Verbraucherforschungsforum

„Künstliche Intelligenz und Verbraucherpolitik: Chancen der Verbraucherinformatik“

zeppelin universität
zwischen
Wirtschaft Kultur Politik

European University Institute
DEPARTMENT OF LAW

ConPolicy

Experten-Workshop
am 30. April 2019 auf Einladung des Forschungszentrums Verbraucher, Markt und Politik (CCMP) der Zeppelin Universität in Kooperation mit ConPolicy-Institut für Verbraucherpolitik Berlin und dem European University Institute (EUI) Florenz im Ministerium für Ländlichen Raum und Verbraucherschutz Baden-Württemberg (MLR), Stuttgart.

Inhalt

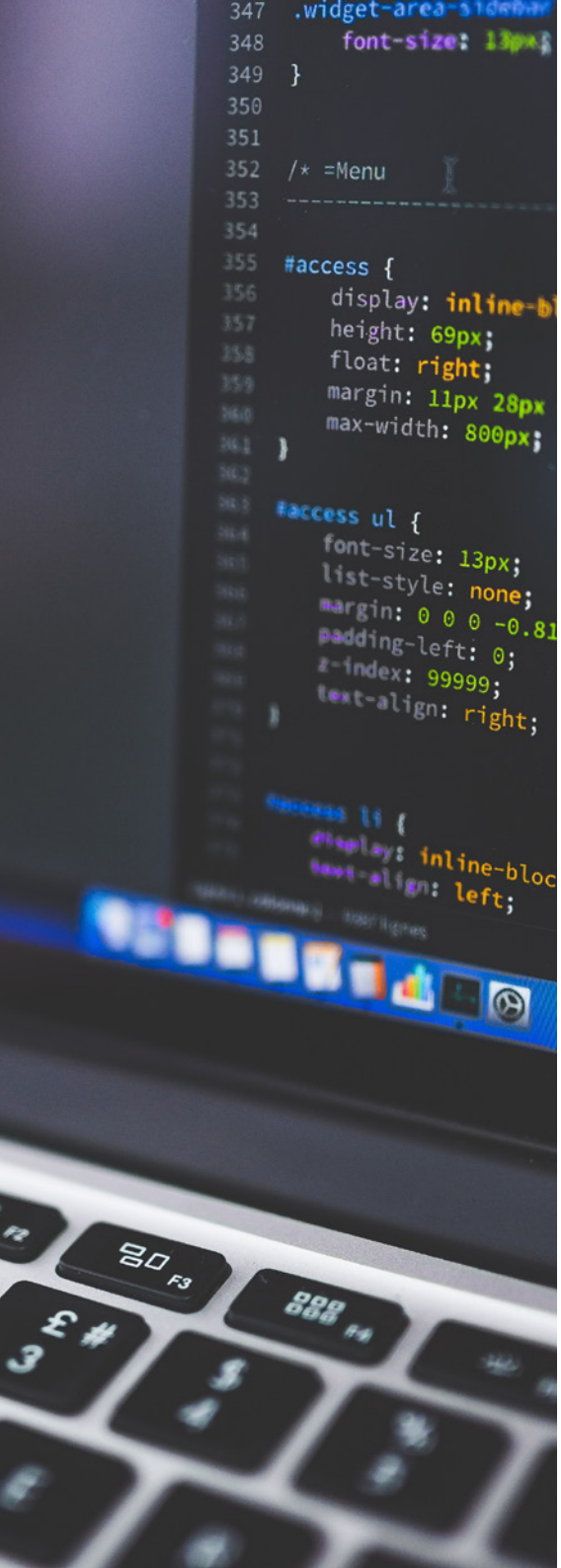
Künstliche Intelligenz und Verbraucherpolitik: Chancen der Verbraucherinformatik

Ministerialdirektorin Grit Puchan

Immer mehr Aufgaben werden von intelligenter Software oder Robotern übernommen. Das betrifft nicht nur die Arbeitswelt, sondern auch den Alltag. Die Digitalisierung unserer Lebensbereiche und die Entwicklung von Künstlicher Intelligenz gehören zu den wichtigsten Themen unserer Zeit. Das Verbraucherforschungsforum des Forschungszentrums Verbraucher, Markt und Politik (CCMP) zum Thema „Künstliche Intelligenz und Verbraucherpolitik – Chancen der Verbraucherinformatik" am 30. April 2019 in Stuttgart widmete sich diesem neuen Thema und lud dazu ein, die drängendsten Fragen zu diskutieren.

Die fortschreitende Digitalisierung verändert nicht nur unsere Arbeitswelt, sondern führt auch zu einem Wandel im Privatleben und beim täglichen Konsum. Hierfür finden sich Beispiele vor allem in den klassischen Konsumfeldern Ernährung, Kleidung, Wohnen und Mobilität, aber natürlich auch bei der Kommunikation und beim Online-Einkauf. Das noch sehr junge Forschungsfeld der „Verbraucherinformatik" setzt an den zentralen Herausforderungen der Digitalen Welt für Verbraucherinnen und Verbraucher an. Das Forschungsfeld ist jedoch bislang noch weitgehend undefiniert. Das Verbraucherforschungsforum in Stuttgart leistet einen Beitrag, den Begriff Verbraucherinformatik mit Inhalt zu füllen, die zentralen Forschungsfragen zu definieren sowie eine erste Forschungsagenda zu entwerfen. In Vorträgen und Diskussionsrunden näherte man sich folgenden Fragen:

- Was ist mit dem Begriff Verbraucherinformatik gemeint, wie grenzt er sich thematisch gegen andere Begriffe ab?
- Welche Bedeutung haben die Verbraucherinformatik und die Künstliche Intelligenz allgemein und speziell für die Verbraucherpolitik?
- Welche konkreten Projekte und Initiativen gibt es bereits und wie sind die Erfahrungen damit?
- Wie sollten algorithmengestützte Angebote aussehen, damit sie in der praktischen Verbraucherpolitik genutzt werden können?
- Welche Chancen und Risiken ergeben sich für Verbraucherinnen und Verbraucher?



Im Forum wurden eine Reihe von Pilotprojekten und praktischer Anwendungen vorgestellt und von den Teilnehmerinnen und Teilnehmern aus der Wissenschaft, der Verbraucherpolitik sowie aus Unternehmen wie Google diskutiert. Am Ende stand die gemeinsame Definition zukünftiger lohnenswerter Forschungsfragen der Verbraucherinformatik.

Die Verbraucherpolitik als Querschnittsaufgabe benötigt Forschung über verschiedene Disziplinen hinweg. Das Verbraucherministerium Baden-Württemberg hat dies früh erkannt. Mit den jährlich stattfindenden Verbraucherforschungsforen werden Akteure der Verbraucherforschung und Verbraucherpolitik in Baden-Württemberg, aber auch darüber hinaus, miteinander vernetzt. Ziel ist es, einen intensiven Wissenstransfer zu ermöglichen sowie einen Austausch zwischen den Forschungsgebieten zu fördern. Die Veranstaltungen sind ein wichtiger Bestandteil der Aufgaben des Verbraucherministeriums Baden-Württembergs, zukunftsrelevante Themen voranzutreiben und die Verbraucherpolitik in der digitalen Welt zu verankern.

Das diesjährige Forum zur Verbraucherinformatik war eine der ersten Veranstaltungen zum Thema Verbraucherinformation. Die bislang noch kleine und exklusive Gruppe von Wissenschaftlern und Wissenschaftlerinnen, die zu diesem Thema bereits arbeiten, war der Einladung gefolgt. Der Veranstaltungsort in Stuttgart wurde dabei bewusst gewählt: Über die Landeshauptstadt hinaus ist Baden-Württemberg bei der Gestaltung der Digitalisierung sehr aktiv. Alleine das Ministerium für Ländlichen Raum und Verbraucherschutz hat in den letzten Jahren eine Vielzahl an Digitalisierungsprojekten initiiert, beispielsweise bei der Online-Information und -Beratung der Verbraucherzentrale Baden-Württemberg e. V. Beinahe täglich starten neue Projekte in den Kommunen, den Schulen und in den Unternehmen. Bei all diesen Aktivitäten ist es umso erfreulicher, was die Digitalisierungsstrategie Baden-Württemberg digital@bw als erstes Ziel formuliert: „Wir stellen die Bevölkerung unseres Landes in den Mittelpunkt, ...und diskutieren mit den Menschen, wie Digitalisierung unser Leben verändern wird und wie wir Digitalisierung gestalten wollen."

Auch das Verbraucherforschungsforum hat dazu beigetragen, die Chancen und Möglichkeiten von Algorithmen und Künstlicher Intelligenz für die Anwender besser zu nutzen, ohne dabei die kritischen Seiten zu übersehen. Mehr noch: Die Agenda für die zukünftige Forschung kommt zur rechten Zeit. Gute Forschung und gute Digitalpolitik können dazu beitragen, das Vertrauen der Verbraucherinnen und Verbraucher in den Einsatz der Künstlichen Intelligenz im Verbraucheralltag zu stärken.

Mein Dank gilt den Organisatoren, vor allem dem Team des Forschungszentrums, aber auch den Referentinnen und Referenten sowie Teilnehmerinnen und Teilnehmern des Forums. Alle gemeinsam haben das Thema der Verbraucherinformatik ein gutes Stück weiter vorangebracht.

Ihre

Grit Puchan

Ministerialdirektorin im Ministerium für Ländlichen Raum und Verbraucherschutz Baden-Württemberg

Künstliche Intelligenz und Verbraucherpolitik: Chancen der Verbraucherinformatik

Christian Thorun, Lucia A. Reisch und Hans-W. Micklitz

Künstliche Intelligenz (KI) und Anwendungen der Verbraucherinformatik bieten heute einmalige Chancen, verbraucherpolitische Ziele durch den Einsatz von digitalen Technologien spürbar zu befördern: Anwendungen, die Verbraucherinnen und Verbraucher darin unterstützen, PC- oder App-Einstellungen gemäß ihren Datenschutzpräferenzen vorzunehmen, verbraucherschützende Browser-Plug_Ins, die Verbraucherinnen und Verbraucher vor Datenkraken beim Internetsurfen warnen, KI-gestützte Textanalyseverfahren, die Aufsichtsbehörden befähigen, unrechtmäßige Allgemeine Geschäftsbedingungen weitgehend automatisiert zu identifizieren, Blockchain-basierte Technologien, die die Produktsicherheit und die Verbraucherinformation verbessern oder Chatbot-Systeme, die von Verbraucherzentralen in der Verbraucherinformations- und Verbraucherberatungsarbeit verwendet werden könnten. Dies sind nur wenige Beispiele von innovativen Anwendungen, die die Praxisprojekte in jüngster Zeit entwickelt haben.

Allerdings ist bislang weitgehend unklar, wo die Chancen und Risiken der Verbraucherinformatik bzw. von Verbraucherschutztechnologien im Allgemeinen und der KI speziell für die Verbraucher(politik) bestehen. Auch mangelt es bislang an einem Diskurs der Akteure über die Fragen, welche konkreten Anwendungen heute bereits existieren und welche absehbar sind, wie diese ethisch und praktisch einzuschätzen sind, welche Akteure dadurch welche Vorteile haben und welche Art von Forschungsunterstützung benötigt wird.

Eine Beantwortung dieser Fragen ist nicht nur vor dem Hintergrund unmittelbarer Mehrwerte für Verbraucherinnen und Verbraucher von zentraler Bedeutung, sondern auch weil die Bundesregierung in ihrer KI-Strategie u.a. angekündigt hat, „die Entwicklung von innovativen Anwendungen [...] zu unterstützen, die die Selbstbestimmung (insbesondere die informelle Selbstbestimmung), die soziale Teilhabe und die Privatheit der Bürgerinnen und Bürger fördern sollen."[1] Das Bundesministerium der Justiz und für Verbraucherschutz hat aus dem Budget dieser Strategie Mittel erhalten, die nun wirksam eingesetzt werden sollten.

