Recht und Technik – Datenschutz im Diskurs

Rüdiger Grimm[1], Gerrit Hornung[2], Christoph Sorge[3], Indra Spiecker genannt Döhmann[4]

Vorwort zu den Workshopbeiträgen

Der Workshop „Recht und Technik – Datenschutz im Diskurs“ ist nach acht Jahren ein kontinuierlicher und fester Bestandteil der Jahrestagung der Gesellschaft für Informatik. Letztes Jahr hatte er pandemiebedingt erstmals online stattgefunden. Zu unserer Freude wurde es trotz der Online-Distanz ein sehr lebendiger Workshop. Im Übrigen war es einer der bestbesuchten Workshops der ganzen Jahrestagung 2020.

Auch dieses Mail findet der Workshop wieder wie die ganze Jahrestagung 2021 online statt. Inhaltlich bleibt die Ausrichtung wie gewohnt: Wir bieten ein Forum für Beiträge von Informatiker/innen, Juristen/innen und Vertreter/innen benachbarter Fächer, die an Fragestellungen des technikbasierten Datenschutzes arbeiten. Wie schon in den Vorjahren werden Themen adressiert, die anwendungsorientiertes Potential für interdisziplinären Diskurs und Zusammenarbeit bieten und die Möglichkeiten aufzeigen, wie Datenschutz durch Technik präzisiert und umgesetzt werden kann.

Der Workshop setzt an den theoretischen und praktischen Aspekten des Schutzes von Daten und Privatheit und der europäischen Datenschutz-Grundverordnung an. Konkret werden datenschutzrechtliche und zugehörige technische Probleme folgender Anwendungsbereiche und Verarbeitungsmethoden thematisiert

- Digitale Wirtschaft
- Smart Cities
- Videoüberwachung
- Videokonferenzen
- Data Mining
- Datenextraktion von Webseiten
- Upload Filter
- Cookies

[1] Fraunhofer SIT Darmstadt und Universität Koblenz-Landau <grimm@uni-koblenz.de>
[2] Universität Kassel <Gerrit Hornung <gerrit.hornung@uni-kassel.de>
[3] Universität des Saarlandes <christoph.sorge@uni-saarland.de>
[4] Goethe-Universität Frankfurt am Main <spiecker@jur.unifrankfurt.de>

Die Beiträge, die wir aus der Vielzahl an qualitätsvollen Einreichungen in einem *peer-reviewed*-Verfahren mit Unterstützung unserer Gutachter/innen auswählen konnten, zeigen die thematische und disziplinären Bandbreite der derzeit im Spannungsfeld von Recht und Technik diskutierten Themen; die Einreichungen gingen darüber noch hinaus. Die zunehmende Regulierung der Digitalisierung, die Konkretisierung der DSGVO-Anforderungen und ein insgesamt gestiegenes Bewusstsein dafür, dass nicht alles technisch Machbare auch gesellschaftlich wünschenswert ist, spiegeln sich in den Beiträgen wieder. Neben sehr konkreten Vorschlägen zur Bewältigung von Einzelproblemen sind auch Beiträge mit übergreifenden Einsichten repräsentiert.

Gerade die Entwicklung der Corona-App hat zudem gezeigt, dass gesellschaftliches Bewusstsein für den Datenschutz sehr wohl vorhanden ist und sich in erheblicher Einflussnahme auf den politischen Prozess niederschlägt. Das Vorgehen illustriert zudem, dass aus den Erkenntnissen von Recht und Technik sehr wohl konstruktive technische Lösungsmöglichkeiten für rechtliche Probleme erwachsen können, die gleichzeitig die Privatheit der Nutzer/innen stärken und einen Markt für neue Produkte kreieren.

In diesem Sinne freuen wir uns mit der Veröffentlichung der Beiträge des diesjährigen Workshops darauf, auch im nächsten Jahr wiederum „Recht und Technik – Datenschutz im Diskurs“ anzubieten.

Unser besonderer Dank gilt den Mitgliedern des Programmkomitees, unter denen in diesem Jahr folgende Personen in die Begutachtung eingebunden waren:

• Matthias Bäcker, Universität Mainz
• Franziska Boehm, KIT
• Jens-Matthias Bohli, Hochschule Mannheim
• Katharina Bräunlich, Diez
• Matthias Enzmann, Fraunhofer SIT, Darmstadt
• Christian Geminn, Universität Kassel
• Nils Gruschka, Universität Oslo
• Christoph Gusy, Universität Bielefeld
• Niko Härting, Rechtsanwalt, Berlin
• Walter Hötzendorfer, Research Institute Digital Human Rights Center, Wien
• Thomas Kahler, DPOblog.eu
• Ronald Petrlic, TH Nürnberg
• Burkhard Schafer, Universität Edinburgh
• Tobias Singelnstein, Ruhr-Universität Bochum
• Jürgen Taeger, Universität Oldenburg

Alles akzeptieren oder Einstellung(en) ändern? – zum Stand der Praxis bei der Nutzung von Cookies

Stefan Grombacher[1,2], Tobias Straub[2]

Abstract: Die Verwendung von Cookies auf Webseiten unterliegt der E-Privacy-Richtlinie bzw. ihrer Umsetzung in nationales Recht sowie der Datenschutz-Grundverordnung. Vorliegend wurden für die 500 am häufigsten aus Deutschland genutzten Webseiten die Dialoge untersucht, mit deren Hilfe um die nötige Einwilligung ersucht wird. Dabei zeigt sich deutlich, dass die Ausgestaltungen vielfach weniger die Bedürfnisse der Nutzenden berücksichtigen und eher versuchen, diese im Sinne der Webseitenbetreiber zu beeinflussen. Es wird diskutiert, inwiefern die in der Praxis verwendeten Mechanismen im Widerspruch zu den rechtlichen Vorgaben stehen könnten.

