurde bereits bei einem ständigen Überwachungsdruck, unabhängig von der eigentlichen Überwachungstätigkeit, angenommen[263]. Dem liegt die Annahme zugrunde, dass die freie Willensbildung des Individuums – ein geschütztes Gut im Rahmen von § 16 ABGB - von der Unkenntnis über Art und Ausmaß seiner Überwachung negativ beeinflusst wird. Eine Entscheidung in Deutschland hat alleine die faktische Möglichkeit genügen lassen, dass der Systemadministrator eines Geräts den ansonsten voll funktionstüchtigen Anonymisierungsalgorithmus abschalten kann – das führe bereits zu einer Persönlichkeitsrechtsverletzung des Beobachteten[264]. Zur Unkenntnis über Ausmaß und Umfang der Überwachung ist demzufolge auch zu zählen, ob die Überwachungstätigkeit in anonymer Form vorgenommen wird oder nicht. Der durchschnittliche Internetbenutzer mit eingeschränktem technischen Hintergrundwissen kann diese Unterscheidung nicht wahrnehmen. Aber auch der technisch versierte Internetbenutzer geht richtig in der Annahme, dass der Betreiber des AdNetworks jederzeit durch Speicherung und Verknüpfung mit der tatsächlichen IP Adresse des Benutzers die Anonymität des Persönlichkeitsprofils auflösen kann. Einen spezialgesetzlichen Schutz gegen diese Maßnahme gibt es nicht[265]. Der Schutz aus dem Datenschutzrecht könnte in bestimmten Situationen hinfällig sein, nämlich wenn der Betreiber eine Rechtfertigung aus einer technischen Notwendigkeit für diese Maßnahme geltend macht[266].

Selbst wenn man, wie hier in der Arbeit vertreten, die Selbstverpflichtung des Betreibers zum Ausschluss der faktischen Auflösung des Personenbezugs als ausreichend anerkennt, kommt man unter der Anerkennung des „gefühlten Überwachungsdrucks“ hier dennoch zu folgendem Ergebnis: Bei einem exzessiven Einsatz der *non-ID Cookie* Technologie, bei der persönlichkeitsrelevante Merkmale gespeichert werden, kann für den hier beschriebenen Anwendungsfall eine Persönlichkeitsrechtsverletzung jedenfalls nicht ausgeschlossen werden. Ein konkretes Ergebnis der Interessensabwägung zwischen dem Internetbenutzer und dem Websitebetreiber soll allerdings an dieser Stelle offen und einer Einzelfallbetrachtung vorbehalten bleiben.

Dennoch sei noch der folgende Hinweis gestattet: Die AdNetwork Betreiber versuchen mittlerweile mehr Transparenz herzustellen. Die Branche folgt einer freiwilligen Selbstregulierung: Die Guidelines der IAB Europe[267] sehen bspw. explizit vor, dass der Benutzer durch Click auf ein kleines Informationssymbol innerhalb des Werbebanners auf eine Website gelangt, die über die Targeting-Methodik und die verwendeten Daten

[263] OGH 28.03.2007, 6 Ob 6/06k = MR 2007, 127 = ÖJZ-LS 2007/52 = Die Presse 2008/14/01 (*Röhsner*).
[264] OLG Berlin 23.07.2015, 57 S 215/14 = NJW-RR 2016, 366.
[265] Den gibt (bzw gab) es hingegeben sehr wohl in § 15 Abs 3 TMG.
[266] Vgl Kapitel 4.1.1.
[267] Das ist der wirtschaftspolitische Dachverband der Onlinewerbebranche: <www.iabeurope.eu>.

aufklärt[268]. Im Rahmen dessen[269] wird auch ein Opt-Out angeboten[270]. Der Benutzer hat unabhängig davon auch die Möglichkeit, die Cookie Einstellungen seines Browsers so anzupassen, dass *Third-Party Cookies* abgelehnt werden. Dies wird aber von den AdNetwork Betreibern teilweise umgangen[271] und diese Umgehung ist nicht durch die freiwillige Selbstregulierung der IAB Europe ausgeschlossen. In der Praxis reduziert sich die strittige Frage somit darauf, ob ein Opt-Out ausreichend sein soll oder eine informierte Einwilligung vorab zu fordern ist – bei Realisierung b) spricht vieles für die erste Option.

zu c) Das Ergebnis der rein technischen Betrachtung aus Kapitel 3.2.3 war, dass der Einsatz von *device fingerprinting* nur dann zu einer Verarbeitung personenbezogener Daten führt und daher potentiell einer Einwilligungspflicht unterliegt, wenn zusätzliche Elemente abgespeichert werden, welche Rückschlüsse auf die reale Identität des Benutzers erlauben. Für den Zweck des *behavioral targeting* ist durchaus denkbar, durch Speicherung der IP Adresse des Internetbenutzers die Treffsicherheit der Wiedererkennung beim Einsatz von *device fingerprinting* zu erhöhen. Unbedingt erforderlich ist es allerdings nicht, denn auch die Speicherung der IP Adresse in verkürzter Form verspricht bereits eine Verbesserung in der Erkennung von *false positives.* Fraglich ist an dieser Stelle daher lediglich, ob ein unterschiedliches Ergebnis verglichen mit a) [mit Personenbezug] bzw b) [ohne Personenbezug] gerechtfertigt ist. Dafür gibt es für die analoge Betrachtung zu a) keinerlei Veranlassung, denn die serverseitige Speicherung sämtlicher Profildaten gemeinsam mit der IP Adresse spricht tendenziell sogar für eine striktere Bejahung des Einwilligungserfordernisses. Bei der Interessensabwägung in analoger Betrachtung zu b) kommt für den Websitebetreiber erleichternd hinzu, dass die Zuordnung zum anonymen Nutzerprofil nicht eineindeutig ist. Erschwerend, und dies ist hier wohl ausschlaggebend, kommt allerdings hinzu, dass der Internetbenutzer sich nur bedingt mit eigenen Mitteln gegen diese Trackingtechnologie wehren kann. Das manuelle Löschen von Cookies bzw das Ablehnen von *Third-Party Cookies* durch die Browsereinstellungen bleibt wirkungslos. Auch ein Wechsel der Webbrowser-Software muss nicht notwendigerweise die Verbindung zwischen dem serverseitigen Nutzerprofil und dem Computer des Benutzers auflösen – intelligente Algorithmen können diese Verbindung möglicherweise wiederherstellen. Beim *active fingerprinting* kommt nocheinmal erschwerend hinzu, dass das Eigentum des Benutzers – sein Computer – quasi als Ausspähwerkzeug gegen ihn selbst gerichtet wird. Auch hier soll die einzelfallbezogene Interessensabwägung auf Basis des allgemeinen Persönlichkeitsrechts offen bleiben. Als Tendenz kann aber festgehalten werden: Die freiwillige Selbstverpflichtung der AdNetwork Betreiber zur Opt-Out Möglichkeit ist hier wohl noch eindringlicher einzufordern als in Realisierung b).