1 Die Bundesregierung (2018). Strategie Künstliche Intelligenz der Bundesregierung, S. 40 Abgerufen von https://www.bmbf.de/files/Nationale_KI-Strategie.pdf.

Vor diesem Hintergrund fand das Verbraucherforschungsforum „Künstliche Intelligenz und Verbraucherpolitik: Chancen der Verbraucherinformatik" am 30. April 2019 im baden-württembergischen Ministerium für Ländlichen Raum und Verbraucherschutz in Stuttgart statt. Es wurde vom Forschungszentrum Verbraucher, Markt und Politik (CCMP) in Kooperation mit dem European University Institute (Florenz) und dem ConPolicy-Institut für Verbraucherpolitik (Berlin) organisiert und durchgeführt. Beim Forum sollten Praktiker aus Verbraucherpolitik und verbrauchernahen Verbänden sowie Forschende in der Schnittmenge künstlicher Intelligenz und Verbraucherpolitik zusammenkommen, um die Potentiale von Anwendungen der künstlichen Intelligenz für die Verbraucherpolitik auszuloten.

In der vorliegenden Dokumentation fassen die Expertinnen und Experten, die am Forum teilgenommen haben, ihre wesentlichen Forschungsergebnisse, Projekte und Gedanken zusammen. Hierdurch wollen wir all denjenigen, die nicht an dem Forum teilnehmen konnten, die Möglichkeit geben, von der Veranstaltung zu profitieren. Die Gliederung orientiert sich an der Tagungsagenda: Nach einführenden Erörterungen zur Forumsthematik folgen grundlegende Ausführungen zur Verbraucherinformatik. Es schließen sich Berichte über fünf Pilotprojekte und deren praktische Erfahrungen an. Abschließend werden die Erwartungen von Anwendern dieser Technologien beschrieben und mögliche Eckpunkte einer Forschungsagenda zusammengefasst. Diese Eckpunkte basieren auf den Arbeitsergebnissen einer Reihe von Kleingruppen.

Wir danken allen Teilnehmern des Verbraucherforschungsforums ganz herzlich für ihr großes Engagement.

Verbraucherinformatik als neues Instrument der Verbraucherpolitik[2]

Christian Thorun und Sara Elisa Kettner

Die Digitalisierung transformiert die Lebenswelten der Verbraucherinnen und Verbraucher. Vernetztes Kinderspielzeug, Sprachassistenzsysteme oder immer stärker individualisierte Produkte und Dienstleistungen sind nur einige Beispiele hierfür. Es überrascht daher auch nicht, dass sich die Verbraucherpolitik intensiv mit der Frage auseinandersetzt, wie u.a. der Schutz der Privatsphäre, die Datensicherheit, die Produktsicherheit und -haftung sowie die Algorithmentransparenz gewährleistet werden kann.

Während diese Diskurse über eine Weiterentwicklung des Rechtsrahmens notwendig sind, mangelt es bislang an einer systematischen Debatte darüber, wie digitale Technologien genutzt werden können und sollten, um verbraucherpolitische Ziele effektiver und effizienter zu erreichen. Genau hierauf zielen neue Forschungsansätze zu Verbraucherschutztechnologien bzw. die Verbraucherinformatik ab. Da es sich hierbei um noch junge Forschungsrichtungen innerhalb der Verbraucherforschung handelt, ist eine Definition notwendig.

Begriffsklärung

Verbraucherschutztechnologien können als ein Teilbereich von Verbrauchertechnologien verstanden werden. Bei Verbrauchertechnologien handelt es sich um digital-technologische Anwendungen, die sich explizit an Verbraucherinnen und Verbraucher richten und ihnen in ihrem Konsumalltag Nutzen stiften. Dieser Nutzen spiegelt sich beispielsweise in finanziellen Einsparungen (z.B. bei Preisvergleichsportalen), in Komfortsteigerungen (z.B. bei Sprachassistenzsystemen) oder in Zeitersparnissen (z.B. Navigationstools) wider. Verbraucherschutztechnologien wiederum stellen einen Teilbereich dieser Verbrauchertechnologien dar. Sie zielen darauf ab, Verbraucherinnen und Verbraucher in Märkten zu unterstützen. Die Unterstützung kann – wie im Folgenden gezeigt wird – in vielfältigster Weise erfolgen. Die Verbraucherinformatik wiederum stellt die Wissenschaftsdisziplin dar, die sich mit dem Einsatz von digitaltechnologischen Verfahren, Instrumenten und Anwendungen zur Förderung des Verbraucherschutzes befasst.

Wesentliche verbraucherpolitische Ziele

Wie die Definition von Verbraucherschutztechnologien zeigt, stellt der Einsatz digitaler Technologien in diesem Anwendungsfeld keinen Selbstzweck, sondern ein Mittel zur Erreichung bestimmter verbraucherpolitscher Ziele dar. Angelehnt an die UN Guidelines for Consumer Protection können verbraucherpolitische Ziele drei übergeordneten Schwerpunktbereichen zugeordnet werden:

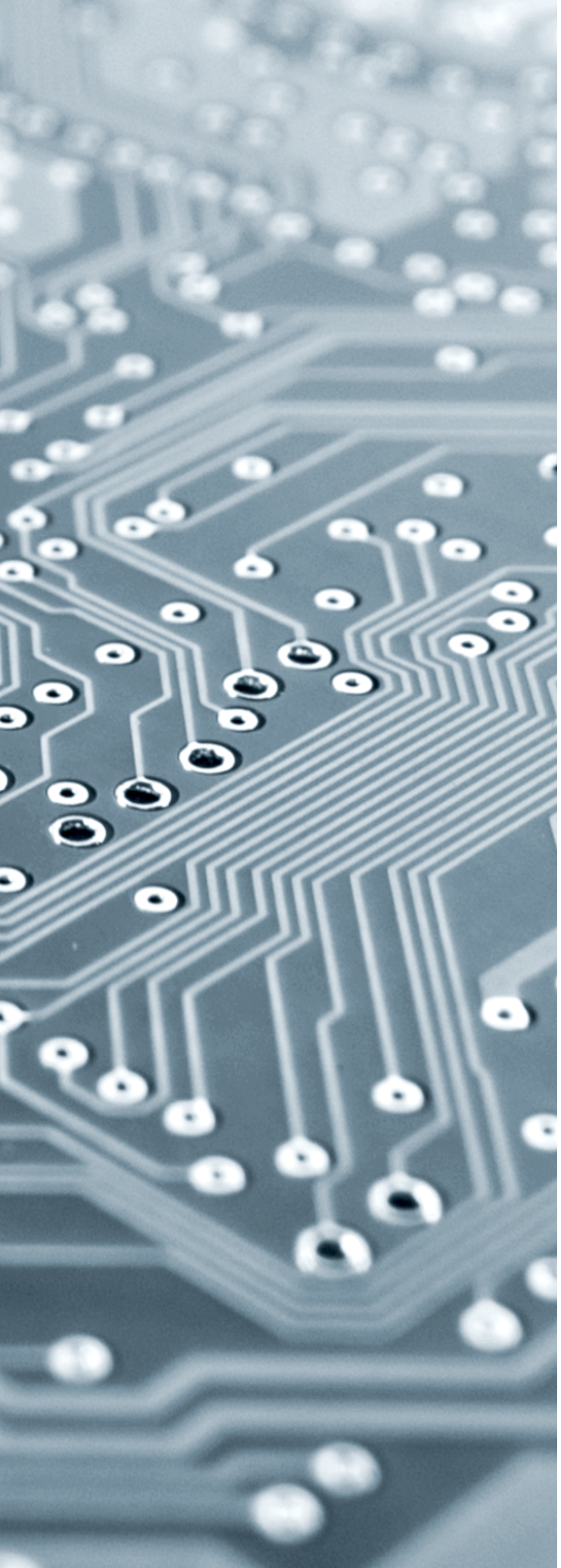
Verbraucherschutz: Hierbei geht es insbesondere darum, für einen fairen Wettbewerb zu sorgen und hierdurch die wirtschaftlichen Interessen der Verbraucherinnen und Verbraucher zu fördern; ein hohes Maß an Produktsicherheit und effektive Rückverfolgbarkeitssysteme zu gewährleisten; und Verbraucherinnen und Verbraucher vor (Produkt-)Fälschungen zu schützen.

Verbraucherbefähigung: Der Fokus in diesem Bereich liegt darauf sicherzustellen, dass Verbraucherinnen und Verbraucher über einen Zugang zu hochwertigen Verbraucherinformationen verfügen; dass es ein Angebot für eine anbieter-unabhängige Verbraucherberatung gibt; und dass der Prosumerismus bzw. die Verbraucherbeteiligung gefördert werden.

Rechtsdurchsetzung: Für einen effektiven Verbraucherschutz ist es nicht nur erforderlich, dass Verbraucherinnen und Verbraucher über adäquate Rechte verfügen, sondern auch, dass das Recht konsequent durchgesetzt wird. Hierbei kommt es zum einen darauf an, dass das Verbraucherrecht im kollektiven Interesse durch Aufsichtsbehörden und Verbraucherorganisationen durchgesetzt wird. Zum anderen ist es essentiell, dass Verbraucherinnen und Verbraucher über effektive Möglichkeiten verfügen, ihre Rechte auch individuell geltend zu machen.

Flankiert werden diese Ziele von zwei horizontalen Zielen: Hierzu zählt zum einen, dass die Verbraucherpolitik insbesondere die Interessen von schutzwürdigen Verbraucherinnen und Verbrauchern (wie Kindern und Jugendlichen, älteren Personen oder Menschen mit körperlichen Beeinträchtigungen) berücksichtigen sollte. Zum anderen zählt hierzu die Förderung eines nachhaltigen Konsums.

2 Dieser Artikel stützt sich in weiten Teilen auf den folgenden Beitrag: Thorun, C., & Diels, J. (2019). Consumer protection technologies: An investigation into the potential of new digital technologies for Consumer Policy. Journal of Consumer Policy, https://doi.org/10.1007/s10603-019-09411-6. Sofern darüberhinausgehende Quellen verwendet wurden, werden diese in den Fußnoten angegeben.



Die Forschung zu Verbraucherschutztechnologien bzw. die Verbraucherinformatik sollte sich daher mit der Frage befassen, welche Beiträge digitale Technologien leisten können, um dazu beizutragen, diese Ziele zu erreichen.

Wesentliche (digital-)technologische Entwicklungen

Wenn man digitaltechnologische Entwicklungen betrachtet, dann zeigt sich, dass grundsätzlich eine Vielzahl von Technologien und Anwendungen eingesetzt werden können, um verbraucherpolitische Ziele voranzubringen. In Anlehnung an Cearley et al. können diese Technologien und Anwendungen drei wesentlichen Feldern zugeordnet werden:[3]

1. **Intelligent theme**: In dieses Feld fallen Technologien wie die des natural-language processings, des machine learnings und der predictive analytics.

2. **Digital theme**: In diesem Feld finden sich Dialogplattformen, die u.a. Chatbots einsetzen oder auch Anwendungen der Virtual und Augmented Reality (VR und AR).

3. **Mesh theme**: Hier finden sich insbesondere Datenbanktechnologien, distributed ledger bzw. blockchain technologies sowie smart contracts.

3 Gartner (2017). Gartner Top 10 Strategic Technology Trends for 2018. Abgerufen von https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/.

Überdies gibt es noch eine Reihe weiterer Technologien, die über diese Dreier-Einteilung hinausgehen und für die Verbraucherpolitik relevant sein könnten. Hierzu zählen etwa der 3D-Druck, online-Plattformen sowie Anwendungen des Internet of Things (IoT).

Anwendungsfelder von Verbraucherschutztechnologien im Überblick

Im Hinblick auf die vorher genannten verbraucherpolitischen Ziele ergibt sich die folgende Zuordnung der Technologien und Anwendungen:

Wenn es um **Verbraucherschutzziele** geht, können gerade Blockchain-basierte Anwendungen eine wichtige Rolle spielen. Sie könnten dafür verwendet werden, die Produktsicherheit durch eine bessere Rückverfolgbarkeit und effektivere Produktrückrufe zu erhöhen. Gerade in Kombination mit IoT-Sensoren könnte die Blockchain-Technologie dafür eingesetzt werden, die Produktqualität durch eine effektive Kontrolle von Produktions- und Distributionsprozessen zu erhöhen. Weiterhin kann der Einsatz der Blockchain-Technologien dazu beitragen, Verbraucherinnen und Verbraucher besser gegen gefälschte Produkte zu schützen.