Keywords: Consent Management Platform, Cookie-Banner, Dark Patterns, DS-GVO, Einwilligung, E-Privacy-Richtlinie, erforderliche/nicht erforderliche Cookies, Telemediengesetz

1 Einleitung

Kaum eine Webseite kommt heute ohne einen Mechanismus aus, der über die jeweiligen Cookies informiert und um Zustimmung zu ihrer Verwendung ersucht. Von Nutzerinnen und Nutzern werden derartige Banner oftmals als störend wahrgenommen.[3] Um schnell zum eigentlichen Inhalt der Webseite vorzustoßen, wird den Dialogen daher wenig Aufmerksamkeit [No20] geschenkt, auch gibt es einige Implementierungen von Browser Add-Ons, die versuchen, die Dialoge von vornherein zu unterdrücken [Ut19]. Aufgrund der Dialoggestaltung besteht der schnellste Weg häufig darin, vorgeschlagene Konfigurationen oder gleich alle Cookies zu akzeptieren – was dann aber eher den Präferenzen des Seitenbetreibers und der Werbewirtschaft entsprechen dürfte, als jenen der Nutzenden [MB20].

Auch die Verbraucherschutz- und Netzpolitik hat die Thematik jüngst im Entwurf der Bundesregierung für ein Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG-E) aufgegriffen.[4] Dass angesichts der noch immer ausstehenden E-Privacy-Verordnung Unsicherheit und

[1] NTT DATA Deutschland GmbH, Hans-Döllgast-Straße 26, D-80807 München, stefan.grombacher@nttdata.com
[2] Duale Hochschule Baden-Württemberg, Center for Advanced Studies, Bildungscampus 13, 74076 Heilbronn, tobias.straub@dhbw-stuttgart.de
[3] https://www.bitkom.org/Presse/Presseinformation/Cookie-Banner-stoeren-Internetnutzer.html (25.07.2018)
[4] Gesetzentwurf der Bundesregierung, Stellungnahme im Bundesrat (26.03.2021) https://www.hamburg.de/bjv/pressemeldungen/14984108/2021-03-25-bjv-cookie-banner-im-internet/ (25.03.2021), Gesetzentwurf: https://www.bundesrat.de/SharedDocs/drucksachen/2021/0101-0200/163-21.pdf?__blob=publicationFile&v=1, BT-Drs. 163/21, § 24

ein Klärungsbedarf für Betreiber besteht, zeigen im europäischen Kontext die bereits von der französischen Aufsichtsbehörde verhängten hohen Bußgelder aufgrund unzureichender Cookie-Banner [Kl20].

Die Gestaltung der Dialoge und der Umgang mit ihnen war bereits Gegenstand von Feld- [Ut19] und Laborstudien mit Nutzenden [MB20, No20], Lösungsvorschläge in Form eines Best Practice-Modells wurden von [KTS20] entwickelt. Die Frage, inwieweit auf Webseiten inner- und außerhalb der EU mittels Cookies ein Tracking ohne Einwilligung erfolgt, wurde von [MBS20, Sa19, Tr19] mit Hilfe automatisierter Werkzeuge untersucht. Der vorliegende Beitrag kombiniert einen vergleichbaren Ansatz mit einer manuellen Analyse (ähnlich derer in [So20] für Online-Nachrichtenseiten), um die 500 am häufigsten aus Deutschland genutzten Webseiten zu untersuchen.[5]

2 Zusammenfassung der Rechtslage

Im Folgenden wird die Rechtslage, soweit für das Verständnis des Beitrags erforderlich, skizziert. Für eine ausführlichere Darstellung wird auf die rechtswissenschaftliche Literatur verwiesen; einen guten Überblick gibt etwa [RE21].

Ursprünglich war geplant, dass 2018 zeitgleich mit dem neuen Datenschutzrecht in Form der EU-Datenschutz-Grundverordnung (DS-GVO) auch eine E-Privacy-Verordnung in Kraft treten sollte. Das Gesetzgebungsverfahren zur E-Privacy-Verordnung, welche die *E-Privacy-Richtlinie* (2002/58/EG, zuletzt geändert durch die „Cookie-Richtlinie" 2009/136/EG) ablösen sollte, ist aber ins Stocken geraten. Insofern sind aktuell die Regelungen der E-Privacy-Richtlinie (nachfolgend: RL) und ihre – lange in Frage stehende – Umsetzung in nationales Recht maßgeblich. Für eine Klarstellung hinsichtlich der Regelungen im Telemediengesetz (TMG) sorgte hierbei im Mai 2020 ein Grundsatzurteil des BGH.[6]

2.1 Erfordernis der Einwilligung

Cookies fallen unter Art. 5 Abs. 3 RL, da es sich dabei um Informationen handelt, die auf einem Endgerät eines Teilnehmers oder Nutzers gespeichert oder von dort gelesen werden. Diese Vorschrift ist wohlgemerkt unabhängig davon anzuwenden, ob die Informationen einen Personenbezug haben.

Nutzt eine Webseite Cookies, so muss der Betreiber gemäß der RL eine informierte Einwilligung einholen, es sei denn, es handelt sich um ein *technisch notwendiges* Cookie

[5] Nach Einreichung dieses Beitrags wurde bekannt, dass NOYB eine Software entwickelt hat, um automatisiert Rechtsverstöße bei der Nutzung von Cookies zu erkennen und Beschwerden zu formulieren (https://noyb.eu/en/project/cookie-banners, Stand: 31.05.2021).

[6] Az. I ZR 7/16; siehe etwa [Sp20] für eine ausführliche Darstellung.

(s.u.). Laut BGH ist die Formulierung[7] in § 15 Abs. 3 TMG richtlinienkonform derart auszulegen, dass damit das Einwilligungserfordernis der RL als in nationales Recht umgesetzt gelten kann. Die RL verweist (indirekt[8]) auf die DS-GVO hinsichtlich der Informationspflichten (Art. 12 ff.) sowie der Ausgestaltung der Einwilligung (Art. 4 Nr. 11, Art. 6 Abs. 1 S.1 lit. a., Art. 7) und betont, dass insbesondere klar und umfassend über die Zwecke der Verarbeitung informiert werden muss.