[268] IAB Europe, Selbstregulierungsguideline: <www.iabeurope.eu/category/policy/self-regulation>.
[269] Vgl Fußnote 250.
[270] Dieses Opt-Out funktioniert wiederum mit Cookies und ist den entsprechenden Einschränkungen dieser Technologie, zB der Möglichkeit des lokalen Löschens durch den Benutzer, unterworfen.
[271] Quelle: <www.eff.org/deeplinks/2017/12/arms-race-against-trackers-safari-leads-criteo-30>.

zu d) Beim Einsatz dieser Technologie im Mobilfunkbereich entspricht die Pseudonymisierung der MSISDN heute der gängigen Praxis[272]. Außerdem erfolgt die Übermittlung der Identifikationsinformationen vorwiegend nur noch an ausgewählte Partnerwebsites und nicht an jede beliebige, erreichbare Internetadresse. Im hier behandelten Anwendungsfall sei ein AdNetwork als Partner des Mobilfunkproviders angenommen. Das AdNetwork muss sich nun nicht selbstständig um die Erstidentifikation des Internetbenutzers kümmern. Mit jedem Lesezugriff, den ein Endgerät eines Benutzers auf einen Werbebanner[273] durchführt, wird eine eindeutige, unveränderliche Benutzerkennung im *HTTP header* mitgeliefert. Das AdNetwork hat demnach sofort einen Identifikator verfügbar, kann ein kundenspezifisches Nutzerprofil anlegen und beginnen, dieses mit historischen Zugriffsdaten anzureichern.

Es sind Konstellationen denkbar, bei denen sich das AdNetwork von seiner Rolle als unabhängiger, offener Internetdienstleister verabschiedet und in eine tiefere (vertragliche und technische) Integration mit dem Mobilfunkbetreiber einsteigt. Das kann so weit gehen, dass das AdNetwork nur noch als Lieferant für Werbebanner herangezogen wird bzw das erstellte Nutzerprofil ausschließlich für den ausgewählten Mobilfunkbetreiber erstellt und benutzt wird[274]. In solch einer Konstellation kann unter Umständen die datenschutzrechtliche Rollenverteilung anders zu beurteilen sein. Sobald das AdNetwork als Auftragsverarbeiter des Mobilfunkanbieters anzusehen ist, entfällt die Notwendigkeit einer isolierten Zulässigkeitsprüfung für das AdNetwork.

Für die Prüfung des Einwilligungserfordernisses erscheint es daher sinnvoller, die interne Datenverarbeitung auf Seiten des Mobilfunkanbieters in seiner Rolle als Access-Provider und Verantwortlicher für die bei ihm gespeicherten, personenbezogenen Kundendaten zu beurteilen. Im Gegensatz zum Anwendungsfall *Direct Carrier Billing* (vgl Kapitel 4.6) ist im gegenständlichen Anwendungsfall strenggenommen keine zwingende De-Pseudonymisierung – zB für die Kundenabrechnung - erforderlich. Die einzelnen Benutzerprofile könnten auch, theoretisch denkbar, mit Identifikatoren versehen sein, die keinerlei Bezug zu den jeweiligen Stammdatensätzen haben. Um die Auswahl der passenden Werbebotschaft zu ermöglichen, muss allerdings weiterhin bei jedem einzelnen Zugriff des Kundenendgeräts auf einen Werbebanner im Internet das jeweils gleiche Pseudonym an den AdNetwork-Betreiber gesendet werden. Dieser Vorgang widerspricht der Basisanforderung an vollständig anonymisierte Daten – Im Proxy des Access-Providers kommt es zwingermaßen zu einer Verknüpfung zwischen einem Identifikationselement des Endgeräts und dem Pseudonym. Durch die immer wiederkehrende Verbindung mit dem Teilnehmerendgerät, zusammen mit der Vielzahl von internen Protokolldaten (zB Speicherung der aktuellen IP Adresse im *HTTP Access Log* des Proxy), erscheint es schwer

[272] *Schlee*, Targeted Advertising Technologies in the ICT Space (2013) 168.
[273] Der Werbebanner ist wiederum annahmegemäß auf einer beliebigen Webseite eines Websiteanbieters eingebunden.
[274] Bspw bietet das Unternehmen *Geolad* so eine Dienstleistung an: <www.geolad.com>.

vorstellbar, das nicht doch eine Beziehung zum tatsächlichen Stammdatensatz des Kunden hergestellt werden kann und damit eine Re-Identifizierung der realen Person ermöglicht wird. Im Zweifelsfall wird man daher den Personenbezug der Datenverarbeitung auch für diejenige technische Realisierung annehmen müssen, in welcher keine fixe Zuordnung zwischen dem Pseudonym und dem Kundenstammdatensatz besteht. Für den Access-Provider ist das Pseudonym daher ein personenbezogenes Datum – er kann auch nicht darauf verzichten, denn nur über das Pseudonym kann das AdNetwork die einzelnen Benutzer voneinander unterscheiden. Es soll auch darauf hingewiesen werden, dass die Verknüpfung mit den tatsächlichen Stammdaten des Mobilfunkkunden - diese enthalten praktisch immer das Geschlecht und das Alter der Person - für *behavioral targeting* ausgesprochen verlockend erscheint.

Das Pseudonym ist jedenfalls als Teil des *HTTP Headers* als Verkehrsdatum einzustufen. Laut § 99 Abs 1 TKG sind „Verkehrsdaten unverzüglich zu löschen oder zu anonymisieren". Das gegenständliche Verkehrsdatum ist aber nicht anonym und wird dennoch aufbewahrt.

Aufgrund fehlender spezialgesetzlicher Erlaubnistatbestände in §§ 97, 99 TKG (vgl Kapitel 4.6.4) ist letztlich wieder § 96 Abs 3 TKG für die finale Beurteilung maßgeblich. Aufgrund der durch die Überlagerung von TKG und DSGVO sehr eingeschränkten Berücksichtigungsmöglichkeit eines berechtigten Interesses auf Seiten des Mobilfunkbetreibers, sowie keiner erkennbaren technischen Rechtfertigung für einen vom Benutzer explizit angeforderten Dienst[275] ist von einem Einwilligungserfordernis auszugehen. Diese Einschätzung wird auch noch durch die Tatsache gestützt, dass der Benutzer im Gegensatz zu den anderen verwendeten Technologien überhaupt keine Möglichkeit hat, selbstständig die Bindung zu seinem servergespeicherten Nutzungsprofil aufzulösen. Der Benutzer müsste hierfür seinen Internetanbieter wechseln.

Die Einwilligung hat der Kunde gegenüber seinem Mobilfunkbetreiber abzugeben, zB auf dessen self-service Portal.