Über die Blockchain hinaus können Verfahren der Predictive Analytics dazu eingesetzt werden, etwa ein dynamisches Mindesthaltbarkeitsdatum bereitzustellen. Security-Programme können wiederum dafür verwendet werden, Verbraucherinnen und Verbraucher beim Schutz ihrer Privatsphäre zu unterstützen.

Im Hinblick auf das verbraucherpolitische Ziel, **Verbraucherinnen und Verbraucher zu befähigen**, können digitaltechnologische Anwendung ebenfalls in vielfältiger Hinsicht genutzt werden. Mit Bezug auf das Ziel, Verbrauchern einen **Zugang zu hochwertigen Informationen** zu ermöglichen, können AR-Technologien etwa dafür eingesetzt werden, vorvertraglich Preisvergleiche bei Printwerbung zu ermöglichen – ähnlich wie beim online-Konsum. Auch können AR-Technologien während des Kaufprozesses verwendet werden, um Verbrauchern am Point of Sale z.B. über eine Informations-App Zusatzinformationen zu Zutaten und Inhaltsstoffen

zur Verfügung zu stellen. Auch können digitale Technologien dafür verwendet werden, Verbraucherinformationen verständlicher und zugänglicher zu machen.

Digitale Technologien können überdies dafür eingesetzt werden, die bereits bestehende **Verbraucherberatung** zu verbessern. So könnten Robo-Advice-Systeme und Chatbots eingesetzt werden, um die Beratungsarbeit der Verbraucherzentralen zu flankieren. Bots und virtual personal assistants können Verbraucherinnen und Verbraucher darin unterstützen, Datenschutzerklärungen im Sinne der Nutzerinnen und Nutzer zu analysieren und dementsprechend Handlungsempfehlungen zu generieren.

Auch können digitale Technologien eingesetzt werden, um **Prosumerism und die Verbraucherbeteiligung** zu fördern. So könnten Blockchain-basierte Anwendungen Märkte ohne Intermediäre ermöglichen; Plattformen können eingesetzt werden, um Angebote der sharing economy zu fördern. Und IT-gestützte Dialogformate können verwendet werden, um den Austausch von Verbrauchern untereinander sowie zwischen ihnen und Unternehmen und der Politik zu fördern.[4] Für Verbraucherinnen und Verbraucher mit Lernbehinderungen bietet das Verfahren des natural language-Processings neue Möglichkeiten um Texte zusammenzufassen. Bilderkennungsverfahren wiederum, können eingesetzt werden, um Bilder in Sprache umzuwandeln und somit die Bildverarbeitung für Menschen mit visuellen Beeinträchtigungen zu ermöglichen.[5]

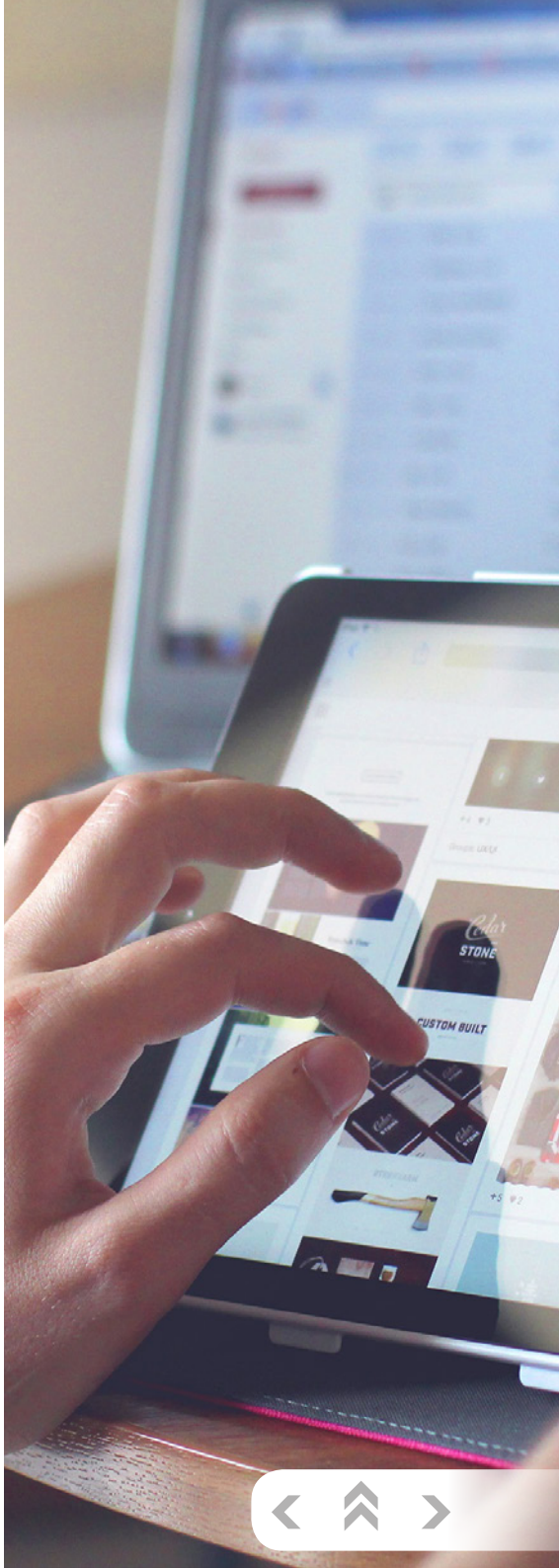
Abschließend können digitale Technologien Beiträge im Bereich der Rechtsdurchsetzung leisten. So könnten Verfahren des natural language processing in der Marktüberwachung verwendet werden, um etwa Datenschutzerklärungen oder AGBs nach rechtswidrigen Inhalten hin zu crawlen und zu analysieren. Hierdurch können diese Technologien einen Beitrag zur kollektiven **Rechtsdurchsetzung** leisten. Überdies können Legal-Tech-Anwendungen etwa bei Fluggast- oder Mietrechten die individuelle Rechtsdurchsetzung für Verbraucherinnen und Verbraucher vereinfachen.

4 Sie hierzu etwa die My Country Talks, die ZEIT ONLINE durchgeführt hat: https://www.mycountrytalks.org/de/.

5 Siehe hierzu etwa das Google-Forschungsprojekt „Tensorflow", „Helpicto" sowie der Microsoft „Presentation Translator". Liu, P., & Xin Pan, X. (2016). Text summarization with TensorFlow. Google AI Blog. Abgerufen von https://ai.googleblog.com/2016/08/text-summarization-with-tensorflow.html (04.06.19); HELPICTO > EQUADEX – INPACTS. (2018). Helpicto – AI for Autism. Abgerufen von http://www.helpicto.com/en/home-2/ (04.06.19) sowie Microsoft Corporation. (2019). Seeing AI. Abgerufen von https://www.microsoft.com/en-us/seeing-ai (04.06.19).

Fazit und Ausblick

Dieser Überblick verdeutlicht dreierlei: Erstens zeigen diese Beispiele, dass digitale Technologien einen signifikanten Beitrag für das Erreichen verbraucherpolitischer Ziele leisten können. Zweitens handelt es sich bei diesem Forschungsfeld noch um eine sehr junge Disziplin innerhalb der Verbraucherforschung. Daher ist es gut, dass das Bundesjustiz- und Verbraucherschutzministerium jüngst etwa eine Förderbekanntmachung zu „Anwendungen künstlicher Intelligenz zur Unterstützung des Verbraucheralltags (consumer enabling technologies)" veröffentlich hat. Weitere Förderung zur Vergrößerung des Forschungsfeldes ist jedoch unbedingt notwendig. Drittens ist zu konstatieren, dass eine viel systematischere Auseinandersetzung durch verbraucherpolitische Akteure mit dem Potential dieser Technologien für die Verbraucherpolitik notwendiger ist als bislang.



Künstliche Intelligenz und Machine Learning als Säulen der Verbraucherinformatik

Micha Kaiser

Big Data, Smart Home, Algorithmen, künstliche Intelligenz (KI), Online-shopping und Sprachassistenten, das Thema Digitalisierung spielt für Verbraucherinnen und Verbraucher in unterschiedlichen Lebensbereichen eine wachsende Rolle. Immer mehr Aufgaben werden von intelligenter Software oder Robotern übernommen, ermöglicht durch Algorithmen, also in Code gegossene mathematische Formeln. Künstliche Intelligenz ist zum Zukunftsthema geworden. Was aber ist Künstliche Intelligenz genau? Nach Definition der bitkom ist künstliche Intelligenz „*die Eigenschaft eines IT-Systems, eine der kognitiven Leistungsfähigkeit des Menschen ähnliche Fähigkeit zu zeigen. Diese Fähigkeit kann ansatzweise ausgebildet sein, sie kann auch über die menschliche Fähigkeit hinausgehen. Dazu sind in unterschiedlichen Anteilen bestimmte Kernfähigkeiten notwendig: wahrnehmen, verstehen, handeln und lernen.*" Diese Eigenschaft wird von KI-Systemen i.d.R. durch die Fähigkeit zu „lernen", sprich bestimmte wiederkehrende Muster zu erkennen und zu systematisieren, erreicht. Obwohl maschinelles Lernen (ML) bei originärer Betrachtung lediglich als ein Teilgebiet im Bereich der KI anzusiedeln ist (beispielhaft für weitere Bereiche seien hier die Robotik oder das sogenannte Reinforcement Learning erwähnt), sind sich die meisten Experten einig, dass maschinelles Lernen momentan das wohl wichtigste Feld im Bereich der Künstlichen Intelligenz darstellt. Konkret versteht man laut Arthur Samuel (einem Begründer des maschinellen Lernens) darunter „*ein Studienbereich, in dem Computer lernen können, ohne explizit programmiert zu werden*". Um dieses Ziel zu erreichen, kommen im ML eine Vielzahl an Techniken und Algorithmen zum Einsatz. Grundsätzlich lassen sich dabei zwei grundlegende Vorgehensweisen unterscheiden. Während Systeme, die sich auf das sogenannte **überwachte Lernen** (engl.: **supervised learning**) stützen, Gesetzmäßigkeiten anhand externer (i.d.R. menschlicher) Vorgaben erlernen, vollzieht sich die Mustererkennung bei unüberwachtem Lernen (engl.: unsupervised learning) im Grunde ohne eine weitere, die Korrektheit des Erlernten beurteilende Instanz.[6] Beispielhaft für die erste Vorgehensweise sind sogenannte **Lineare Regressionsmodelle, Neuronale Netze, oder Entscheidungsbäume**, anhand derer der Einfluss von bestimmten (exogenen) Faktoren und Eigenschaften auf eine weitere (endogene) Bezugsgröße abgeschätzt wird.

6 James, G., Witten, D., Hastie, T., & Tibshirani, R. (2013). An introduction to statistical learning, Vol. 112. New York: Springer. S. 26-28.

Innerhalb der Klasse des überwachten Lernens separiert man die in Frage kommenden Algorithmen wiederum in Bezug auf die Ausprägung der endogenen Variablen. Liegt diese nämlich in kategorialer Form vor (ja/nein, schwarz/weiß, männlich/weiblich etc.) so kommen sogenannte Klassifikationsalgorithmen zum Einsatz, deren Ziel darin besteht, die (möglichst präzise) Wahrscheinlichkeit vorherzusagen, dass eine mit bestimmten Merkmalen (exogenen Faktoren) ausgestattete Beobachtung in eine dieser Kategorien fällt. Die Idee wird beispielhaft in Tabelle 1 verdeutlicht. Anhand der Merkmale „Einkommen", „Geschlecht" und „Alter" soll der Algorithmus erlernen mit welcher Wahrscheinlichkeit eine bis dato unbekannte Person ein Kaufinteresse aufweist.