2.2 Anforderungen an die Gestaltung der Interaktion

Zum Teil sind Cookie-Hinweise als Einblendung am Rand ausgestaltet, die sich ignorieren lassen und eine Nutzung der Webseite ohne Unterbrechung ermöglichen. Ein derartiges konkludentes Verhalten genügt aber nicht den Anforderungen an eine aktiv zu erteilende Einwilligung [Sp20]. Dem Urteil des BGH zufolge ist beim Ersuchen um eine Einwilligung insbesondere auch eine Dialogform unzulässig, bei der Checkboxen vorausgewählt sind und erst deaktiviert werden müssen, wenn eine Einwilligung verweigert werden soll (*Opt-out*).

Hinsichtlich der optischen und textuellen Gestaltung der Dialoge lässt sich eine hohe Variabilität beobachten, da sich z.B. auch die von dafür spezialisierten Dienstleistern bezogenen Consent Management Tools (s.u.) von den Webseitenbetreibern anpassen lassen. Teilweise wird durch als *Dark Patterns*[9] bezeichneten Designprinzipien (in unterschiedlicher Abstufung) versucht, Nutzende zu Handlungen zu verleiten, die ihren eigenen Interessen zuwiderlaufen. Als unzulässig werden dabei Designs angesehen, die auf der ersten Ebene keine echte Wahl lassen und für die Ablehnung der Einwilligung einen zusätzlichen Klick erfordern, wohingegen strittig ist, inwieweit dies auch für die rein optische Hervorhebung der vom Betreiber bevorzugten Option gilt [RE21 mwN].

2.3 Zusammenspiel von RL und DS-GVO

Wie oben aufgeführt, sind im Kontext von Cookies hinsichtlich des „Wie“ der Einwilligung i.S.v. § 15 TMG die Vorschriften der DS-GVO anzuwenden.

Uneinheitlich wird in der Literatur dagegen das genaue Verhältnis von RL und DS-GVO beschrieben. Art. 95 DS-GVO wird der hM nach so verstanden, dass die Vorgaben der RL (bzw. ihrer Umsetzungen in nationales Recht) jene der DS-GVO verdrängen, wenn beide konkurrierende Pflichten enthalten, die dasselbe Ziel verfolgen [BH20, PK20]. Dagegen sehen [RE21] bei Cookies, die personenbezogene Daten verarbeiten, eine aufgrund von § 15 TMG nötige Einwilligung wegen der Verweisung auch als Rechtsgrundlage für die

[7] entgegen dem Wortlaut „sofern der Nutzer dem nicht widerspricht“
[8] Über Art. 94 Abs. 2 Satz 1 DS-GVO.
[9] Eine Zusammenfassung der Taxonomien aus der Literatur enthält [LS21]. Beispiele und weiterführende Literatur finden sich z.B. beim Dark Pattern Detection Project (http://www.dapde.de/).

Verarbeitung gem. Art. 6 Abs. 1 S. 1 lit. a DS-GVO an, während bei technisch notwendigen Cookies auch eine andere Rechtsgrundlage (insb. Art. 6 Abs. 1 S. 1 lit. b oder lit. f) in Frage käme.

Verarbeitungen personenbezogener Daten durch Webseitenbetreiber unterfallen, sofern es nicht nur die in Art. 5 Abs. 3 RL genannten Verarbeitungsformen Speichern und Abrufen betrifft, den allgemeinen Vorgaben der DS-GVO [BH20], d.h. insbesondere den Rechtmäßigkeitsvoraussetzungen gem. Art. 6 Abs. 1 (bzw. Art. 9 Abs. 2, sofern es sich um sensitive Daten handelt).

2.4 „Erforderliche“ Cookies

Hinsichtlich der Frage, welche Cookies als erforderlich gelten können und somit unter den Ausnahmetatbestand von Art. 5 Abs. 3 Satz 2 RL fallen, wird häufig auf eine ältere Stellungnahme der Aufsichtsbehörden verwiesen, die folgende Arten umfasst [Gi20,RE21].

- Cookies zur Fehleranalyse
- Session-Cookies für Onlineformulare oder Warenkörbe
- Authentifizierungscookies für eine Browsersitzung
- Sicherheitscookies
- Multimedia-Player-Sitzungscookies
- Lastverteilungs-Sitzungscookies
- Cookies zur vom Nutzer angeforderten Anpassung der Benutzeroberfläche
- Content-Sharing-Cookies sozialer Plug-ins in Bezug auf beim Netzwerk angemeldete Nutzer

Nach Auffassung der französischen Aufsichtsbehörde (CNIL) können zu dieser Kategorie auch Cookies für eine „einfache“ Webanalyse zählen, bei der nur *anonyme* Auswertungen erstellt werden, wobei die Nutzenden informiert werden und die Möglichkeit zum Widerspruch haben müssen.[10]

3 Cookie-Banner in der Praxis

Auch wenn dies unter dem Aspekt der Transparenz und Benutzbarkeit erstrebenswert wäre, hat sich bislang kein einheitliches Format für Cookie-Dialoge etabliert. Nachfolgend werden daher zunächst Kriterien genannt, anhand derer sich die bestehenden Ansätze unterscheiden lassen. Das Gros der Webseiten bindet eine Lösung eines Consent Management Providers (CMP, auch Consent Management Platform) zum Verwalten der Einstellungen ein. Auf diese Systeme sowie die technische Spezifikation, auf der sie typischerweise basieren, geht der zweite Abschnitt ein.