4.7.5 Einwilligungserfordernis (beurteilt anhand der ePrivacy VO)

Fraglich ist zunächst, ob die ePrivacy VO für den betrachteten Anwendungsfall eine spezielle Regelung vorsieht. Art 4 Abs 3 lit f ePrivacy VO iVm ErwGr 32 dürfte *Online Behavioral Targeting* als Direktwerbung klassifizieren[276], allerdings nach dem Wortlaut nur dann, wenn das Ziel für die Werbebotschaft eine *identifizierte* oder *identifizierbare* Person ist. Ob die fehlende Bestimmbarkeit des realen Internetbenutzers einen Ausschlussgrund für die genannte Klassifikation darstellt, ist unklar. Ebenso ist unklar, ob *Online Behavorial Targeting* als *unsolicited communication* gemäß Art 16 ePrivacy VO eingeordnet werden kann, welche

[275] Vgl die Argumentation in Kapitel 4.7.4, Realisierung a).

[276] Diese Klassifikation ist auf Basis des Wortlauts des Kommissionsentwurfs nicht eindeutig herstellbar. Die Stellungnahme des EU Parlaments sowie die Protokolle der Arbeitsgruppe des EU Rates (zB vom 22. März 2018 <www.parlament.gv.at/PAKT/EU/XXVI/EU/01/58/EU_15804/index.shtml>) bestätigen allerdings diese Sichtweise, und zwar durch die Aufnahme der Worte „or presents" in ErwGr 32 bzw Art 4 Abs 3 lit f.

dort außerhalb von bestehenden Geschäftsbeziehungen explizit als einwilligungspflichtig ausgewiesen wird[277]. Zum derzeitigen, unsicheren Stand des Gesetzgebungsprozesses soll auf diese beiden Spezialregelungen daher nicht tiefer eingegangen werden.

Jedenfalls findet sich für die *Cookie Technologie* und der *device fingerprinting* Technologie*,* ohne dass hier eine Unterscheidung notwendig ist, die Lösung in Art 8 ePrivacy VO. Unabhängig von der Frage des Personenbezugs der verarbeiteten Daten ist aus Art 8 Abs 1 ePrivacy VO keine Rechtfertigung für die Speicherung und das Auslesen von Daten des Benutzerendgeräts herauszulesen. Insbesondere greift hier Art 8 Abs 1 lit c zur technischen Notwendigkeit der Diensterbringung nicht. Daher ist ein Einwilligungserfordernis aus heutiger Sicht für diese technischen Realisierungen zu bejahen - also konkret für: a), b), c). Es erscheint unzufriedenstellend, dass dieses Ergebnis über den Umweg der technischen Realisierung und nicht über eine zweckbezogene Analyse dieses – im Internet sehr weit verbreiteten - Anwendungsfalls hergestellt wird[278], aber aus dem derzeitigen Stand des Gesetzgebungsverfahrens zur ePrivacy VO kann keine andere Aussage abgeleitet werden[279]. Zu den Diskussionen zur möglichen Erweiterung der Erlaubnistatbestände für Kommunikationsmetadaten siehe übernächster Absatz.

zu d) Die Beurteilung erfolgt auf Basis der allgemeineren Bestimmung, Art 6 ePrivacy VO. Der Kommissionsentwurf sieht nur wenige Möglichkeiten vor, bei denen Metadaten, welche nicht für die unmittelbare Zurverfügungstellung des abgerufenen Dienstes technisch notwendig sind, verarbeitet werden dürfen. Für den hier untersuchten Anwendungsfall *behavioral targeting* sind insbesondere auch die zusätzlichen Erlaubnistatbestände aus Art 6 Abs 2 lit b ePrivacy VO für die Zwecke der Abrechnung sowie der Sicherstellung der Kommunikationssicherheit und Netzintegrität nicht einschlägig. Auch die Ausnahmebestimmungen für TSM-VO konforme Verkehrsmanagementmaßnahmen (siehe Kapitel 3.3.4) in Art 6 Abs 2 lit a führen hier zu keiner Ausnahme von dem generellen Einwilligungsvorbehalt, da es sich nicht um eine Verkehrsmanagementmaßnahme handelt.

Der letzte Satz in Art 6 Abs 2 lit c[280] des Komissionsentwurfs erlaubt jedoch die Interpretation, dass eine vereinfachte Zustimmung zur Verarbeitung von anonymisierten Kommunikationsmetadaten in Verbindung mit dem Abruf bestimmter Dienste vorgesehen ist. Die neueren Protokolle der Arbeitsgruppe des EU Rates[281] zeigen bei der Formulierung dieser Ausnahmebestimmung eine rege Diskussionsaktivität. Aus den Diskussionsbeiträgen ist zu entnehmen, dass die Verarbeitung von personenbezogenen Metadaten, welche nicht durch technische Notwendigkeiten ohnehin bereits erlaubt sind, unter bestimmten

[277] ErwGr 33 fordert für *unsolicited communication* eine „privacy intrusion" und nennt als Beispiele ausschließlich gerichtete Kommunikationskanäle wie SMS, email und dergleichen aber nicht die personalisierte Darstellung von Webinhalten.
[278] *Schleipfer,* ZD 2017, 460 (466).
[279] Vgl Fußnote 163.
[280] im Volltext: " (...) provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous".
[281] Vgl Fußnote 227.

Umständen vom Erlaubnisvorbehalt ausgeschlossen werden bzw einer Opt-Out Lösung zuzuführen sind. In den Vorschlägen wird in diesem Zusammenhang auf die Zweckänderungslehre aus Art 6 Abs 4 DSGVO rekurriert. Auch die Kategorie *pseudonymisierte Daten* wird explizit in einem der Vorschläge genannt.

Bei den technischen Realisierungen c) und d) erfolgt jedenfalls eine Verarbeitung von Metadaten im Sinne des Verordnungsentwurfs, und zwar in Form des Auslesens des *HTTP headers*. Auch beim Einsatz von Cookies, Realisierung a) und b), fallen neben Inhaltsdaten auch Kommunikationsmetadaten an. Jedoch ist unklar, wie sich letztlich ein Erlaubnistatbestand in Art 6 Abs 2 lit c für pseudonymisierte Metadaten gegenüber der strikten, endgerätebezogenen Verbotsregelung in Art 8 Abs 1 behaupten kann[282].

Es deutet einiges darauf hin, dass der hier beschriebene Anwendungsfall des *behavioral targeting* in Abgrenzung zu anderen Zwecken (zB Webanalyse) einer eigenen, technologieneutralen Regelung unterzogen werden könnte – die Ausgestaltung und die Rechtsfolge dieser Regelung können aber zum derzeitigen Stand des Gesetzgebungsprozesses nicht seriös vorhergesagt werden.