Tabelle 1: Klassifikationsalgorithmus

Kunde	Einkommen	Geschlecht	Alter	Kauf-interesse
1	5000 €	Männlich	50	Ja
2	3000 €	Weiblich	48	Nein
3	2000 €	Männlich	20	Nein
4	2500 €	Weiblich	29	?

Liegt die endogene Variabel nicht in kategorialer, sondern in stetiger Ausprägung vor, so spricht man von **Regressionsanalysen** oder Regressionsmodellen. Wie Tabelle 2 beispielhaft verdeutlicht, wird hier vom Algorithmus nicht eine mit einem bestimmten kategorialen Verhalten verknüpfte Wahrscheinlichkeit vorhergesagt, sondern eine konkrete, quantifizierbare Entscheidungsgröße (in unserem Beispiel die Zahlungsbereitschaft) berechnet bzw. prognostiziert.

Tabelle 2: Regressionsmodelle

Kunde	Einkommen	Geschlecht	Alter	Zahlungs-bereitschaft
1	5000 €	Männlich	50	120 €
2	3000 €	Weiblich	48	100 €
3	2000 €	Männlich	20	80 €
4	2500 €	Weiblich	29	?

Beispielhaft für den Ansatz des unüberwachten Lernens stehen sogenannte **Clusteranalysen**, die allein aufgrund der unterschiedlichen Ausprägung von Merkmalen bestimmter Faktoren auf die Eigenschaften der durch die Merkmale charakterisierten Beobachtungen schließen lassen.[7] In anderen Worten: Unüberwachtes Lernen wird dazu genutzt, um anhand von beobachtbaren Merkmalen unterschiedliche Gruppen zu bilden.

Tabelle 3 verdeutlicht beispielhaft das Ergebnis eines Clusteralgorithmus. Anhand der Merkmale „Einkommen", „Geschlecht", „Alter" und Zahlungsbereitschaft" hat das lernende System zwei untereinander möglichst heterogene und innerhalb möglichst homogener Gruppen identifiziert.

Tabelle 3: Clusteranalyse

Kunde	Einkommen	Geschlecht	Alter	Zahlungs-bereitschaft	Gruppe
1	5000 €	Männlich	50	120 €	1
2	3000 €	Weiblich	48	100 €	1
3	2000 €	Männlich	20	80 €	2
4	2500 €	Weiblich	29	60 €	2

7 Friedman, J., Hastie, T., & Tibshirani, R. (2001). The elements of statistical learning, Vol. 1, No. 10. New York: Springer. S. 460-462.

Beiden Ansätzen - überwachtem sowie unüberwachtem Lernen - ist zudem gemein, dass zur korrekten Beantwortung der gegebenen Fragestellung (bspw.: Mit welcher Wahrscheinlichkeit kauft Kunde X Produkt Y; Welches ist der Maximalpreis, den ich von Kunde X verlangen kann ohne dass dieser von der Kaufentscheidung absieht), enorme Datenmengen vorgehalten und analysiert werden müssen. Wenn man sich beispielsweise verdeutlicht, dass ausgereifte **Neuronale Netze** (darunter versteht man im weitesten Sinne Algorithmen, die sich an der Funktionsweise des menschlichen Gehirns orientieren) zum Erlernen von Zusammenhängen und Mustern in hinreichend großen Datensätzen mitunter mehrere Wochen benötigen wird deutlich, dass neben verbraucherpolitischen auch technische Fragestellungen eine zunehmende Rolle spielen werden.

Grundsätzlich können die geschilderten Algorithmen nicht mit menschlicher Intelligenz gleichgesetzt werden, da die heutigen Methoden der KI im Allgemeinen und des ML im Speziellen weit davon entfernt sind, eine umfassende, den Turing Test bestehende Intelligenz zu verkörpern. Nichtsdestotrotz stellen diese Methoden ein sehr effektives Mittel zur **Mustererkennung** da. Basierend auf komplexen statistischen Modellen werden diese Algorithmen schon heute dazu genutzt, um in der Industrie, im Verkehr, in der Medizin, bei der Optimierung von Geschäftsprozessen oder in Bezug auf das Verbraucher- und Konsumverhalten Muster in großen Datenmengen zu erkennen, Vorhersagen zu treffen und somit die bis dato menschliche Entscheidungsfindung auf Rechenprogramme zu übertragen.

DATENSCHUTZscanner – Mehr Transparenz und Kontrolle beim Datenschutz in Smartphone-Apps

Sara Elisa Kettner und Christian Thorun[8]

Hintergrund und Motivation

Im Jahr 2018 hatten 81% der Deutschen ein Smartphone und in den App-Stores waren weltweit über 2 Mio. Apps verfügbar.[9] Viele Untersuchungen wie bspw. von der Stiftung Warentest stellen regelmäßig fest, dass viele dieser Apps für Verbraucherinnen und Verbraucher zwar viele Mehrwerte mit sich bringen. Allerdings erheben sie oft zu viele Daten und das auch noch heimlich.[10] Zu ähnlichen Ergebnissen hinsichtlich eines unzureichenden Privatsphäreschutzes führte eine stichprobenartige Untersuchung der beliebtesten Apps durch das DATENSCHUTZscanner-Projekt für das Handelsblatt.[11] So wurden bspw. Defizite bei der Gestaltung der Kontaktmöglichkeiten für datenschutzrechtliche Anliegen festgestellt und viele der geprüften Apps boten den Nutzerinnen und Nutzern keine verständliche Datenschutzerklärung an.

Eine eigene Nutzerbefragung der repräsentativen deutschen Online-Bevölkerung zeigte, dass sich Nutzerinnen und Nutzer im App-Dschungel häufig überfordert fühlen. 81% gaben an, dass es für sie wichtig sei, die Datenschutzerklärung von Apps zu verstehen. Jedoch gaben lediglich 28% an, dass ihnen das Verstehen von App-Datenschutzerklärungen auch einfach fiele.[12]

8 Das DATENSCHUTZscanner-Projekt haben Dr. Sara Elisa Kettner und Prof. Dr. Christian Thorun für den Projektpartner Quadriga Hochschule Berlin umgesetzt.

9 Bitkom Research. (2019). Smartphone-Markt wächst um 3 Prozent auf 34 Milliarden Euro. Abgerufen von https://www.bitkom.org/Presse/Presseinformation/Smartphone-Markt-waechst-um-3-Prozent-auf-34-Milliarden-Euro (17.06.2019); appfigures. (2018). App Analytics & ASO. Abgerufen von https://appfigures.com (17.06.2019)

10 Stiftung Warentest. (2018). Apps von Fernsehsendern schicken Daten weiter. test, 7/2018, 40-42 sowie Stiftung Warentest. (2018). Lovoo, Tinder & Co. Wie schludrig Dating-Apps mit Daten umgehen, test 3/2018, 37-41.

11 Handelsblatt. (2018). Viele Apps halten sich nicht an die neuen Datenschutzregeln. Abgerufen von https://www.handelsblatt.com/politik/international/exklusive-analyse-viele-apps-halten-sich-nicht-an-die-neuen-datenschutzregeln/23018084.html (17.06.2019)

12 Kettner, S. E., et al. (2019). Privacy Guard - Abschlussbericht. Abgerufen von https://datenschutz-scanner.de/detail/news/forschungsprojekt-veroeffentlicht-gemeinsamen-abschlussbericht/ (17.06.2019)

Um Nutzerinnen und Nutzer beim Umgang mit diesen Herausforderungen zu unterstützen, wurde zwischen Januar 2016 und Juni 2018 das Projekt „DATENSCHUTZscanner"(PrivacyGuard) umgesetzt. Übergeordnetes Ziel des Projekts war es, mit Hilfe technischer Möglichkeiten Nutzerinnen und Nutzern von Apps mehr Transparenz und Kontrolle beim Thema Datenschutz in Smartphone-Apps zu geben. Wichtig waren dabei vier übergeordnete Teilziele, die die Anwendungen des DATENSCHUTZscanners erfüllen soll:

Selbstbestimmtheit fördern: Der DATENSCHUTZscanner soll Nutzerinnen und Nutzern nicht eine vorgefertigte Meinung oder Einstellung vorgeben, sondern Informationen liefern, die die Selbstbestimmtheit fördern.

Informationen zu technischen Aspekten und Datenschutzerklärungen einfach und verständlich darstellen: Da nicht jede Nutzerin und jeder Nutzer mit juristischem und technischem Fachwissen ausgestattet ist, ist es notwendig, die Funktionsweise von Apps und deren Datenumgänge nutzerfreundlich aufzubereiten.

Individuelle Präferenzen berücksichtigen: Nutzerinnen und Mindesthaltbarkeitsdatum bereitzustellen haben oftmals unterschiedliche Präferenzen, was Datenumgänge in Apps angeht. Manche begrüßen bspw. die Verarbeitung des Gerätestandorts, um App-Funktionen nutzen zu können. Andere ziehen es vor, dass Standortdaten nicht erhoben werden. Der DATENSCHUTZscanner erlaubt Nutzerinnen und Nutzern diese Differenzierung und passt Handlungsempfehlungen an die Präferenzen der Nutzerinnen und Nutzer an.

Konkrete Handlungsempfehlungen anbieten: Viele Datenschutzanwendungen empfehlen Nutzerinnen und Nutzern lediglich die De-Installation von Apps, um Datenschutzproblemen aus dem Weg zu gehen. Der DATENSCHUTZscanner fördert hingehen die Befähigung zu anderen Schutzmaßnahmen wie bspw. die Änderung von Gerätekennungen oder -IDs.

Umsetzung

Das DATENSCHUTZscanner-Projekt wurde mit knapp 2 Mio. Euro vom Bundesministerium für Bildung und Forschung gefördert und durch ein interdisziplinäres Team umgesetzt. Zum Projektteam zählten das Institut für angewandte Informatik Leipzig, mediaTest digital, die Quadriga

Hochschule Berlin und der Verein Selbstregulierung Informationswirtschaft.

Die Forschung konzentrierte sich hierbei auf folgende übergeordnete Bereiche:

1. Eine semantische Analyse von Rechtstexten und Automatisierung,

2. eine technische Analyse der tatsächlichen Datenverarbeitungen einer App, zwecks Abgleiches und Ergänzung der semantischen Analyse und

3. die Erforschung der relevanten Aspekte für Verbraucherinnen und Verbraucher bei der Verwendung mobiler Endgeräte und eine damit einhergehende, laienverständliche Aufbereitung.

Anwendungen

Im Rahmen des Projekts wurden drei Prototypen entwickelt:

DATENSCHUTZscanner App Client: Der App Client kann auf dem Android-Smartphone der Nutzerinnen und Nutzer installiert werden. Durch Abgleich der eigenen, installierten Apps mit der Projektdatenbank, die Informationen zu relevanten Datenverarbeitungen einer Vielzahl geprüfter Apps beinhaltet, wird Nutzern knapp und bündig dargestellt, wie sich ihre Apps auf dem eigenen Smartphone verhalten. D.h. es werden Informationen darüber gegeben, welche Daten erhoben und zu welchem Zweck diese vom Anbieter verarbeitet werden. Nutzerinnen und Nutzer können innerhalb der DATENSCHUTZscanner-App kontextspezifisch und auf Grundlage eigener Präferenzen einstellen, welche Art der Datenverarbeitungen sie für ihre anderen Apps zulassen möchten. Darüber hinaus erhalten sie verständliche Erklärungen und Handlungsempfehlungen.

DATENSCHUTZscanner Browser Extension: Der zweite entwickelte Prototyp ist eine Browser-Erweiterung für Google Chrome, die den Google Playstore durch die Informationen der DATENSCHUTZscanner-Datenbank ergänzt. Wenn Nutzerinnen und Nutzer eine App-Beschreibung öffnen, werden die Standard-Informationen zur App durch datenschutzrelevante Informationen ergänzt. Zusätzlich werden Handlungsempfehlungen für die App-Einstellungen gegeben.