[10] Art. 5, Délibération n° 2019-093, 4.7.2019

3.1 Unterscheidungskriterien

Hinsichtlich des generellen *Interaktionsmusters* lassen sich die Cookie-Banner in zwei Hauptgruppen unterteilen:

1. Zunächst einmal gibt es reine *Info-Banner*, welche vor allem vor Inkrafttreten der DS-GVO gebräuchlich waren und typischerweise darauf hinweisen, dass die jeweilige Webseite Cookies enthält, deren Verwendung man durch die weitere Nutzung der Seite zustimme.
2. Eine Möglichkeit zur echten Entscheidung zwischen Ablehnung und Zustimmung bieten dagegen erst *Consent-Banner*, wobei sich diese weiter unterscheiden lassen:
   a) Vorschaltseiten und modale Dialoge verlangen eine unmittelbare Reaktion und machen es – zumindest ohne Manipulation der Seite – unmöglich, diese zu nutzen, bevor man mit dem Dialog interagiert hat und seine Zustimmung oder Ablehnung durch eine aktive Handlung zum Ausdruck gebracht hat.
   b) Daneben gibt es auch nicht-modale Dialoge, welche aber bei manchen Webseiten wesentliche Teile des Inhalts verdecken und somit indirekt doch zu einer Handlung zwingen. In der Theorie sollte es jedoch so sein, dass ohne eine explizite Handlung auch keine einwilligungspflichtigen Cookies gesetzt werden dürfen, d.h. ein Ignorieren des Banners einer Ablehnung der Einwilligung gleichkommen muss.

Einen Einfluss auf den *Grad der Beeinflussung* von Nutzenden haben die vom Dialog vorgesehenen Interaktionspfade sowie die textuelle (Wortwahl, Umfang, Verständlichkeit) und visuelle Gestaltung der Oberfläche. Eine Beeinflussung der Nutzenden wird im Englischen auch als *Nudging* bezeichnet [Ut19]. Erfolgt eine solche entgegen der Interessen der Nutzenden, so spricht man von den erwähnten Dark Patterns. Bei einem neutralen Design sind die Annahme und Verweigerung der Einwilligung als gleichwertige Alternativen visualisiert.

3.2 Consent Management Provider

Um die Zustimmungssysteme hat sich eine eigene Dienstleistungsbranche von Anbietern gebildet, die Consent-Banner bereitstellen. Zu den bekanntesten gehören Cookiebot, OneTrust, Quantcast und SourcePoint. Das Funktionsprinzip ist dabei jeweils, dass ein Betreiber seine Webseite automatisch vom Anbieter auf die verwendeten Cookies scannen und diese vorkategorisieren lassen kann. Die Systeme erlauben ein Customizing und Branding der Dialoge gemäß den Vorstellungen des Webseitenbetreibers. Sie werden per JavaScript eingebunden, wobei der Betreiber selbst darauf zu achten hat, dass am Ende das Zusammenspiel mit eigenem Skript-Code und den tatsächlich gesetzten Cookies rechtskonform ist und insbesondere keine Cookies gesetzt werden, bevor der Dialog beantwortet wurde.

Das vom Interactive Advertising Bureau (IAB Europe), einem internationalen Wirtschaftsverband der Onlinewerbebranche, entwickelte *Transparency & Consent Framework* (TCF)[11] ist eine technische Spezifikation, gemäß der die Zustimmung von Nutzenden rechtskonform eingeholt, gespeichert und an Werbetreibende mitgeteilt werden kann. Dazu wurden CMPs als neue Beteiligte eingeführt, die sich, wie auch die Werbetreibenden, bei IAB Europe registrieren müssen. Das Framework definiert u.a. ein einheitliches Format eines *Consent String* zur Speicherung der von den Nutzenden geäußerten Präferenzen, welcher vom CMP verwaltet und Werbetreibenden über standardisierte Schnittstellen zugänglich gemacht wird. Die 2019 durchgeführte Untersuchung von [MBS20] ergab allerdings, dass etwa bei der Hälfte der Webseiten trotz des Einsatzes eines TCF-kompatiblen CMPs ein nicht richtlinienkonformes Verhalten vorlag.

4 Untersuchung

Ziel der empirischen Untersuchung war es festzustellen, wie die aus Deutschland am häufigsten genutzten Webseiten Cookie-Banner einsetzen. Konkret sollten dabei jeweils folgende Fragen aus Sicht von datenschutzsensiblen Nutzerinnen und Nutzern beantwortet werden:

1. Wie *aufwändig* ist das Ablehnen aller Cookies im Gegensatz zum Akzeptieren?
2. Erfolgt eine *Beeinflussung* der Nutzenden durch die Gestaltung des Banners?
3. (Wie einfach) ist es möglich, den *Einstellungs-Dialog* beim Besuch der Webseite später erneut aufzurufen?
4. Werden bereits *Cookies gesetzt*, ohne dass mit dem Banner interagiert wurde?

4.1 Methodik

Um eine einheitliche und zumindest teilautomatisierte Auswertung zu ermöglichen, wurden die Begriffe dabei wie folgt operationalisiert:

1. Der Aufwand wird in der mindestens erforderlichen Zahl von Mausaktionen, wozu Klicks oder Scrollvorgänge (unabhängig von deren Länge) zählen, für die Ablehnung aller (nicht notwendigen) Cookies gemessen.
2. Der Grad der Beeinflussung wird anhand der Farbgebung, Größe und Anordnung der Steuerelemente im Dialog untersucht.
3. Die Zahl der Mausaktionen zum Aufruf des Einstellungs-Dialogs wird ermittelt.

[11] https://iabeurope.eu/tcf-2-0/ (Stand vom: 21.08.2019)

4. Es wird untersucht, ob 3rd Party Cookies gesetzt werden, ohne dass eine User Interaktion stattfindet.

Als Untersuchungsgegenstand wurden alle im Ranking von Alexa[12] (Stand: 06.01.21) unter den Top 500 gelisteten Webseiten betrachtet, unabhängig davon, ob es sich dabei um deutsch- oder rein fremdsprachige Angebote handelte. Am selben Tag wurden zunächst automatisiert Screenshots der Startseiten[13] aller Webseiten in der Liste aufgenommen (Browser: Chrome, Bildschirmauflösung: 1920 ´ 1080 Pixel, standardmäßige Zoomstufe 100%). Dies erfolgte durch ein JavaScript-Programm, welches Webseitenaufrufe mittels Protractor,[14] einem Framework für automatisierte Browser-Tests, simulierte.