4.8 Ermitteln einer aussagekräftigen Besucherstatistik durch den Websitebetreiber *ohne* Einbeziehung eines Drittanbieters

4.8.1 Kurzbeschreibung des Anwendungsfalls

Neben der Gesamtzahl der Zugriffe auf eine Website, welche durch einen einfachen Zählprozess gemessen werden kann, ist die Anzahl der sogenannten *unique visitors*[283] eine ausgesprochen wichtige Kennzahl, die Reichweite einer Website und damit ihren Erfolg beim Publikum zu messen. Um Erstbesucher von Wiederkehrern zu unterscheiden, müssen alle Besucher entsprechend markiert und bei ihrem nächsten Besuch wiedererkannt werden. Nur Erstbesucher werden im Beobachtungszeitraum (zB ein Monat) als *unique visitor* gezählt. Das Element des *unique visitors* wird vom Websitebetreiber außerdem auch dafür benötigt um ausgewählte *clickstreams* innerhalb seiner Website zu erkennen und danach den Aufbau seiner Website optimieren zu können. Dabei steht nicht der einzelne Benutzer und seine Vorlieben für bestimmte Themen im Vordergrund, sondern der Websitebetreiber möchte die Popularität der einzelnen Unterseiten sowie die Popularität der einzelnen Verlinkungen innerhalb dieser Unterseiten auswerten.

In der hier beschriebenen Ausprägung ist der eigentliche Zählmechanismus komplett in der Website integriert[284] (sogenannte *self-hosted* Webanalyse). Es findet für den Zweck der

[282] Stellungnahme 29/2017 des Deutschen Anwaltvereins durch die Ausschüsse Informationsrecht und Gefahrenabwehrrecht zum ePrivacy VO Kommissionsentwurf (März 2017) 15 ff, <www.computerundrecht.de/DAV-SN_29-17.pdf>.

[283] Vgl dazu als Beispiel: <de.statista.com/statistik/daten/studie/180570/umfrage/meistbesuchte-websites-in-deutschland-nach-anzahl-der-besucher>.

[284] Eine Übersicht über verschiedene Web-Analyse Produkte, sowohl *self-hosted* als auch *external-hosted* ist zu finden unter: <en.wikipedia.org/wiki/List_of_web_analytics_software>.

Zählung keine Einbettung von Fremdinhalten und keine Weiterleitung zu Webangeboten von Drittanbietern statt. Für den Benutzer ist der komplette Vorgang iA nicht erkennbar. Die Benutzerzählung hat keinerlei unmittelbaren Einfluss auf Gestaltung und Funktion des Webangebots.

4.8.2 Datenschutzrechtliche Rollenzuteilung

Der Websitebetreiber ist Verantwortlicher und wäre als solcher der Verpflichtete zur Einholung der Einwilligung. Der Internetbenutzer ist Betroffener iSd DSGVO und somit derjenige, der die Einwilligung zu erteilen hätte.

4.8.3 Datenschutzrechtliche Einordnung der technischen Verarbeitungsvorgänge

Die Realisierung dieses Anwendungsfalls erfolgt

a) bevorzugt durch die Zuweisung einer eindeutigen *BenutzerID* und deren Abspeicherung in einem *HTTP First-Party Cookie*[285]
b) alternativ durch die Zuweisung eines *device fingerprints*

Die Zugriffsanalyse alleine auf Basis von IP Adressen aus dem *HTTP access log* heraus[286] ist für die Erkennung von *unique visitors* zu ungenau und soll daher hier keine Betrachtung finden. Für die datenschutzrechtliche Beurteilung soll außerdem angenommen werden, dass der Websitebetreiber nur aggregierte Kennzahlen zu *unique visitors* und *clickstreams* an Dritte weitergibt bzw veröffentlicht, insbesondere nicht gemeinsam mit den verwendeten *BenutzerIDs.*

4.8.4 Einwilligungserfordernis (de lege lata)

zu a) Auf Basis von § 96 Abs 3 TKG ist nur eine sehr eingeschränkte Berücksichtigung eines berechtigten Interesses des Websitebetreibers möglich. Eine technische Notwendigkeit zur Verarbeitung des Cookies ist nicht ersichtlich. Aus dieser Analyse ergibt sich direkt ein Einwilligungserfordernis für die Realisierung dieses Anwendungsfalls mit *HTTP Cookies*. Das Einwilligungserfordernis ist unabhängig von der Möglichkeit zu beurteilen, ob das Web-Analyse Produkt nur verkürzte IP Adressen verarbeitet/abspeichert oder nicht. Dieses Ergebnis deckt sich mit der Sichtweise der *Art-29-Datenschutzgruppe* auf Basis der Richtlinie 2009/136/EG Art 5 Abs 3 (vgl Kapitel 3.3.2), wobei die *Art-29-Datenschutzgruppe* bereits im Jahr 2012 darauf hingewiesen hat, dass in einem zukünftigen Gesetzgebungsprozess eine Ausnahmebestimmung für diesen Anwendungsfall erwogen werden sollte[287].

An dieser Stelle kann aus Platzgründen nicht näher ausgeführt werden, ob es für den Websitebetreiber technische Möglichkeiten geben könnte, das in weiten Teilen als

[285] ZB beim Web-Analyse Produkt *Matomo* (bisher bekannt unter dem Namen: *PIWIK*): <matomo.org/faq/general/#faq_21418>.
[286] ZB durch das Web-Analyse Produkt AWSTATS: <awstats.sourceforge.io/docs/awstats_glossary.html>.
[287] *Art-29-Datenschutzgruppe*, WP194, 11.

unsachgemäß empfundene Einwilligungserfordernis zu vermeiden. Ein vielversprechender Denkansatz dazu wäre der Einsatz von zeitlich auf den Berichtszeitraum (zB ein Monat) beschränkten *BenutzerIDs*. Die hier vertretene Auslegung des TKG 2003 steht der Berücksichtigung von nicht technisch motivierten Interessen des Websitebetreibers aber weiterhin entgegen.

Das Einwilligungserfordernis führt letztlich dazu, dass dem Benutzer auch nach einem eventuellen Widerruf seiner Einwilligung – welche er beispielsweise bei seinem ersten Besuch durch bewusste Interaktion mit einem Cookie-Banner ausgedrückt hat - die Möglichkeit gegeben werden muss, die Website weiterhin zu benutzen. Praktisch – aber nicht juristisch[288] - kann dies mit einer Opt-Out Option als Eingabeelement auf der Website realisiert werden. So wird dies bspw von den deutschen Aufsichtsbehörden gefordert[289].

zu b) im Vergleich zur Analyse des Anwendungsfall unter Kapitel 4.5.4, Realisierungsvariante b) ergibt sich hier keine technische Notwendigkeit zur serverseitigen Abspeicherung der vollständigen IP Adresse. Viele Web-Analyse Tools verwenden für die interne Verarbeitung verkürzte, und damit anonymisierte, IP Adressen[290]. Aufgrund des Fehlens der Verarbeitung personenbezogener Daten ergibt sich hier im Ergebnis kein Einwilligungserfordernis nach dem Datenschutzrecht.