DATENSCHUTZscanner Datenschutz-Analyzer: Der Analyzer ist eine Anwendung, die Nutzerinnen und Nutzer über eine Webseite erreichen. Dort können Sie eine beliebige Datenschutzerklärung einfügen und automatisch analysieren lassen. Der DATENSCHUTZscanner-Algorithmus prüft den Text auf relevante Datenschutzaspekte und fasst diese in einem Report zusammen. Neben verständlichen Erläuterungen zu den Datenverarbeitungen werden Handlungsempfehlungen angezeigt.

Einsatzmöglichkeiten

Die Einsatzmöglichkeiten der DATENSCHUTZscanner-Anwendungen sind vielfältig. Zum einen können, wie für die Prototypen bereits vorbereitet, Anwendungen für Nutzerinnen und Nutzer geschaffen werden, die die Selbstbestimmtheit fördern. Durch Nutzung der Anwendungen können Nutzerinnen und Nutzer so ihre Informationslage bezüglich der eigenen Apps verbessern und durch präferenzbasierte Einstellungen ihren Datenschutz auf dem eigenen Endgerät verbessern.

Darüber hinaus kann die Technologie jedoch auch durch Behörden oder Verbraucherorganisationen eingesetzt werden. So können bspw. Marktanalysen durchgeführt werden oder Vorbewertungen von Anwendungen durch die DATENSCHUTZscanner-Technologie bei der Marktüberwachung assistieren.

Pilotprojekt PrivacyScore

Dominik Herrmann

PrivacyScore (https://privacyscore.org) ist ein im Jahr 2017 gestartetes nichtkommerzielles Crowdsourcing-Portal für den Vergleich von Webseiten hinsichtlich der Einhaltung gängiger Sicherheits- und Datenschutz-Best-Practices. PrivacyScore wird vom Lehrstuhl für Privatsphäre und Sicherheit in Informationssystemen an der Universität Bamberg bereitgestellt.

Motivation

Das aktuell geltende Datenschutzrecht sieht vor, dass die Betreiber von Webseiten ihre Nutzerinnen und Nutzer mittels einer Datenschutzerklärung über die auf der Webseite stattfindende Datenverarbeitung aufklären müssen. Eine im Jahr 2015 im Auftrag von Bitkom Research durchgeführte Umfrage ergab, dass die meisten Nutzerinnen und Nutzer solche Erklärungen nicht lesen, unter anderem wegen ihrer abschreckenden Länge (mehrere Tausend Wörter).

Manche Datenschutzerklärungen enthalten zudem Aussagen, die gar nicht zutreffen. Wir haben dazu im Jahr 2018 über eine Million deutsche Webseiten analysiert, die in der Datenschutzerklärung behaupteten, Google-Analytics zu verwenden – und zwar wohlgemerkt in Verbindung mit der zur Gewährleistung eines angemessenen Datenschutzes erforderlichen Funktion zur IP-Anonymisierung. Unsere Analyse ergab: Bei über 10% der Seiten war diese Behauptung faktisch falsch.

Datenschutzerklärungen beschreiben das „Soll-Verhalten". Ihre Effektivität ist naturgemäß begrenzt. Wünschenswert wäre es stattdessen, wenn Internetnutzerinnen und Internetnutzer den Ist-Zustand in puncto Sicherheit und Datenschutz ermitteln könnten.

Am ehesten gelingt dies mit Scanning-Diensten wie dem SSL-Test der US-amerikanischen Firma Qualys (https://www.ssllabs.com/ssltest/), dem Observatory von Mozilla (https://observatory.mozilla.org) oder dem schwedischen Projekt Webkoll (https://webbkoll.dataskydd.net). Mit diesen Diensten kann man eine Webseite auf bekannte Schwachstellen überprüfen lassen. Auch Verstöße gegen Best-Practices sowie der Einsatz von Tracking-Diensten von Drittanbietern kann dadurch aufgedeckt werden.

Die Ergebnisse der bisherigen Scan-Dienste sind allerdings nur beschränkt aussagekräftig. Wenn der Dienst Webkoll etwa 18 Tracker auf der Homepage einer bekannten Online-Apotheke meldet stellen sich viele Nutzerinnen und Nutzer sicher die Frage: „Sollte mich diese Anzahl beunruhigen oder ist das heute normal?" Gleiches gilt etwa für den Fall, dass die Webseite einer Krankenkasse beim SSL-Test von Qualys die Note „B" erreicht – ist dieses Schutzniveau ausreichend oder gehört die Seite damit bei den Krankenkassen zu den Schlusslichtern?

In beiden Fällen fehlt es für eine aussagekräftige Bewertung an Kontextinformationen. Dieser Missstand gab den Ausschlag für die Entwicklung von PrivacyScore.

Die Idee von PrivacyScore

PrivacyScore ist ein Webseiten-Scanner, mit dem sich zusätzlich Kontextinformationen zur Einordnung der Ergebnisse erheben und darstellen lassen. Dies betrifft vor allem die bereits im vorigen Abschnitt aufgeworfene Frage: Wie schneidet eine Seite im Vergleich zu vergleichbaren anderen Seiten ab? Bei PrivacyScore ist es daher möglich, nicht nur einzelne Seiten scannen zu lassen, sondern gleich mehrere Seiten, die zu einer bestimmten Gruppe gehören („Listen"). Beispiele für Listen, die es auf PrivacyScore inzwischen gibt, sind etwa alle Hochschulen in Deutschland, alle Krankenkassen und Krankenversicherungen, alle Schulen eines Bundeslands, etc. Die Bewertungen der Seiten, die zu einer Liste gehören, werden in einem sortierten Ranking leicht vergleichbar dargestellt.

Neben dem Vergleich innerhalb einer Liste sind auch Vergleiche hinsichtlich anderer Dimensionen vorgesehen: Wie haben sich die Ergebnisse im Zeitverlauf verändert? Gibt es einen Zusammenhang zwischen dem guten oder schlechten Abschneiden einer Seite und bestimmter Eigenschaften (z.B. hinsichtlich des Standorts, Finanzierungsform, Anzahl der Mitarbeiter)? Entsprechende Auswertungsfunktionen sind bislang zwar nur rudimentär angelegt, werden jedoch mit einem zukünftigen Update auch rückwirkend möglich werden, da historische Scan-Daten aufbewahrt werden.

PrivacyScore verfolgt einen Crowdsourcing-Ansatz: alle Internetnutzerinnen und Internetnutzer können jederzeit neue Listen anlegen. Die Webseiten, die zu einer Liste gehören, werden dann von PrivacyScore automatisiert gescannt. Sobald die Ergebnisse vorliegen, werden sie auf

der PrivacyScore-Webseite zusammen mit einer vom Listen-Ersteller hinterlegten Kurzbeschreibung öffentlich zugänglich gemacht. Inzwischen existieren mehr als 300 solcher Listen, die ein breites Spektrum an Branchen und Ländern abdecken.

Anreize durch Transparenz?

Das durchaus kontrovers diskutierte Alleinstellungsmerkmal von PrivacyScore besteht darin, dass nicht nur die Scan-Ergebnisse veröffentlicht werden, sondern auch ein darauf basierendes Ranking, in dem die Webseiten einer Liste anhand ihres Abschneidens sortiert werden. PrivacyScore wird dadurch zu einem Vergleichsportal für Internetseiten, das die Praktiken von Seitenbetreibern transparent macht. So wird es Nutzern möglich, mit geringem Aufwand miteinander konkurrierende Angebote miteinander zu vergleichen.

An dieser Stelle setzt auch eine der Forschungsfragen an, die wir mit PrivacyScore beantworten wollen: Inwiefern entsteht durch die von PrivacyScore erzeugte Transparenz ein Anreiz für Seitenbetreiber, ihre Webseite hinsichtlich der Sicherheits- und Datenschutzkonfiguration zu verbessern?

Nutzen für verschiedene Stakeholder

PrivacyScore verfolgt einen Open-Data-Ansatz: Die Scan-Ergebnisse werden nicht nur für Menschen aufbereitet, sondern auch in maschinenlesbarer Form (CSV, JSON) zur Verfügung gestellt. Dies erleichtert die Datenerhebung bei wissenschaftlichen Studien. Zudem lassen sich Studien einfach wiederholen und erhaltene Ergebnisse nachvollziehen.

Neben Nutzern und Wissenschaftlern sind die Betreiber von Webseiten eine wichtige Zielgruppe. Sie können mit PrivacyScore nicht nur Compliance-Überprüfungen automatisieren, sondern auch einen Eindruck vom Stand der Technik in ihrer Branche erhalten. Langfristig ist zudem geplant, für alle überprüften Kriterien technische Informationen sowie konkrete Handlungsempfehlungen zur Verfügung zu stellen.

PrivacyScore kann auch von Datenschutzbehörden eingesetzt werden. Der Code von PrivacyScore ist Open-Source-Software (MIT- bzw. GPLv3-Lizenz, https://github.com/PrivacyScore/). Aufsichtsbehörden können somit eine eigene Instanz betreiben und für eigene Zwecke nutzen.

Realisierung der Scans und deren Aussagekraft

PrivacyScore überprüft anhand von mehr als 80 Kriterien, ob beim Besuch einer Internetseite die Privatsphäre der Besucher mit – von außen erkennbaren – Mechanismen möglichst gut geschützt wird. Das tatsächliche Sicherheitsniveau lässt sich durch einen automatisierten Test von außen naturgemäß nicht ermitteln. Das Ergebnis eines Scans kann jedoch Hinweise darauf geben, wie ernst ein Seitenbetreiber den Schutz der Privatsphäre nimmt.

So wird insbesondere überprüft, ob und ggf. welche Tracking-Dienste verwendet werden (Kategorie „NoTrack"), ob ausgewählte Angriffe auf Server (etwa der Abruf eines ungeschützten Datenbank-Backups) oder Browser (z.B. Cross-Site-Scripting) verhindert werden („Attacks") sowie die Qualität der Verschlüsselung bei der Datenübertragung zur Webseite („EncWeb") bzw. beim Versand von Mails an einen ggf. vorhandenen E-Mail-Server („EncMail").

Zur Überprüfung wird jede Webseite automatisch mit einem instrumentierten Browser (derzeit Google Chrome) abgerufen, um ein möglichst unverfälschtes Ergebnis zu erhalten. Die Erkennung von Drittanbieter-Trackern basiert auf der bekannten EasyList, die auch in vielen Werbeblockern verwendet wird. Für die Überprüfung der Qualität der Verschlüsselung kommt derzeit das Tool „testssl" (https://testssl.sh) zum Einsatz.

Erste Betriebserfahrung

Seit Aufnahme des Betriebs im Juni 2017 hat PrivacyScore mehr als 1,7 Mio. Scans für 125.000 verschiedene Webseiten überprüft (Stand: Juli 2019). Für viele Seiten liegen mehrere Scan-Ergebnisse von verschiedenen Zeitpunkten vor.

Uns sind zahlreiche Fälle bekannt, wo Betreiber durch PrivacyScore auf Missstände aufmerksam wurden, die sie in der Folge behoben haben. Schlagzeilen machte im Jahr 2018 eine mit PrivacyScore gefundene Fehlkonfiguration, die die Kunden von mehr als 170 Online-Apotheken gefährdete (https://www.spiegel.de/netzwelt/web/online-apotheken-sicherheit-spanne-betraf-mehr-als-170-websites-a-1209251.html).

PrivacyScore wird jedoch nicht immer wohlwollend wahrgenommen. Im Rahmen einer auf der Konferenz

Wirtschaftsinformatik 2018 veröffentlichten Studie wurden alle auf PrivacyScore gelisteten Krankenkassen und -versicherungen mit ihrem Ergebnis konfrontiert (https://arxiv.org/abs/1811.12775). Mehrere Betreiber reagierten daraufhin mit der Androhung juristischer Schritte und verlangten, aus dem öffentlichen Ranking entfernt zu werden.