Diese Screenshots wurden anschließend manuell untersucht, um festzustellen, welche Webseiten überhaupt Banner einsetzen. Die Webseiten, welche ein Consent-Banner einbinden, wurden dann einzeln manuell daraufhin untersucht, wie viele Mausklicks benötigt werden, um alle Cookies abzulehnen.

Gleichzeitig wurde für die Consent-Banner auch manuell vermerkt, ob und welche Techniken der Beeinflussung bei der Gestaltung der Steuerelemente (Links oder grafische Buttons) zum Einsatz kommen. Sofern ein Button zur Ablehnung (oder zum Akzeptieren einer Vorauswahl ausschließlich notwendiger Cookies) vorhanden war, wurde dieser mit dem Annahme-Button verglichen. War kein Ablehne-Button vorhanden, wurde der Annahme-Button mit demjenigen Button verglichen, welcher auf die zweite UI-Schicht führt. Falls das Ablehnen nur über die zweite UI-Schicht möglich war, wurde diese entsprechend untersucht. Es wurden in dem Fall wieder der Button zum Annehmen mit dem Button zum Ablehnen bzw. zum Akzeptieren der Vorauswahl ausschließlich notwendiger Cookies verglichen.

- Als tendenziös wurde eine *Farbgebung* gewertet, bei der sich der Button für die Annahme im Vergleich zu jenen für die Alternativen deutlich wahrnehmbarer vom Hintergrund des Banners abhob. Darunter fallen insbesondere Varianten, bei denen die Alternativen nur mit Grautönen oder gar nicht hinterlegt sind.
- Analog wurde auf das Vorliegen eines unausgewogenen *Größenverhältnisses* der Steuerelemente geprüft. Ein solches liegt v.a. dann vor, wenn eine der Alternativen nur als verlinkter Text realisiert wurde oder so erscheint, weil es sich zwar um einen Button handelt, dieser aber keinen erkennbaren Rahmen und die gleiche Farbe wie der Hintergrund des Banners hat.
- Eine Beeinflussung durch die *Positionierung* liegt vor, wenn sich das Steuerelement für das Ablehnen bzw. für das Betreten der zweiten UI-Schicht nicht an einer ver-

[12] https://www.alexa.com/topsites/countries/DE
[13] Die URL wurde aus dem Domainnamen ohne Pfadangabe sowie dem Schema „http“ zusammengesetzt.
[14] https://www.protractortest.org, verwendete Version: 5.4.2

gleichbaren Stelle befindet wie der Annahme-Button, beispielsweise wenn das Ablehnen nur durch einen in den Fließtext eingebetteten Link zu erreichen ist oder wenn auf der zweiten UI-Ebene das Steuerelement zum Akzeptieren aller Cookies sichtbar ist, während für die Wahl ausschließlich notwendiger Cookies ein Scrollen nötig ist.

Zur Untersuchung des dritten Kriteriums wurden jene Webseiten manuell untersucht, welche ein Consent-Banner eingebunden hatten. Es wurde dabei ermittelt, wie viele Mausaktionen erforderlich sind, lediglich um den Dialog wieder aufzurufen (ohne dann die getroffene Auswahl zu ändern). Falls kein Link mit einer gängigen Bezeichnung (etwa „Cookies“, „Cookie-Einstellungen“, „Einwilligung“, „Datenschutz“, „Privacy“) im Header oder Footer der Webseite oder deren Impressum vorhanden war und auch keine vergleichbare Funktion innerhalb von drei Minuten gefunden werden konnte, um den Dialog wieder zu öffnen, wurde der Versuch aufgegeben. Der Aufwand, den Nutzende hierfür zu investieren bereit sind, dürften in aller Regel recht begrenzt sein. Das Kriterium wurde nicht als erfüllt angesehen, wenn eine Webseite etwa Hinweise auf eine manuelle Löschung von Cookies über Browserfunktionen enthält oder darauf verweist, es aber selbst nicht möglich ist, den eigentlichen Dialog wieder aufzurufen.

Die Untersuchung, welche Cookies schon vor Interaktion mit einem Banner gesetzt werden, konnte wiederum vollautomatisiert ablaufen. Da aufgrund der Same-Origin Policy per JavaScript nicht auf die von einer dritten Seite gesetzten Cookies zugegriffen werden kann, wurde der Ansatz gewählt, stattdessen direkt die von Chrome zur Speicherung der Cookies verwendete SQLite-Datenbank auszuwerten, welche vor jedem Aufruf einer Webseite bereinigt wurde. Konkret wurden die einzelnen Webeseiten wieder mittels Protractor aufgerufen, jedoch keine weitere Aktion veranlasst. Nach 50 Sekunden Wartezeit wurde vom Protractor-Skript die Chrome-Datenbank mit Hilfe des Packages sqlite3[15] ausgelesen und die gefundenen 3rd Party Cookies zur späteren Auswertung in eine JSON-Datei geschrieben.

Eine Bewertung, ob es sich bei einem Cookie um ein notwendiges oder nicht-notwendiges im Sinne der RL handelt, ist auf automatisierte Weise schwerlich möglich. Als Annäherung wurde die vereinfachende Annahme getroffen, dass es sich bei 3rd Party Cookies, die keine Session Cookies sind, typischerweise um nicht-notwendige handeln dürfte. Bei den vorhandenen persistenten Cookies wurde auch die vom Server initial[16] gesetzte Gültigkeitsdauer ermittelt.