Im Gegensatz zum Anwendungsfall *behavorial targeting*[291] werden auch keine Teilabbilder der Persönlichkeit des Benutzers erstellt und es erfolgt auch keine intransparente, unterschiedliche Behandlung einzelner Nutzer durch Einblenden bzw Ausblenden benutzerspezifischer Inhalte. Selbst beim Erstellen detaillierter *clickstreams* fehlt weiterhin – technologieimmanent - die Eindeutigkeit der Zuordnung zu einem bestimmten Benutzer. Der Zweck für die Erstellung des *clickstreams* ist hier außerdem nicht das Erkennen von Vorlieben oder Abneigungen der einzelnen Benutzer, sondern lediglich die aggregierte Auswertung von Beliebtheitswerten von einzelnen Unterseiten. Im Ergebnis ist auch über die Konstruktion §§ 16, 1328a ABGB kein persönlichkeitsrechtlicher Eingriff vorliegend und daher weder ein Einwilligungserfordernis noch eine Opt-Out Verpflichtung de lege lata zu vertreten. Dieses Ergebnis steht allerdings im Widerspruch zur Sichtweise der *Art-29-Datenschutzgruppe*[292].

4.8.5 Einwilligungserfordernis (beurteilt anhand der ePrivacy VO)

Der Kommissionsentwurf der Verordnung sieht unter Art 8 Abs 1 lit d eine Ausnahmebestimmung vom Einwilligungserfordernis für die Realisierung des

[288] Das primäre Einwilligungserfordernis bleibt! Auf Basis der österreichischen Rechtslage ist eine echte Opt-Out Lösung, bei der das Informieren des Benutzers und das Anbieten einer Opt-Out Möglichkeit ausreichend ist, unzulässig (vgl *Riesz* in *Riesz/Schilchegger* TKG § 96 Rn 8).

[289] Orientierungshilfe zum Einsatz von *Google Analytics*, <www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/oh_google-analytics.pdf>.

[290] ZB bei *Matomo* <matomo.org/faq/general/#faq_21418>.

[291] Vgl Kapitel 4.7.3, Realisierungsvariante b) und c).

[292] *Art-29-Datenschutzgruppe,* WP224, Kapitel 7.1.

Anwendungsfalls „Web audience measurement“ vor. Diese Ausnahme ist jedenfalls auf *self-hosted* Webanalyselösungen anwendbar und es werden hierfür keine weiteren Einschränkungen oder Anforderungen statuiert. Die EU Kommission ist damit der Empfehlung der *Art-29-Datenschutzgruppe* gefolgt (vgl Fußnote 287). Aus den Stellungnahme des EU Parlaments und den Protokollen der Arbeitsgruppe des EU Rates ist keine drohende Abkehr von dieser Regelung erkennbar[293].

4.9 Ermitteln einer aussagekräftigen Besucherstatistik durch den Websitebetreiber *mittels* Einbeziehung eines Drittanbieters

4.9.1 Kurzbeschreibung des Anwendungsfalls

Viele Websitebetreiber greifen auf cloudbasierte Webanalyse-Werkzeuge von Drittanbietern zurück. Das bekannteste Produkt am Markt ist *Google Analytics,* allerdings gibt es auch andere Anbieter. Der Anbieter Innocraft bspw. bietet eine cloudbasierte Lösung auf Basis des *Matomo* (bisher bekannt unter dem Namen: PIWIK) Open-Source Produkts an[294]. Bei der Integration solcher Lösungen werden Inhalte des Drittanbieters in die Webseiten integriert. Es kommt iA zu einer bewusst herbeigeführten, direkten Kontaktaufnahme zwischen dem Benutzer und dem Drittanbieter – für ersteren ist diese Kontaktaufnahme allerdings nicht ohne weiteres erkennbar. Die technische Realisierung der Einbettung ist vergleichbar mit dem Anwendungsfall *behavioral targeting* (vgl Kapitel 4.7).

4.9.2 Datenschutzrechtliche Rollenzuteilung

Trotz der technischen Ähnlichkeiten zum Anwendungsfall *behavioral targeting* (vgl Kapitel 4.7) gab es in der deutschsprachigen rechtswissenschaftlichen Literatur in den letzten Jahren kaum Einwände dagegen, Dienste wie *Google Analytics* als Auftragsdatenverarbeitung im datenschutzrechtlichen Sinn einzustufen. Das mag vorwiegend daran liegen, dass der *Hamburgische Beauftragte für Datenschutz* federführend für die Aufsichtsbehörden in Deutschland bereits zwischen 2009 und 2011 intensive Verhandlungen mit der Firma *Google* geführt hat. Das Ziel war, eine BDSG konforme Lösung für den Einsatz von *Google Analytics* auf deutschen Websites zu finden[295]. Diese Lösung beinhaltet unter anderem die implizite Anerkennung des Dienstes als Auftragsdatenverarbeitung unter den von *Google* verwendeten AGBs. Die derzeitige Bezeichnung dieses Vertrags ist „Google Ads Data Processing Terms“[296], welcher in Ziffer 5.1.1 lit b im Rahmen einer Eigendeklaration *Google* als Auftragsverarbeiter bezeichnet und den Websitebetreiber als Verantwortlichen. Es gibt keine Hinweise darauf, dass im Hinblick auf diese Rollenzuteilung nach Wirksamwerden der DSGVO eine andere Ansicht zu

[293] Vgl die Referenzen in Fußnoten 168, 227.
[294] Website des Herstellers: <www.innocraft.cloud>.
[295] Vgl Fußnote 289.
[296] <privacy.google.com/businesses/processorterms>.

vertreten ist. Kritisch sei an dieser Stelle allerdings angemerkt, dass eine Beurteilung nach den Kriterien wie oben abgeleitet[297], auch ein anderes Ergebnis zulassen würde: nämlich eine geteilte Verantwortlichkeit.

4.9.3 Datenschutzrechtliche Einordnung der technischen Verarbeitungsvorgänge

Die Realisierung dieses Anwendungsfalls erfolgt

a) bevorzugt durch die Zuweisung einer eindeutigen *BenutzerID* und deren Abspeicherung in einem *HTTP First-Party Cookie*[298] oder einem *Third-Party Cookie*
b) alternativ durch Zuweisung eines *device fingerprints*

Alle Datenaufzeichnungen sowie die Vergabe und das Management der *BenutzerIDs* erfolgt durch den Drittanbieter. Der Benutzer wird bei jedem Besuch der Website im Hintergrund mit dem Drittanbieter verbunden und tauscht mit diesem Daten aus. Bei dieser Verbindung wird notwendigerweise die IP Adresse des Benutzers als Teil der Datenkommunikation übertragen. Obwohl der Cookie vom Drittanbieter erzeugt und ausgelesen wird, verwenden einige Anbieter eine besondere Technik und erzeugen *First-Party Cookies*[299]*.* Dies ist eine wirksame Maßnahme um auch Benutzer zu identifizieren, welche ihren Webbrowser so eingestellt haben, dass dieser *Third-Pary Cookies* nicht verarbeitet. Diese Schutzfunktion geht dann ins Leere.

Der Websitebetreiber ist auch bei der Auswertung der Ergebnisse der Webanalyse auf die Dienste des Drittanbieters angewiesen, zB indem er sich aussagekräftige Statistiken regelmäßig zuschicken lässt oder online auf der Website des Dritten einsieht.