Interessenausgleich

Solchen Löschforderungen nachzukommen würde das Ziel der Transparenz verletzen. Auf Wunsch können Seitenbetreiber ihre Seiten durchaus von allen zukünftigen Scans ausnehmen lassen. Um die Interessen der Nutzerinnen und Nutzer angemessen zu berücksichtigen, bleibt in diesem Fall das letzte gültige Scan-Ergebnis und ein entsprechender Sperrvermerk öffentlich einsehbar.

Manche Seitenbetreiber sind mit diesem Kompromiss unzufrieden – rechtliche Schritte hat bislang allerdings noch niemand eingeleitet. Tatsächlich haben wir schon beim Entwurf der Plattform Juristen eingebunden, um sicherzustellen, dass der Betrieb von PrivacyScore in Deutschland zulässig ist (https://arxiv.org/abs/1705.08889).

Unabhängig von der Rechtslage stellt sich die Frage, ob es auch aus ethischer Sicht vertretbar ist, PrivacyScore zu betreiben. Immerhin werden dort potenziell ausnutzbare Sicherheitslücken veröffentlicht. Hier wurde eine sorgfältige Abwägung vorgenommen, die sowohl die durchaus erwünschten Effekte (zusätzlicher Anreiz für die Betreiber) als auch unerwünschte Effekte (Ausnutzung der Lücken durch Angreifer) berücksichtigt. Dies führte zu folgendem Kompromiss: Informationen zu Sicherheitslücken werden nicht künstlich zurückzuhalten, sondern wie alle anderen Scan-Ergebnisse veröffentlicht. Es wird aber keine Möglichkeit angeboten, systematisch nach allen verwundbaren Seiten zu suchen.

Weiterentwicklung

Es gibt zahlreiche Ideen zur Weiterentwicklung von PrivacyScore. Im Zuge eines Facelifts der Oberfläche ist geplant, die Auswertungen weitgehend personalisierbar zu machen. Sowohl Listen-Erzeuger als auch Nutzerinnen und Nutzer sollen die Gelegenheit bekommen, die Darstellung nach ihren Wünschen zu beeinflussen. Ferner sind komplexere Analysen in Entwicklung, die invasive Praktiken wie Browser-Fingerprinting und Cookie-Syncing feststellen und die Verwendung alter Software-Versionen mit bekannten Sicherheitslücken erkennen können.

SaToS: Ein LegalTech Tool zur Analyse von Allgemeinen Geschäftsbedingungen aus Verbrauchersicht

Daniel Braun und Florian Matthes

Die digitale Revolution hat zahlreiche Aspekte des alltäglichen Lebens demokratisiert. Zugang zu Wissen ist nicht länger denen vorbehalten, die sich die 32 Bände der Encyclopædia Britannica leisten können oder Zugang zu einer Universitätsbibliothek haben. Stattdessen ist das Wissen der Welt für jeden frei zugänglich im Internet. Der Zugang zu Kunst und Kultur, aber auch zu einst teuren Dienstleistungen, wie Übersetzung, wurde durch die Digitalisierung neuen Bevölkerungsschichten zugänglich.

Die Jurisprudenz hat sich lange erfolgreich gegen Digitalisierung gewehrt und hängt in vielen Aspekten noch heute dem Stand der Technik in anderen Bereich hinterher. Trotzdem hat die Digitalisierung die juristischen Professionen in Form von sogenannten „LegalTech" Tools, einem Kofferwort aus „legal services" und „technology", erreicht. Anders als in vielen anderen Lebensbereichen sind es aber vor allem große Unternehmen und Kanzleien, die bisher von dieser Entwicklung profitieren. Fast alle existierenden LegalTech Tools, wie Lexis Advance, „Juristische Textanalyse" von DATEV und Lawlift, um nur einige wenige zu nennen, richten sich nicht an Konsumenten, sondern an Unternehmen und große Kanzleien. Dabei verpassen LegalTech Tools nicht nur die Möglichkeit den Zugang zu juristischem Wissen zu demokratisieren, sie unterstützen auch aktiv das Ungleichgewicht der Kräfte das zwischen großen Unternehmen und Verbrauchern existiert, indem sie Unternehmen zusätzliche Vorteile verschaffen.

Aktuell gibt es nur wenige Tools, wie Flightright oder Chevalier, die Verbraucherinnen und Verbraucher unterstützen. Und selbst diese sind so gebaut, dass sie hauptsächlich die kommerziellen Interessen der Betreiber bedienen. In diesem Artikel wollen wir die Idee verbraucherzentrierter LegalTech Tools erläutern und präsentieren dazu zwei Tools die Allgemeine Geschäftsbedingungen (AGB, oder Englisch ToS) semantisch analysieren, juristisch bewerten und vereinfacht zusammenfassen.

Bedeutung von AGB

Konsumenten werden täglich mit AGB konfrontiert, zum Beispiel beim Onlineeinkauf oder bei der Registrierung auf einer Webseite. Studien mit mehr als 45.000 Teilnehmern haben gezeigt, dass lediglich 0.1% bis 0.2% der Konsumenten die AGB von Onlineshops lesen.[13] Während einseitig entworfene Verträge, wie AGB, regelmäßig ein Kräfteungleichgewicht zwischen den Vertragsparteien darstellen, wird dieses Ungleichgewicht noch weiter verstärkt, wenn eine der Parteien ein Unternehmen ist und die andere ein Konsument ohne juristischen Hintergrund. Die Bedeutung von AGB wird schon durch die Anzahl der Gerichtsentscheidungen in diesem Themenbereich deutlich, alleine in Deutschland gibt es mehr als 28.000 Urteile aus diesem Bereich.[14]

In Anerkennung dieser Fakten hat der europäische Gesetzgeber der Kreativität von Firmen beim Erstellen von AGB Grenzen gesetzt. Daher stellt sich die Frage, wieso illegale Klausen überhaupt Relevanz für Konsument haben, da sie im Falle eines Rechtsstreits ohnehin keinen Bestand haben. In der Realität ist es jedoch, zumindest im Fall des Onlineeinkaufs, häufig so, dass die strittigen Beträge meist so gering sind, dass Konsumenten rechtliche Schritte scheuen, selbst wenn sie im Recht sind.

13 Bakos, Yannis; Marotta-Wurgler, Florencia; Trossen, David R: Does anyone read the fine print? Consumer attention to standard-form contracts. The Journal of Legal Studies, 43(1):1–35, 2014.

14 JURIS Rechtsinformationsdatenbank. https://www.juris.de/r3/search

Ansätze

Wir haben zwei mögliche Ansätze identifiziert, um das Kräfteungleichgewicht zwischen Anbietern und Verbrauchern zu adressieren:

1. Direkte Unterstützung von Verbrauchern: Durch automatisches Auffinden, Bewerten und Zusammenfassen von AGB, mit Hinblick auf Rechtmäßigkeit und Verbraucherfreundlichkeit, können mündige Verbraucherinnen und Verbraucher in ihren Entscheidungen unterstützt werden.

2. Unterstützung von Verbraucherschützern: Statt Verbraucherinnen und Verbraucher direkt zu unterstützen, können auch Organisationen unterstützt werden, die deren Interessen vertreten, zum Beispiel mit Tools zur automatischen Analyse großer Mengen von AGB. Sol-

che Organisationen sind häufig bereit, Rechtsstreitigkeiten aufzunehmen, die Verbraucherinnen und Verbraucher scheuen, und können damit die Durchsetzung existierender Verbraucherschutzrichtlinien bewirken.

Prototypen

Um das Potential von LegelTech Anwendungen im Verbraucherschutz zu zeigen, haben wir unter dem Namen „SaToS – Software-aided Analysis of Terms of Services" zwei Prototypen entwickelt, die die oben beschriebenen Ansätze prototypisch implementieren. Beide Prototypen wurden als Webapplikationen implementiert und müssen daher nicht lokal installiert werden. Beide Backends wurden in Java implementiert und kommunizieren über eine REST-Schnittstelle mit dem Frontend.

Verbraucher-Prototyp

Der Verbraucher-Prototyp richtet sich an Menschen ohne juristische Vorbildung, die sich einen schnellen Überblick über den Inhalt der AGB eines bestimmten Webshops verschaffen wollen. Hierzu geben Nutzerinnen und Nutzer zunächst die URL des Webshops ein, dessen AGB geprüft werden sollen.

Abbildung 1 URL-Eingabe

Der Prototyp sucht dann zunächst die Unterseite, die die AGB enthält. Hierzu wird, ausgehend von der Startseite, eine Breitensuche durchgeführt. Alle verlinkten Seiten werden mit Hilfe eines Naive Bayer Classifiers darauf geprüft, ob sie AGB enthalten oder nicht. Um den Vorgang zu beschleunigen kommt außerdem ein regelbasiertes Verfahren zum Einsatz, das die Links selbst auf Schlagworte wie „AGB" analysiert und somit besonders vielversprechende Kandidaten identifizieren kann, ohne alle Seiten laden zu müssen. Als Zwischenergebnis wird die URL der AGB angezeigt (vgl. Abbildung 1).

Sobald die AGB-Seite identifiziert wurde, wird zunächst der eigentliche Inhalt extrahiert und störende Elemente wie Kopfzeilen oder Navigationselemente entfernt. Danach werden mithilfe eines regelbasierten Algorithmus Informationen aus dem Text extrahiert. Aktuell zum Beispiel der zulässige Zeitraum für Rücksendungen und Gewährleistungsrechte. Die extrahierten Informationen werden dann

mit einer Wissensdatenbank abgeglichen, die rechtliche Vorgaben für den Online-Versandhandel enthält. Basierend auf diesem Vergleich werden die Klauseln der AGB in drei Kategorien eingeteilt: rechtswidrig, gültig und besonders kundenfreundlich. Außerdem wird aus den extrahierten Informationen eine kurze und prägnante Zusammenfassung der Klausel in vereinfachter Sprache generiert. All diese Informationen werden den Nutzerinnen und Nutzern grafisch aufbereitet vorgestellt (vgl. Abbildung 2).

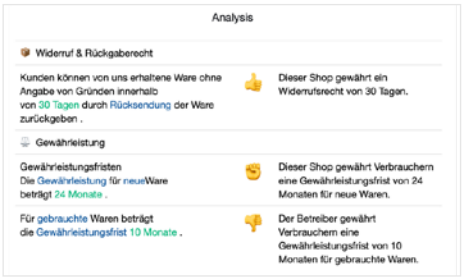


Abbildung 2 Verbraucher-Prototyp

Auf der linken Seite des Bildschirms befindet sich der Originaltext der Klausel, hier werden die Teile des Texts farbig hervorgehoben, auf deren Grundlage die Software ihre Entscheidung getroffen hat. In der Mitte befindet sich die Bewertung und auf der rechten Seite die Zusammenfassung.

Während es sich bei der Software aktuell nur um einen Prototypen handelt, hätte der produktive Betrieb eines solchen Programms juristische Implikationen, die es zu bedenken gibt. Neben der Frage nach der Haftung stellt sich insbesondere auch die Frage nach der Kompatibilität mit dem Rechtsdienstleistungsgesetz. Es könnte argumentiert werden, dass hier keine spezifische Rechtsberatung stattfindet, sondern das Tool lediglich allgemeine Erklärungen zu den analysierten AGB bietet. Trotzdem handelt es sich hierbei um eine offene Frage, die über die technische Machbarkeit hinausgeht und die es zu klären gilt, um in Zukunft auch Verbraucherinnen und Verbraucher an der technischen Entwicklung partizipieren zu lassen.

Verbraucherschützer-Prototyp

Der Verbraucherschützer-Prototyp richtet sich an Domänenexperten mit juristischer Vorbildung, die sich für den Schutz von Verbrauchern einsetzen. Sie wollen häufig mehrere Angebote auf einmal überprüfen und komplexere Analysen durchführen. Anders als im Verbraucher-Prototyp ist es deshalb möglich, mehrere URLs gleichzeitig, getrennt durch Kommata, anzugeben. Alternativ ist es außerdem möglich, PDF-Dateien zu analysieren oder einen Text direkt in die Webapplikation zu kopieren.