4.2 Ergebnisse

Von den 500 berücksichtigten Seiten wiesen 219 ein Consent-Banner, 61 ein reines Info-Banner und 211 keines von beidem auf. Neun Seiten waren zum Testzeitpunkt nicht

[15] https://www.npmjs.com/package/sqlite3, verwendete Version: 5.0.1

[16] Der Standard (RFC6265, https://tools.ietf.org/html/rfc6265) lässt es prinzipiell zu, dass ein Server, an den ein Cookies zurückgeschickt wird, dessen Gültigkeitsdauer modifiziert.

erreichbar. Im Anhang ist in Tab. 1 für die Seiten mit Consent-Banner näher aufgeschlüsselt, wie groß der Aufwand für die Einwilligung bzw. ihre Verweigerung ist, welche irreführenden Designs zum Einsatz kommen und wie leicht sich die Einstellungen später verändern lassen.

Art des Banners
Die Tatsache, dass einige Webseiten nach wie vor kein Banner oder nur ein Info-Banner anzeigen, ist zunächst überraschend. Allerdings handelt es sich dabei in vielen Fällen um fremdsprachige Seiten aus dem Ausland wie z.B. aparat.com oder um solche mit pornografischen oder rechtlich fragwürdigen Inhalten (z.B. s.to). Nicht untersucht wurde, ob Seiten aus der Gruppe ohne jegliches Banner vielleicht nicht doch ausschließlich notwendige (oder gar keine) Cookies verwenden, aller Erfahrung nach dürfte dies aber eher die Ausnahme sein.

Aufwand
Die vorherrschende Ausgestaltung (70%; 154/219) des Consent-Banners als modaler Dialog, der die Webseite solange sperrt, bis eine Aktion der Nutzerin erfolgt ist, und die dabei häufige (82,8%; 127/154) Erschwernis der Ablehnung deuten darauf hin, dass Betreiber sich höhere Zustimmungsraten erwarten, indem sie Nutzenden die Möglichkeit nehmen, den Besuch der Seite mit geringem Aufwand fortzusetzen. Zu den Webseiten, die keine Möglichkeit bieten, Cookies abzulehnen, gehören Zeitungen und Nachrichtenmagazine wie z.B. spiegel.de, die aber einen alternativen Zugang gegen Bezahlung anbieten (so genannte *Tracking Wall*).

Dark Patterns im UI
Die große Mehrzahl (85,8%; 188/219) der Seiten mit Consent-Banner nutzt eine oder mehrere Techniken der UI-Gestaltung, um Nutzenden in ihrem Sinne zu beeinflussen. Dem gegenüber steht ein verschwindend geringer Anteil (3,2%) dieser Seiten, die dabei wenigstens eine 1-Klick-Ablehnung ermöglichen.

Wiederauffindbarkeit des Einstellungs-Dialogs
Nur bei 39,6% der Seiten genügen eine oder zwei Mausaktionen zum erneuten Aufruf des Dialogs, so dass sich Nutzende ihre beim ersten Seitenbesuch getroffenen Festlegungen ansehen und in der Folge ggf. anpassen können. Zwei Mausaktionen sind in dieser Hinsicht als akzeptabel anzusehen, da nicht erwartet werden kann, den Dialog von überall auf der Seite mit einem Klick zu erreichen und die erste Aktion meist im Scrollen ans Seitenende besteht, wo typischerweise z.B. auch ein Link zum Impressum zu finden ist.

Ohne Einwilligung gesetzte Cookies
Tab. 2 zeigt, wie viele persistente Cookies ohne Zutun des Nutzenden gesetzt werden. Da eine automatisierte Feststellung deren Zwecke nicht möglich war, werden hier nur 3rd Party Cookies gezählt, da diese viel eher für Werbung und Tracking eingesetzt werden als 1st Party Cookies. Zugunsten der Betreiber wird davon ausgegangen, dass eines der 3rd

Party Cookies vom Einsatz der Reichweitenmessung[17] oder eines externen CMP-Tools herrührt und somit als „erforderlich“ gelten kann. Dennoch ist bei ca. einem Drittel der Seiten mit Consent-Banner das Verhalten hinsichtlich automatisch gesetzter 3rd Party Cookies zumindest auffällig und sollte näher überprüft werden.[18] 3rd Party Cookies mit einer Gültigkeit von über einem Jahr wurden ohne Zutun nur in wenigen Fällen gesetzt, wenn Consent-Banner (7,8%; 17/219) bzw. Info-Banner (18%; 11/61) verwendet werden. Dagegen ist der Anteil von Seiten mit solch langlebigen Cookies mit 37,0% (78/211) deutlich höher in der Gruppe jener Seiten, die gar keine Banner enthalten.

5 Diskussion

Mit Hilfe eines teil-automatisierten Ansatzes wurden die Praktiken im Umgang mit Cookies der in Deutschland am häufigsten genutzten Webseiten untersucht. Wie erwähnt, sind die Ergebnisse mit einer gewissen Unschärfe behaftet. Einerseits wurde nicht überprüft, ob die Webseitenbetreiber tatsächlich dem Anwendungsbereich von RL bzw. DS-GVO unterliegen. Andererseits konnten die tatsächlichen Zwecke einzelner Cookies nicht festgestellt werden, so dass vereinfachende Annahmen getroffen werden mussten. Auch wurden ausschließlich Cookies als Technologie berücksichtigt und andere Methoden wie *Tracking Pixels* oder *Browser Fingerprinting* außer Acht gelassen. Dennoch lassen sich einige Erkenntnisse ableiten, die bei der Beurteilung der Frage, welche Gestaltungs- und Realisierungsvarianten rechtlich zulässig sind, Berücksichtigung finden sollten:

- Consent-Banner werden vorwiegend als **modale Dialoge** ausgestaltet, die die unmittelbare Aufmerksamkeit der Nutzenden verlangen. Ein Konflikt könnte sich dadurch mit *Erwägungsgrund 32 Satz 6* der DS-GVO ergeben, welcher fordert, dass bei Einwilligungen auf elektronischem Wege die Aufforderung hierzu ohne unnötige Unterbrechung des Dienstes zu erfolgen hat. Während die Nutzenden beim Besuch der Seite ohne Einschränkungen der Funktionalität auf die nicht erforderlichen Cookies verzichten könnten, wird ihnen der bequemste Weg, das Banner zu ignorieren, wenn sie keine Einwilligung erteilen möchten, verwehrt.
- In den meisten Fällen ist eine **Verweigerung der Einwilligung aufwändiger als ihre Erteilung**, da dafür zwingend die zweite UI-Schicht aufgerufen werden muss. Es ist zu vermuten, dass sich die Betreiber dadurch höhere Zustimmungsraten erhoffen, da die Annahme nur mit einem Klick die für die Nutzenden aufwandsärmste Methode darstellt.[19] Angesichts der Tatsache, dass es technisch problemlos möglich

[17] z.B. durch INFOnline

[18] In [Tr19] wurde für im Zusammenhang mit der Identifikation von Tracking Cookies eine Heuristik verwendet, die darunter 3rd Party Cookies mit einer Gültigkeit von mindestens einem Monat versteht. Unter dieser Einschränkung reduziert sich im vorliegenden Datenmaterial der Anteil der Webseiten mit Consent-Banner und mindestens zwei 3rd Party Cookies auf lediglich 6%.

[19] Ein solcher Effekt auf die Entscheidung der Nutzenden wurde etwa in [No20] nachgewiesen.

ist, eine gleichrangige Wahl zwischen der kompletten Ablehnung und Annahme sowie Detaileinstellungen[20] anzubieten, muss hinterfragt werden, inwieweit der bestehende Mechanismus den Grundsätzen von *Privacy by Design* und *Privacy by Default* (Art. 25 DS-GVO) genügt – wird doch die datenschutzfreundlichste Alternative bewusst verkompliziert und die für die Nutzenden ungünstigste als die am einfachsten zugängliche gestaltet. Ab wann der unbestreitbar größere (zeitliche und kognitive) Aufwand für den Nutzenden schon als Nachteil, der einer „echten und freien" Wahl nach *Art. 4 Nr. 11 und Erwägungsgrund 42 Satz 5 DS-GVO* entgegensteht, zu werten ist, muss von der Rechtsprechung noch geklärt werden. In der Literatur und bei einigen Aufsichtsbehörden im europäischen Ausland wird diese Praxis [RE21] zufolge als unzulässig betrachtet. Die Analogie zum unerlaubterweise vorausgewählten Kästchen liegt jedenfalls nicht allzu fern (vgl. Abschnitt 2.2).

- Die sehr häufig festzustellende **irreführende optische Gestaltung** der Dialoge verleitet Besucherinnen und Besucher der Webseiten, eine Auswahl zu treffen, die ihren Interessen zuwiderläuft, wie auch Nutzerstudien gezeigt haben [Ut19, MB20]. Neben dem Grundsatz der Verarbeitung nach Treu und Glauben (*Art. 5 Abs. 1 lit. a DS-GVO*) berührt dies die grundlegenden Anforderungen aus *Art. 4 Nr. 11 DS-GVO*, dass eine Einwilligung informiert und unmissverständlich zu erfolgen hat.[21]

- Während in fast allen Fällen eine Einwilligung mit einem Klick erteilt werden kann, ist der **spätere Widerruf deutlich aufwändiger**, da mehrere Mausaktionen benötigt werden, um den Dialog erneut aufzurufen und dann dort die Einstellungen zu modifizieren. *Art. 7 Abs. 3 Satz 4 DS-GVO* fordert jedoch ausdrücklich, dass der Widerruf genauso einfach wie die Erteilung sein muss.

- Angesichts der **sehr großen Anzahl von 3rd Party Cookies**, die von manchen Webseiten automatisch gesetzt werden, ist es fraglich, ob all diese tatsächlich „erforderlich" im Sinne von *Art. 5 Abs. 3 RL* sind und etwa einem der in Abschnitt 2.4 aufgeführten Zwecke dienen. Mit dem Grundsatz der Datenminimierung (*Art. 5 Abs. 1 lit. c DS-GVO*) dürfte jedenfalls eine exzessive Übermittlung (in einem Fall wurden auf einer Seite mit Consent-Banner über 130 persistente 3rd Party Cookies gesetzt, ohne die Nutzerinteraktion abzuwarten) personenbezogener Daten ebenfalls schwerlich in Einklang zu bringen sein. (Möglicherweise lässt sich das Phänomen im Einzelfall aber auch schlicht durch eine nachlässige Implementierung erklären, bei der versäumt wurde, das Setzen von Cookies bis zur erteilten Einwilligung zu unterdrücken.)

[20] Diese Möglichkeit könnte aufgrund von Erwägungsgrund 32 Satz 5 geboten sein.

[21] Angesichts der sehr umfangreichen Informationen, die Dialoge bei manchen CMPs enthalten, drängt sich im Übrigen auch der Verdacht auf, dass damit der psychologischer Effekt ausgenutzt werden soll, dass Nutzende im Lichte einer überwältigenden Zahl von Einstellungsmöglichkeiten oft darauf verzichten, überhaupt eine Entscheidung zu treffen [RS20].