Die weitergehenden Funktionen von *Google Analytics*, wie zB die Verknüpfung mit Login Daten von bei *Google* registrierten Usern, die websiteübergreifende Analyse von Benutzungsstatistiken sowie die Verknüpfung mit den *trackingdaten* aus *Googles* eigenem Werbenetzwerk *AdSense,* werden hier nicht betrachtet.

An dieser Stelle soll angenommen werden, dass der Drittanbieter die physische Datenverarbeitung entweder in der EU oder den USA durchführt. Aufgrund des EU-US-Privacy-Shield Abkommens ergeben sich bspw für *Google* derzeit keine rechtlichen Probleme in Bezug auf den Datentransfer in die USA gemäß DSGVO. Eine detaillierte Analyse der aktuellen *Google Analytics* AGBs hinsichtlich ihrer Konformität zu den DSGVO Anforderungen an einen Auftragsverarbeitungsvertrag erfolgt hier nicht.

4.9.4 Einwilligungserfordernis (de lege lata)

Der Websitebetreiber ist der Verantwortliche für die Datenverarbeitung – er muss demnach die Verarbeitung personenbezogener Daten gegenüber dem Betroffenen rechtfertigen. Selbst wenn, wie im einfachsten Fall der Integration der Webanalyse-Lösung, der

[297] Vgl Kapitel 4.7.2.
[298] Die Unterscheidung zwischen den beiden Cookie Typen ist verschwimmend, siehe nachfolgenden Absatz.
[299] *First-Party Cookies* sind das default setting bei *Google Analytics*, Quelle*:* <developers.google.com/analytics/devguides/collection/analyticsjs/cookies-user-id>.

Websitebetreiber letztlich nicht in der Erstellung, Administration und Speicherung der Pseudonyme involviert ist, so muss er sich dennoch die Verwendung und Verarbeitung dieser Pseudonyme durch seinen Auftragsverarbeiter zurechnen lassen. Insofern ergibt sich bei der Beurteilung des Einwilligungserfordernisses keine andere Situation als im entsprechenden Zwei-Parteien Anwendungsfall (vgl Kapitel 4.8.4) und somit ein Einwilligungserfordernis für die Realisierungsvariante a), hingegen kein Einwilligungserfordernis für die Realisierungsvariante b).

4.9.5 Einwilligungserfordernis (beurteilt anhand der ePrivacy VO)

Der Wortlaut des Kommissionsentwurfs in Art 8 Abs 1 lit d[300] kann so interpretiert werden, dass die Ausnahmebestimmung zum Einwilligungserfordernis auch für cloudbasierte Webanalyse-Lösungen von Drittanbietern anwendbar ist. Der Websitebetreiber führt die Messung nämlich auch dann selbst durch, wenn er mit einem Dienstleister zu diesem Zweck einen Auftragsverarbeitungsvertrag geschlossen hat[301] - diese Argumentation entspricht der in der DSGVO vorgesehenen, rechtsdogmatischen Funktion des Verantwortlichen. Die Stellungnahme des EU Parlaments sowie die Protokolle der Arbeitsgruppe des EU Rates sehen bereits eine textuelle Klarstellung vor, die die obige Interpretation weiter stützt[302].

[300] Im Volltext: „(...) such measurement is carried out by the provider of the information society service.".
[301] *Schleipfer,* ZD 2017,460 (466).
[302] Vgl Referenzen in Fußnoten 168, 227.

5. Schlußbetrachtungen

Die *Breyer* Entscheidung des EuGH hat in der jahrelangen Diskussion zur Frage „Was sind personenbezogene Daten“ zwei wesentliche Orientierungspunkte vorgegeben: Zum einen gibt es nun eine Leitlinie zur Beurteilung, welcher Aufwand und welche Mittel vertretbar erscheinen, um den Personenbezug eines Pseudonyms wiederaufleben zu lassen. Gleichzeitig lässt der EuGH erkennen, dass die Möglichkeit der Herstellung des Personenbezugs auf die reale Person gerichtet sein muss und eine reine *Online-Identität* ohne Verknüpfbarkeit zu einer realen Person nicht vom Schutzkonzept des Datenschutzrechts umfasst ist. Auf diesen beiden Eckpfeilern aufsetzend, wird in dieser Arbeit die *Theorie über die Verkettung der pseudonymisierten IP Adresse* abgeleitet. Diese Theorie führt zu einer breiten Anwendung des Datenschutzrechts beim Einsatz von Identifikatoren im Internet, fordert allerdings die systemimmanente Eindeutigkeit des Identifikators zu einem Endgerät und eine laufende Aktualisierung der Verknüpfung zwischen IP Adresse und Pseudonym (=Identifikator) durch die Wiederkehr des Benutzers. Ohne das starre Verhältnis zur IP Adresse gibt es unter alleiniger Betrachtung des Pseudonyms keine Bestimmbarkeit der realen Person über den Umweg des Access- Providers und somit keinen datenschutzrechtlichen Bezug. Nach der aktuellen Fassung des Telekommunikationsgesetzes - unter Berücksichtigung des Spezialitätsverhältnisses zur DSGVO - führt erst der datenschutzrechtliche Bezug zu einem Einwilligungserfordernis im Hinblick auf die Personalisierung von Webangeboten mithilfe von Identifizierung und Wiedererkennung des Internetbenutzers. Dh solange ein technisches Verfahren zur Identifikation und Wiedererkennung nicht notwendigerweise zur Verarbeitung von personenbezogenen Daten führt, führen die darauf aufbauenden praktischen Anwendungsfälle iA nicht zu einem Einwilligungserfordernis des Internetbenutzers. Im Zuge der Untersuchung wurde dies bspw für verschiedene Ausprägungen der Cookie Technologie unterschiedlich beurteilt. Hingegen löst der Einsatz der *device fingerprinting* Technologie mangels Personenbezug der verarbeiteten Daten für sich alleine noch keine datenschutzrechtliche Zulässigkeitsprüfung aus. Die datenschutzrechtlichen Problembereiche der *MSISDN forwarding* Technologie wurden bislang in der deutschsprachigen, rechtswissenschaftlichen Literatur nur ganz vereinzelt angesprochen. Access-Provider, die diese Technologie weiterhin ohne Einwilligung ihrer Kunden großflächig einsetzen und keine zweckbezogene Rechtfertigung vorbringen können, verstoßen gegen das Datenschutzrecht.

Wird ein inhärenter Personenbezug auf der technologischen Ebene bejaht, so kann es dennoch auf der Ebene des jeweiligen Anwendungsfalls zu einer datenschutzkonformen, zweckbezogenen Rechtfertigung der Datenverarbeitung kommen. Womit letztlich das Einwilligungserfordernis wiederum fallweise abgelehnt wird. Mit Hilfe dieser zweistufigen Beurteilung, wie sie hier in dieser Arbeit konsequent angewendet wird, können auch

zukünftige Identifikationstechnologien und die darauf aufbauenden Anwendungsfälle auf ihre Datenschutzkonformität geprüft werden.