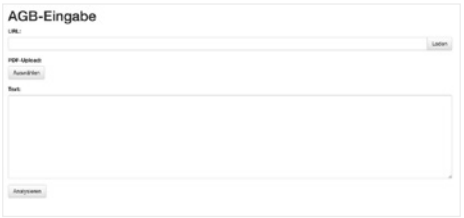


Abbildung 3 Eingabemaske

In einem ersten Schritt konvertiert das Tool zunächst alle möglichen Eingaben zu Text. Danach werden, wie zuvor beim Verbraucher-Prototyp, die eigentlichen AGB-Texte extrahiert und von Fußzeilen und Ähnlichem befreit. Anders als zuvor kommt zur Informationsextraktion kein einfacher regelbasierter Algorithmus zum Einsatz. Stattdessen wird zunächst, mit Hilfe eines neuronalen Netzwerks, ein sogenannter Dependency Tree für jeden Satz der AGB erstellt (vgl. Abbildung 4).

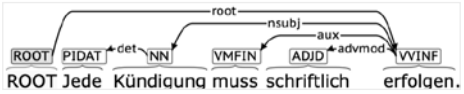


Abbildung 4 Dependency Tree

Diese Baumstruktur ermöglicht eine genauere Analyse komplexere Sätze, insbesondere zum Beispiel von Verneinungen, Nebensatzstrukturen und ähnlichen grammatikalischen Konstrukten. Am Ende werden auch hier die extrahierten Informationen mit einer Wissensbasis abgeglichen. Diesmal findet allerdings nur eine binäre Klassifikation in zulässig und unzulässig statt.

Abbildung 5 Verbraucherschützer-Prototyp

Die Anzeige der Ergebnisse ist optimiert für größere Datenmengen (vgl. Abbildung 5). Die Abbildung zeigt zum Beispiel unzulässige Einschränkungen der Kündigungsform aus mehreren AGB. Über den Button „Nur Einschränkungen anzeigen" werden nur solche AGB angezeigt, die illegale Klauseln enthalten (gekennzeichnet durch das rote Feld auf der rechten Seite). Im Mittelpunkt steht diesmal der Originaltext. Einschränkungen des Kündigungsform sind rot markiert im Text, vorgeschriebene Kündigungsformen sind grün markiert.

Zusammenfassung

Die beiden vorgestellten Prototypen geben einen Ausblick auf das Potential von LegalTech Tools für den Verbraucherschutz. Die Analyse von AGB ist dabei nur ein Beispiel für mögliche Anwendungsgebiete. Neben der prototypischen Implementierung der semantischen Analyse wollen wir vor allem Aufmerksamkeit dafür schaffen, dass nicht nur Unternehmen und Kanzleien von der Digitalisierung im Rechtsbereich profitieren können, sondern auch Verbraucher. Neben den technischen Fragen gilt es dazu aber auch, die skizzierten juristischen Fragen zu klären.

AVARE (Eine Anwendung zur Verteilung und Auswahl rechtskonformer Datenschutzeinstellungen)

Gunther Schiefer

Mobile Geräte (Smartphones) sind inzwischen aus dem täglichen Leben der meisten Verbraucherinnen und Verbraucher nicht mehr wegzudenken. Sie nutzen täglich mehrfach verschiedene Anwendungen (Apps), welche oftmals eine Vielzahl von Informationen vom Gerät abfragen und diese Informationen – für Verbraucherinnen und Verbraucher nicht kontrollierbar– an den Anbieter und ggfs. an Dritte weitergeben. Demgegenüber ist es das Grundrecht jedes Verbrauchers darüber zu bestimmen, wer welche personenbezogenen Daten über ihn zu welchem Zweck erhebt und verarbeitet und wie lange er diese speichert. In der Praxis können viele mobile Dienste nur genutzt werden, wenn der Anwender dem Dienstanbieter eine umfassende Datenerfassung und -analyse erlaubt. Teilweise ist dies für die Kernfunktionalität der Anwendung erforderlich, teils jedoch nur, um ggfs. Zusatzfunktionalität anzubieten, welche Verbraucherinnen und Verbraucher nicht benötigen oder sogar, um ein auf den Daten basierendes Geschäftsmodell umzusetzen. Oftmals können Verbraucherinnen und Verbraucher nur entscheiden, ob sie ihre Daten weitergeben und damit den Dienst nutzen können, oder den Dienst nicht zu nutzen. Die Weigerung, personenbezogene Daten zur Verfügung zu stellen, führt teilweise zu erheblichen Nachteilen für die soziale Interaktion.

Ziel von AVARE ist es daher, die Datensouveränität von Verbrauchern zu stärken. Dazu soll ihnen ein einfach zu nutzendes Werkzeug an die Hand gegeben werden, mit dem Verbraucherinnen und Verbraucher ihr Recht auf informationelle Selbstbestimmung innerhalb der rechtlichen Schranken besser durchsetzen können. AVARE solle es Ihnen ermöglichen, die an eine App übermittelten Daten auf das unbedingt notwendige Maß zu beschränken, ohne die gewünschte Funktionalität zu verlieren.

Um dies zu realisieren, kann die entwickelte AVARE-App auf einem Smartphone installiert werden. Diese erzeugt einen abgeschotteten Bereich („Sandbox" genannt) in den die zu kontrollierenden Apps eingepackt werden. AVARE ist somit in die Verbindung zwischen dem Smartphone und der App „eingeklinkt". Dies ist rechtlich zulässig, da es sich bei dem zugrundeliegenden Betriebssystem (Android) um eine Open-Source-Software handelt, die eine solche Modifikation des Programmablaufs in den Lizenzbedingungen zulässt. Durch das Einklinken kann AVARE jetzt kontrollieren, welche Daten vom Smartphone an die App weitergegeben werden. Die Betriebssysteme von Smartphones ermöglichen inzwischen ebenfalls, bestimmte Kategorien von Daten (z.B. die gespeicherten Kontakte) für eine App freizugeben oder zu sperren. Eine totale Sperre führt jedoch oftmals dazu, dass die App nicht mehr funktioniert. AVARE erweitert die Möglichkeiten, indem es den Verbrauchern feingranularere Filter für Datenkategorien an die Hand gibt, in denen sie detailliert einstellen könne, welche Informationen eine App bekommen darf. Damit können z.B. an eine Messenger-App aus den Kontakten nur Name und Mobiltelefonnummer eines Kontaktes weitergegeben werden, alle weiteren Informationen zu diesem Kontakt werden vorher herausgefiltert. Weiterhin können gezielt nur bestimmte Kontakte überhaupt freigegeben werden, alle weiteren Kontakte bleiben vor der App verborgen. Ein anderes Beispiel ist die Vergröberung der Genauigkeit der Ortung. Eine Anwendung, welche z.B. das aktuelle Wetter am derzeitigen Standort anzeigen soll, benötigt keinen adressengenauen Aufenthaltsort. Hier reicht auch eine Ortungsgenauigkeit, welche um mehrere Kilometer ungenau („falsch") sein kann. Eine solche „unscharfe" Ortung kann AVARE ebenfalls durch einen Filter für die Kategorie Ortung realisieren.

Zunehmend werden von Verbrauchern mehrere Geräte verwendet, z.B. ein Smartphone unterwegs und zu Hause ein Tablet. Damit hier die Einstellungen nicht mehrfach vorgenommen werden müssen, wurde weiterhin der AVARE-Sync-Server entwickelt. Darüber können die Einstellungen zwischen mehreren Geräten synchronisiert werden. Der AVARE-Sync-Server wurde entsprechend der Projektziele auf Datensparsamkeit und einfache Anwendbarkeit hin konzipiert. Der Server lernt insbesondere aufgrund einer Client-seitigen Verschlüsselung und eines Schlüsselaustausches unabhängig vom Server keine Informationen über

die eigentlichen Einstellungen. Dabei ist der Schlüssel nur dem Verbraucher bekannt, die Einstellungen selber können vom Serverbetreiber nicht eingesehen werden. Ebenso ist keine persönliche Registrierung nötig. Es wird lediglich eine Kennung (Pseudonym) benötigt, welches keine Hinweise auf die Identität des Verbrauchers oder die ID-Kennungen seiner Geräte enthält.

Die AVARE-Anwendungen bauen auf existierenden Open-Source-Komponenten auf. Unabhängig davon ist die gesamte entwickelte Software unter einer Open-Source-Lizenz mit weitreichenden Verwendungsmöglichkeiten veröffentlicht (Apache-2.0-Lizenz). Damit können die Anwendung oder auch Teile davon vielfältig in anderen Anwendungsfällen (z.B. des Verbraucherschutzes) weiter verwendet werden. Bisher sind erst wenige Filter technisch konzipiert bzw. in der Entwicklung. Das Konzept von AVARE erlaubt es jedoch, AVARE um weitere Filter zu ergänzen und damit die Funktionalität zu erweitern. Ebenso bedingen Änderungen am Betriebssystem teilweise auch Änderungen an der AVARE-App. Aus diesem Grund ist das bisherige Entwickler-Team auf der Suche nach weiteren Mitstreitern ebenso wie nach zukünftigen Finanzierungsquellen für eine Weiterentwicklung von AVARE als technische Unterstützung für den Verbraucherschutz.

Weitere Informationen zu AVARE finden sich unter http://privacy-avare.de, eine erste Testversion der AVARE-App ist unter https://avare.app/ verfügbar. Das Projekt AVARE („Anwendung zur Verteilung und Auswahl rechtskonformer Datenschutzeinstellungen") wurde von der Baden-Württemberg Stiftung gGmbH im Rahmen des Forschungsprogramms „IKT-Sicherheit" finanziert. Projektträger war das DLR.

CLAUDETTE: The automated unfair clause detector

Kasper Drążewski und Hans-W. Micklitz

Hintergrund

Die im Jahr 2018 eingeführte Allgemeine Datenschutzverordnung war als Mittel zur Stärkung der Position des Verbrauchers durch ein strenges Korsett von Regeln für die Verarbeitung personenbezogener Daten geplant. Die Einführung betonte jedoch nur die wachsende Asymmetrie zwischen Verbrauchern und Online-Dienstleistern. Studien zum Verbraucherverhalten zeigen, dass es angesichts der Länge und Komplexität der Datenschutzrichtlinien nur wenige Nutzerinnen und Nutzer gibt, die diese Dokumente tatsächlich lesen, was nicht überraschen sollte, da Studien zeigen, dass die Zeit, die für das verständnisorientierte Durchlesen aufgewendet wird, auch einen finanziellen Wert hat.

CLAUDETTE (ein **Portmanteau** von Automated Clause Detector) ist ein Experiment, das darauf abzielt, festzustellen, ob Verbraucherinnen und Verbraucher ihre eigenen KI-basierten Werkzeuge einsetzen können, um die mühsame Aufgabe des Lesens und Analysierens von Nutzungsbedingungen und Datenschutzrichtlinien zu übernehmen, und Verbraucherinnen und Verbrauchern eine kondensierte Zusammenfassung von Klauseln zur Verfügung zu stellen, die potenziell unfair sind, oder nicht den Anforderungen der DSGVO entsprechen.

AGB Analyse mit einer Kombination aus Machine Learning und SVM

Der erste Prototyp von Claudette ist 2018 angelaufen mit einem Korpus von 50 AGB Verträgen und eingesetzten Machine Learning Architekturen zur Textkategorisierung und einem strukturierten SVM (**Support Vector Machine**) zur kollektiven Klassifizierung von Sätzen. Im Trainingsdatensatz wurden unfaire Klauseln identifiziert, in Kategorien eingeteilt und nach Grad der Rechtswidrigkeit zwischen 1 und 3 eingestuft. So würde beispielsweise eine Haftungsklausel, die besagt, dass der Dienstleister eine Haftung übernimmt, als „1" angesehen und mit „<ltd1>" getagged werden, während eine Klausel, die Ausschlüsse wie vorsätzliche Beschädigung oder grobe Fahrlässigkeit enthält, als „3" eingestuft und somit mit „<ltd3>" getagged würde.