6 Fazit

Unter den untersuchten Webseiten, die Consent-Banner einsetzen, verzichtet nur eine Minderheit auf den Einsatz von mehr oder minder subtilen Mechanismen der Beeinflussung von Nutzenden, indem sie die typischerweise zum Einsatz kommenden CMP-Tools entsprechend konfiguriert. Erschwerend kommt hinzu, dass es kein gängiges Format für die Einwilligungsdialoge gibt (wie es etwa der Fall ist bei Berechtigungsanfragen des Browsers für Standortabfragen oder Kamera- und Mikrofonfreigaben). Selbst wenn die Praktiken der Webseitenbetreiber – nach gegenwärtiger Rechtslage – noch als zulässig gelten können, sind die Notwendigkeit eines datenschutzfreundlichen Designs und der Bedarf für unterstützende Werkzeuge klar erkennbar, um den Bedürfnissen der Nutzenden gerecht zu werden. Als Ansätze in diese Richtung sind etwa der ab 2012 eingeführte, mittlerweile aber in der Umsetzung als gescheitert geltende, optionale „do not track" (DNT)-Header im Browser[22] zu nennen oder die bislang unberücksichtigten Vorschläge des EU-Parlaments in der Diskussion um die ePrivacy-Verordnung.[23]

Die weitere technische Entwicklung sollte aber beobachtet werden, denn die Bedeutung von Cookies im Allgemeinen und 3rd Party Cookies im Besonderen könnte weiter nachlassen. Beispielsweise werden sie im Safari-Browser standardmäßig blockiert, während Google mit *FLoC* (Federated Learning of Cohorts) eine Technologie plant, bei der Nutzende aufgrund ihres Surfverhaltens durch den Browser selbst einer werberelevanten Zielgruppe zugeordnet werden sollen.

Literaturverzeichnis

[BH20] Böhm, W.; Halim, V.: Cookies zwischen ePrivacy und DS-GVO – was gilt?, MMR, S. 651-656, 2020.

[Gi20] Gierschmann, S.: Verwendung personenbezogener Daten – Cookie-Einwilligung II, MMR, S. 609-617. 2020.

[KTS20] Kettner, S.; Thorun, C.; Spindler, G.: Innovatives Datenschutz-Einwilligungsmanagement, https://www.bmjv.de/SharedDocs/Downloads/DE/News/PM/090720_Datenschutz.html?nn=6705022, Stand: 7.9.2020.

[Kl20] Kleinz, T.: Frankreich: Datenschützer verhängen Millionen-Bußgelder gegen Google und Amazon, heise online, https://heise.de/-4985956, News vom 10.12.2020.

[LS21] Luguri, J.; Strahilevitz, L. J.: Shining a light on dark patterns. Journal of Legal Analysis 13.1, S. 43-109, 2021.

[MB20] Machuletz, D.; Böhme, R.: Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. Proc. on Privacy Enhancing Technologies, S. 481-498, 2020.

[22] https://www.w3.org/TR/tracking-dnt/

[23] Amendment 106 ff. zu Artikel 10, https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html (Stand: 20.10.2017)

[MBS20] Matte, C.; Bielova, N.; Santos, C.: Do Cookie Banners Respect my Choice?: Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. Proc. IEEE Symposium on Security and Privacy, S. 791-809, 2020.

[No20] Nouwens, M. et al.: Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. Proc. CHI Conference on Human Factors in Computing Systems, S. 194-206, 2020.

[RE21] Rauer, N.; Ettig, D.: Update Cookies 2020 / Aktuelle Rechtslage und Entwicklungen, ZD, S. 18-24, 2021.

[RS20] Rieger, S.; Sinders, C.: Dark Patterns: Design mit gesellschaftlichen Nebenwirkungen. Stiftung Neue Verantwortung, https://www.stiftung-nv.de/sites/default/files/dark.patterns.pdf, 13.05.2020.

[Sa19] Sanchez-Rola, I. et al.: Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. Proc. ACM Asia Conference on Computer and Communications Security, S. 340-351, 2019.

[So20] Soe, T.H. et al.: Circumvention by design – dark patterns in cookie consent for online news outlets. Proc. Nordic Conference on Human-Computer Interaction, S. 1-12, 2020.

[Sp20] Spindler, G.: Klarheit für Cookies, NJW, S. 2513-2517, 2020.

[Tr19] Trevisan, M. et al.: 4 Years of EU Cookie Law: Results and Lessons Learned. Proc. on Privacy Enhancing Technologies, S. 126-145, 2019.

[Ut19] Utz, C. et al.: (Un) informed consent: Studying GDPR consent notices in the field. Proc. ACM SIGSAC Conf. on Computer and Communications Security, S. 973-990, 2019.

Anhang

Aufwand		(absolut)
Annehmen mit 1 Klick	99,5%	218
Ablehnen möglich	95,4%	209
mit 1 Klick	20,1%	44
2 Klicks	53,0%	116
3 oder mehr Klicks	22,4%	49
Ablehnen nicht möglich	4,6%	10
Dark Patterns im UI		
Farbe	82,6%	181
Größe	36,1%	79
Anordnung	24,7%	54
mindestens eine Form der *Beeinflussung*	85,8%	188
Wiederauffindbarkeit des Einstellungs-Dialogs		
möglich	87,7%	192
mit 1 Mausaktion	4,6%	10
2 Mausaktionen	39,7%	87
3 Mausaktionen	16,9%	37
4 Mausaktionen	20,5%	45
5 oder mehr	5,9%	13
lediglich *Hinweis* auf Browser-Einstellungen oder Drittanbieter	11,0%	24
keine Möglichkeit gefunden	1,4%	3

Tab. 1: Ergebnisse für Webseiten mit Consent-Banner (n = 219).

			Anzahl			
Art des Banners	absolut	keine	1	2-4	5-20	20+
alle	491	40,5%	15,7%	18,5%	18,7%	6,5%
Consent-Banner	219	44,3%	22,4%	19,2%	10,5%	3,7%
modal	154	46,1%	22,1%	17,5%	10,4%	3,9%
nicht-modal	65	40,0%	23,1%	23,1%	10,8%	3,1%
Info-Banner	61	36,1%	9,8%	19,7%	21,3%	13,1%
modal	3	66,7%	0%	33,3%	0%	0%
nicht-modal	58	34,5%	10,3%	19,0%	22,4%	13,8%
ohne Banner	211	37,9%	10,4%	17,5%	26,5%	7,6%

Tab. 2: Ohne aktive Zustimmung gesetzte persistente 3rd Party Cookies.