Dem hier gefunden Ergebnis steht allerdings folgendes gegenüber: Internetbenutzer haben oftmals den Eindruck, dass *ihre* Aktivitäten beobachtet werden und Daten, zB in der Form von Nutzerprofilen, *über* sie gesammelt werden. Das wird weit verbreitet als ungerechtfertigt empfunden und zwar unabhängig davon, ob es eine Verknüpfung zur tatsächlichen Identität der Person gibt oder nicht. Falls sich durch die oben erwähnte Einschränkung auf personenbezogene Daten eine Schutzlücke für den einzelnen Internetbenutzer ergibt, dann muss diese außerhalb des Datenschutzrechts geschlossen werden und nicht über eine weitere Ausdehnung desselben. Diese Schutzlücke könnte durch ein paralleles, spezialgesetzliches Schutzregime adressiert werden. Erst mit der Diskussion über die ePrivacy VO hat sich unstrittig ergeben, dass der europäische Gesetzgeber solch ein neues Schutzregime anstrebt. Über die Implementierung der ePrivacy Richtlinie aus dem Jahr 2009 ist dies bislang nicht gelungen. In dieser Arbeit wird schließlich auch noch ein anderer Weg aufgezeigt, wie mithilfe des allgemeinen Persönlichkeitsrechts und den Wertungen von Art 8 EMRK gegen eine exzessive Verfolgung, Beobachtung und Aussonderung des nicht bestimmbaren, aber real existierenden Internetbenutzers vorgegangen werden kann.

Abkürzungsverzeichnis

aA	andere Ansicht
aaO	am angegebenen Ort
Abs	Absatz
ABl	Amtsblatt der europäischen Union
Art	Artikel
BDSG	dt. Bundesdatenschutzgesetz
BGBl	Bundesgesetzblatt
BGH	dt. Bundesgerichtshof
BlgNR	Beilagen zu den Stenographischen Protokollen des Nationalrats
bspw	beispielsweise
BVerfG	dt. Bundesverfassungsgericht
bzw	beziehungsweise
dh	das heißt
EBRV	Erläuternde Bemerkungen zur Regierungsvorlage
EMRK	Europäische Menschenrechtskonvention
ErwGr	Erwägungsgrund
GRC	Grundrechte Charta der EU
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
Hrsg	Herausgeber
hM	herrschende Meinung
ID	Identifikator
IP	Internet Protocol
ISP	Internet Service Provider
IMSI	International Mobile Subscriber Identity
iA	im Allgemeinen
iSd	im Sinne des
iSe	im Sinne eines
iVm	in Verbindung mit
MSISDN	Mobile Station International Subscriber Directory Number
OGH	Oberster Gerichtshof
OLG	Oberlandesgericht
RFC	Request for Comments
RL	Richtlinie
Rn	Randnummer
RTR	Rundfunk- und Telekomregulierungsbehörde
TCP/IP	Transmission Control Protocol / Internet Protocol
TKK	Telekom Control Kommission
TMG	dt. Telemediengesetz
TSM-VO	Telecom Single Market Verordnung
URL	Uniform Ressource Locator
UUID	Universally Unique Identifier
uA	und Andere
uÄ	und Ähnliches
uU	unter Umständen
vgl	vergleiche
VO	Verordnung
WAP	Wireless Application Protocol
WWW	World Wide Web
zB	zum Beispiel
zT	zum Teil

Literaturverzeichnis (Ohne Online Referenzen)

Alich, Stefan/Voigt, Paul, Mitteilsame Browser – Datenschutzrechtliche Bewertung des Trackings mittels Browser-Fingerprints, CR 2012, 344-348

Art-29-Datenschutzgruppe, Opinion 4/2007 on the concept of personal data, WP136, 20.06.2007

Art-29-Datenschutzgruppe, Opinion 1/2008 on data protection issues related to search engines, WP148, 04.04.2008

Art-29-Datenschutzgruppe, Opinion 2/2010 on online behavioural advertising, WP171, 22.06.2010

Art-29-Datenschutzgruppe, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP224, 25.11.2014

Art-29-Datenschutzgruppe, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, WP188, 08.12.2011

Art-29-Datenschutzgruppe, Opinion 04/2012 on Cookie Consent Exemption, WP194, 07.06.2012

Art-29-Datenschutzgruppe, Opinion 15/2011 Consent, WP187, 13.07.2011

Baston-Vogt, Marion, Der sachliche Schutzbereich des zivilrechtlichen allgemeinen Persönlichkeitsrechts, 1. Auflage, Verlag Mohr-Siebeck, Tübingen 1997

BEREC, Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, DocNo BoR (16) 127

Brink, Stefan/Wolff,Heinrich Amadeus (Hrsg), Beck Online-Kommentar Datenschutzrecht, 24. Auflage, Verlag C.H. Beck, München 2018

Christl, *Alexander*,Datenschutz im Internet: Cookies, Web-Logs, Location Based Services, eMail, Webbugs, Spyware, 1. Auflage, Disserta Verlag, Hamburg 2014

Dieterich, Thomas, Canvas Fingerprinting - Rechtliche Anforderungen an neue Methoden der Nutzerprofilerstellung, ZD 2015, 199-204

Engeler, Malte, Die ePrivacy-Verordnung zwischen Trilog und Ungewissheit, ZD 2017, 549 – 550

Engeler, Malte/Felber, Wolfram, Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis, ZD 2017, 251–257

Feiler, Lukas/Forgó, Nikolaus, EU-DSGVO, 1. Auflage, Verlag Österreich, Wien 2016

Feiler, Lukas/Horn, Bernhard, Umsetzung der DSGVO in der Praxis, 1. Auflage, Verlag Österreich, Wien 2018

Forgó, Nikolaus/Helfrich, Marcus/Schneider, Jochen, Betrieblicher Datenschutz, 2. Auflage, C.H. Beck Verlag, München 2014

Funke, Michael/Wittmann, Jörn, Cloud Computing – ein klassischer Fall der Auftragsdatenverarbeitung?, ZD 2013, 221 –228

Geuer, Ermano/Reinisch, Fabian, Direktwerbung und Cookies im Spannungsfeld des TKG und der DSGVO, MR 2018, 123 - 135

Gola, Peter/Schomerus, Rudolf (Hrsg), Bundesdatenschutzgesetz, 12. Auflage, Verlag C.H. Beck, München 2015

Hanloser, Stefan, Geräte-Identifier im Spannungsfeld von DS-GVO, TMG und ePrivacy-VO, ZD 2018, 213-218

Häberle, Peter (Hrsg), Erbs/Kohlhaas - Strafrechtliche Nebengesetze Loseblattsammlung, 219. Ergänzungslieferung, Verlag C.H. Beck, München 2018

Härting, *Niko*, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065 – 2071

Heckmann, Dirk (Hrsg), JurisPK-Internetrecht, 5. Auflage, Juris Online, Saarbrücken 2017

Helmich, *Elisabeth*, Schadenersatz bei Eingriffen in die Privatsphäre, ecolex 2003, 888

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg), Handbuch Multimedia-Recht, Losblattsammlung, 46. Auflage, Verlag C.H. Beck, München 2018

Jahnel, Dietmar, Datenschutz im Internet Rechtsgrundlagen, Cookies und Web-Logs, ecolex 2001, 84

Jahnel, Dietmar, Glosse zu EuGH 19.10.2016, C-582/14 (*Breyer*), JusIT 2016, 252 - 254

Jahnel, Dietmar, Spamming, Cookies, Logfiles und Location Based Services im TKG 2003, ÖJZ 9/2004, 336

Jahnel, Dietmar/Mader, Peter/Staudegger, Elisabeth (Hrsg), IT-Recht, 3. Auflage, Verlag Österreich, Wien 2012

Karg, Moritz, Die Rechtsfigur des personenbezogenen Datums - Ein Anachronismus des Datenschutzes?, ZD 2012, 255 - 260

Kaushik, *Avinash*, Web Analytics 2.0, Verlag Wiley, Indianapolis 2010

Keppeler, Lutz Martin, Was bleibt vom TMG-Datenschutz nach der DS-GVO?, MMR 2015, 779 - 783

Kilian, Wolfgang/Heussen, Benno (Hrsg), Computerrechts-Handbuch, 34. Auflage, Verlag C.H. Beck, München 2018

Koziol, Helmut/Bydlinski, Peter/Bollenberger, Raimund, ABGB, 5. Auflage, Verlag Österreich, Wien 2017

Kremer, Sascha, Wer braucht warum das neue BDSG?, CR 2017, 367 - 378.

Kunnert, Gerhard, Die datenschutzkonforme Vernetzung des Automobils, CR 2016, 509 - 516

Kutscha, Martin, Mehr Schutz von Computerdaten durch ein neues Grundrecht, NJW 2008, 1042 – 1044

Kühling, Jürgen/Schall, Tobias, E-Mail-Dienste sind Telekommunikationsdienste iSd. TKG, CR 2016, 173 - 185

Lust, Philipp, Telekommunikationsrechtliche Änderungen aus Kundensicht, VbR 2016/6, 17

Maisch, Marc, Der Browser Fingerprint als personenbezogenes Datum im Telemedienrecht?, JurisAnwZert ITR 5/2010 Anm 3

Meyer, Julia, Identität und virtuelle Identität natürlicher Personen im Internet, 1. Auflage, Verlag Nomos, Baden-Baden 2011

Moos, Flemming, Unmittelbare Anwendbarkeit der Cookie-Richtlinie - Mythos oder Wirklichkeit?, K&R 2012, 637 - 640

Karg, Moritz/Kühn, Ulrich, Datenschutzrechtlicher Rahmen für "Device Fingerprinting", ZD 2014, 285 – 290

Mutz, *Uwe*, Flash CS3 – AJAX & PHP, 1. Auflage, Verlag Addison-Wesley, München 2007

Nebel, Maxi/Richter, Philipp, Datenschutz bei Internetdiensten nach der DS-GVO , ZD 2012, 407 - 413

Paal, Boris/Pauly, Daniel (Hrsg), Datenschutz-Grundverordnung - Bundesdatenschutzgesetz: DS-GVO BDSG, 2. Auflage, Verlag C.H. Beck, München 2018

Pachinger, Michael, Achtung Cookies – Verpflichtung zur Einwilligung beim Online-Targeting, JusIT 2011/10, 18 – 22

Pachinger, Michael, Der neue „Cookie-Paragraph" – Erste Gedanken zur Umsetzung des Art 5 Abs 3 E-Privacy-RL in § 96 Abs 3 TKG 2003 idF BGBl I 2011/102, jusIT 2012/8, 16 – 22

Pachinger, Michael, Aktuelles zur datenschutzrechtlichen Zustimmung beim Online-Targeting, jusIT 2012/84, 173 – 178

Plath, Kai-Uwe (Hrsg), DSGVO/BDSG/TMG, 3. Auflage, Verlag Otto Schmidt, Köln 2018

Riesz, Thomas/Schilchegger, Michael (Hrsg), Telekommunikationsgesetz, 1. Auflage, Verlag Österreich, Wien 2016

Roßnagel , *Alexander*, Entwurf einer E-Privacy-Verordnung – Licht und Schatten, ZRP 2017, 33

Roßnagel, Alexander, Fahrzeugdaten – wer darf über sie entscheiden?, Straßenverkehrsrecht 8/2014, 281-287

Russel, Matthew A, Dojo: The definitive guide, Verlag O´Reilly, Sebastopol 2008

Schenk(Stratil), Katharina, Zugriffsanalyse, Online-Targeting und Social Media-Plug-ins - bereichsspezifischer Datenschutz im DSG 2000 und TKG 2003, Master-Thesis Universität Wien 2013

Schlee, Christian, Targeted Advertising Technologies in the ICT Space, 1. Auflage, Verlag Springer Vieweg, Wiesbaden 2013

Schleipfer, *Stefan*, Datenschutzkonformer Umgang mit Nutzungsprofilen, ZD 2015, 399 – 405

Schleipfer, Stefan, Datenschutzkonformes Webtracking nach Wegfall des TMG, ZD 2017, 460 – 466

Schmädel, Judith von, Persönlichkeitsrechte im österreichischen und deutschen Filmrecht unter besonderer Beachtung der Rechte des Filmschauspielers, Dissertation Universität Wien 2009

Schmidtmann, Karin/Schwierig Sebastian, Datenschutzrechtliche Rahmenbedingungen bei Smart-TV, ZD 2014, 448 - 453

Schirmbacher, Martin, Online-Marketing- und Social-Media-Recht, 2. Auflage, Verlag MITP, Frechen 2017

Schwartmann, Rolf (Hrsg), Praxishandbuch Medien, IT- und Urheberrecht, 4. Auflage, Verlag C.F Müller, Heidelberg 2018

Simitis, Spiros (Hrsg), Bundesdatenschutzgesetz, 8. Auflage, C.H. Beck Verlag, München 2014

Specht, Louisa, Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2016, 288 – 296

Spindler, Gerald/Schuster, Fabian (Hrsg), Recht der elektronischen Medien, 3. Auflage, C.H. Beck Verlag, München 2015

Stiemerling, Oliver/Lachenmann, Matthias, Erhebung personenbezogener Daten beim Aufruf von Webseiten - Notwendige Informationen in Datenschutzerklärungen, ZD 2014, 133 – 136

Venzke-Caprarese, Sven, Retargeting in der Onlinewerbung, DuD 2017, 577 – 582

Voigt, Paul/Alich, Stefan, Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber, NJW 2011, 3541 – 3544

Zimmeck, Sebastian/Li, Jie/Hyungtae, Kim/Bellovin, Steven/Jebara, Tony, A Privacy Analysis of Cross-device Tracking, published in SEC'17 Proceedings of the 26th USENIX Conference on Security Symposium, August 2017, 1391-1408