In Experimenten, in denen Claudette

gegen Nutzungsbedingungen, die bisher nicht vom System verwendet wurden, eingesetzt wurde, reichte die Genauigkeit der Identifizierung spezifischer Kategorien von 72,7% bei Schiedsklauseln bis hin zu 89,7% bei Zuständigkeitsklauseln. Der Prototyp von Claudette 1.0, der einen Trainingsdatensatz von 50 Serviceverträgen verwendet, steht unter http://claudette.eui.eu/demo/ zur freien Verfügung.

Claudette 2.0: DSGVO Konformitätsbewertung

Damit Claudette eine Prüfung der Datenschutzrichtlinien durchführen kann, musste der Standard für eine korrekt gestaltete Datenschutzrichtlinie festgelegt werden. Als Maßstab für die Analyse der Einhaltung der Datenschutzrichtlinien wurden drei Dimensionen für die Bewertung entwickelt: 1) Vollständigkeit der Informationen, wobei darauf zu achten ist, dass die nach den Artikeln 13 und 14 der DSGVO erforderlichen Informationen tatsächlich enthalten sind; 2) wesentliche Konformität, wobei es geprüft wird ob die Richtlinie nur die Verarbeitung personenbezogener Daten zulässt, die mit der DSGVO übereinstimmen; 3) Klarheit des Ausdrucks, womit die Formulierung aus der Perspektive von Verständlichkeit und Genauigkeit bewertet wird. Zusammengenommen schufen diese drei Dimensionen den sogenannten **Goldenen Standard**. Die Leistungsgrade in den einzelnen Kategorien wurden in einer Weise bewertet, wie sie zuvor für die Analyse missbräuchlicher Klauseln verwendet wurde.

Umfassende Informationsvielfalt

Diese Dimension der Bewertung konzentriert sich darauf, wie umfassend die Informationen sind, die eine Klausel vermittelt. So wird beispielsweise bei der Bewertung einer Klausel, die das Recht auf Einreichung einer Beschwerde bei einer Aufsichtsbehörde angibt, eine Einstufung vorgenommen, je nachdem, ob erklärt wird, ob die betroffene Person das Recht hat, eine Beschwerde bei einer Aufsichtsbehörde des Mitgliedstaats einzureichen, in dem sie ihren gewöhnlichen Aufenthalt, ihren Arbeitsplatz oder ihren Ort einer angeblichen Verletzung der DSGVO hat. In diesem Fall, gilt die Klausel als informationell vollständig und wird mit <complain1> getagged. In allen anderen Fällen wird sie als <complain2> markiert.

Beispiel: Uber Datenschutzerklärung (zuletzt aktualisiert am 25. Mai 2018)

<complain2>"Users in the EU also have the right to file a complaint relating to Uber's handling of your personal information with the Autoriteit Persoonsgegevens, the Dutch Data Protection Authority."</complain2>

Wesentliche Konformität

Diese Dimension betrifft die Frage, ob die in einer Datenschutzerklärung festgelegten Verarbeitungsarten DSGVO-konform sind. Viele Datenschutzregeln enthalten derzeit „problematische" Klauseln, die signalisieren, dass der Datenverantwortliche nicht DSGVO-konform handelt (unter anderem gemessen an Artikeln 5, 6 und 9 der DSGVO). So wird beispielsweise eine Klausel, wonach die Daten einen externen Datenverantwortlichen weitergegeben werden dürfen, wenn der Gegenstand der Übermittlung und der Umfang nicht angegeben sind und die Zustimmung nicht fakultativ ist und/oder die Übermittlung für die Erfüllung des Vertrags nicht erforderlich ist, als nicht konform getagged (<tc3>).

Beispiel: Apple Datenschutzerklärung (zuletzt aktualisiert am 9. Mai 2019)

<tc3>At times Apple may provide third parties with certain personal information to provide or improve our products and services, including to deliver products at your request, or to help Apple market to consumers.</tc3>

Klarheit des Ausdrucks

Im Hinblick auf das Erfordernis einer klaren und verständlichen Sprache haben wir zwei Arten von Klauseln identifiziert, nämlich Klauseln, die in einer klaren Sprache ausgedrückt sind (nicht markiert), und Klauseln, die in einer unklaren Sprache ausgedrückt sind, für die wir das folgende Tag definiert haben: < vag>. Dies wird durch die Verwendung der folgenden Indikatoren ausgelöst: 1) **an Bedingungen geknüpfte Bestimmungen** („wenn wir glauben, dass eine solche Offenlegung notwendig ist"); 2) **Verallgemeinerungen** („Wir sammeln typischerweise oder allgemein Informationen..."), 3) **Modalitäten** („wir können Ihre personenbezogenen Daten verwenden, um neue Dienstleistungen zu entwickeln") und 4) **unspezifische numerische Quantifizierer** („wir können eine Vielzahl von Informationen erfassen, einschließlich Ihres Namens, Ihrer Postanschrift, Telefonnummer, E-Mail-Adresse, Kontaktpräferenzen [....]").

Beispiel: Airbnb Datenschutzerklärung vom 16. April 2018

<vag>"Some of this information as indicated in your Account settings is part of your public profile page, and will be publicly visible to others."</vag>

Die Zukunft von Claudette: Ambitionen für 2019 und darüber hinaus

Mehrsprachigkeit

Claudette wird auf Englisch entwickelt. Da es sich jedoch um ein EU-Projekt zur Verbrauchergegenmachtbildung handelt, ist die Inklusion weiterer Sprachen von entscheidender Bedeutung. Um einen zeitaufwändigen und kostspieligen Aufbau eines Trainingsdatensatzes in jeder neuen Sprache zu vermeiden, testen wir, ob die Wiederverwendung des vorhandenen Datensatzes zur Automatisierung des Aufbaus neuer Trainingsdatensätze in anderen Sprachen möglich ist.

Dieser Ansatz basiert auf der Erstellung einer Referenzdatei in der Zielsprache, bei der ein bereits markiertes Dokument aus dem englischen Trainingsdatensatz mit einer maschinellen Übersetzungsmaschine übersetzt wird. Beispielsweise müsste für Deutsch eine mit einem Tag versehene Datenschutzerklärung in englischer Sprache maschinell ins Deutsche übersetzt werden. Die Referenzdatei wird dann mit der offiziellen deutschen Datenschutzerklärung verglichen, um entsprechende Sätze zu identifizieren. Danach kann das Tagging in die offizielle deutsche Datenschutzerklärung übertragen werden, wodurch ein deutschsprachiger Trainingsdatensatz entsteht. Obwohl dieser Ansatz stark von der Qualität der maschinellen Übersetzung und der Ähnlichkeit der politischen Dokumente in verschiedenen Sprachen abhängt, ist es wichtig zu beachten, dass dieses Vorgehen den Aufbau eines neuen Systems mit sich bringt, wenn eine neue Sprache integriert wird, wodurch eine Feinabstimmung der natürlichen Sprachverarbeitungsalgorithmen für jede Sprache separat möglich ist.

Rechtfertigungen

Ein weiteres Feature, mit dem wir experimentieren, ist, dass Claudette die bereit gestellten Ergebnisse begründet. Mit anderen Worten, Ziel ist es, zu sehen, ob das System lernen kann, die Gründe zu identifizieren, warum eine bestimmte Kategorie der Rechtswidrigkeit oder eine bestimmte Art von Compliance-Problem für die gegebene Klausel hervorgehoben wurde. Einer der hier getesteten Ansätze ist es, die Begründung der Gerichte zu nutzen und dem System beizubringen, wie man die am besten geeignete Argumentation findet und wählt. Hierzu muss das Gerichtsurteil in eine Kette von Implikationen zerlegt werden, die verwendet werden können, um das System darin zu trainieren, ähnliche Denkmuster zu verfolgen.

Beispiel: C-137/08, VB Penzügyi

eine Klausel in einem Vertrag ist aus GründenderGerichtsbarkeitungerecht

wenn

der Vertrag ein Verbrauchervertrag ist

die Zuständigkeitsklausel nicht einzeln ausgehandelt wurde

Die Klausel zu einem erheblichen Ungleichgewicht zum Nachteil des Verbrauchers führt

wenn

die Klausel ie ausschließliche Zuständigkeit auf ein Gericht überträgt, bei dem der Verkäufer oder Lieferant seinen Hauptgeschäftssitz hat

Der Web Crawler

Um Situationen entgegenzuwirken, in denen sich die Nutzungsbedingungen ohne Vorankündigung ändern können, ist Überwachungsfunktion in Entwicklung, die Verbraucherinnen und Verbraucher über Änderungen der Nutzungsbedingungen oder Datenschutzdokumente einer vorab ausgewählten Liste von Dienstleistern informiert. In seiner Grundform steht die Funktionalität bereits zur Verfügung, wenn Änderungen anhand eines einfachen Datums- und Textvergleichs identifiziert werden. Die gewünschte Funktionalität setzt jedoch ein hohes Maß an inhaltlicher Sensibilität voraus, bei dem das System in der Lage sein muss, Bedeutungsänderungen auf der Grundlage von Änderungen des Wortlauts des betreffenden Rechtsdokuments zu entschlüsseln. Mit einem ausreichenden Budget kann aber auch dies zweifellos erreicht werden.

"Verbraucher Empowerment durch Künstliche Intelligenz: Elemente einer Forschungsagenda" - Zusammenfassung

Lucia A. Reisch, Christian Thorun und Hans-W. Micklitz

Die Veranstaltung hat gezeigt:

Die Verbraucherforschung steht vor der Aufgabe, ein **neues Forschungsgebiet** systematisch zu entwickeln, sowohl inhaltlich (theoretisch und empirisch) als auch strukturell und institutionell.

Neben dem wissenschaftlichen Interesse steht das politische Ziel, die Handlungsmöglichkeiten der Verbraucherinnen und Verbraucher durch den Einsatz von Künstlicher Intelligenz und Machine Learning zu erweitern. Es geht um **digitale Souveränität** der Einzelnen, auf kollektiver Ebene auch um **Gegenmacht**.

Der **Bedarf an Evidenz** und praxisrelevanten Projekten („proof of concept") ist hoch (siehe u.a. Digitalstrategie der Bundesregierung; Digitalstrategie der Bundesländer, insbesondere die Digitalisierungsstrategie Baden-Württemberg; nationale Strategie Künstliche Intelligenz; diverse Gutachten des Sachverständigenrats für Verbraucherfragen u.a. zu „Digitale Souveränität"[15]).

Die technologische Entwicklung ist rasant. Die politische Rahmensetzung läuft hinterher. Die Verbraucherpolitik muss sich dahingehend einmischen, gemeinsam eine gute, **verbraucherfreundliche Datenpolitik** zu entwickeln. Teil davon ist, die technologischen Möglichkeiten auch der Verbraucherseite zugänglich zu machen, ggf. in Partnerschaften mit Akteuren der Wirtschaft und der Digital-Szene.

15 Bundesregierung. (2019). Digitalisierung gestalten. Umsetzungsstrategie der Bundesregierung. Aktualisierung März 2019. Berlin: Presse- und Informationsamt der Bundesregierung; Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg. (2017). Digitalisierungsstrategie der Landesregierung Baden-Württemberg. Stuttgart: Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg im Auftrag der Landesregierung. Abgerufen von https://www.digital-bw.de/documents/20142/0/DigitalisierungsstrategieBaWue2017.pdf/2ca4e48e-0830-c81c-8dc2-6ebde1a93024; Die Bundesregierung (2018). Strategie Künstliche Intelligenz der Bundesregierung. https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstliche-intelligenz-der-bundesregierung.pdf?__blob=publicationFile&v=6; Sachverständigenrat für Verbraucherfragen. (2016). Verbraucherrecht 2.0 - Verbraucher in der digitalen Welt. Gutachten des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen. Sachverständigenrat für Verbraucherfragen. (2017). Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen. Berlin: Sachverständigenrat für Verbraucherfragen.

Es gibt bereits einige **innovative Projekte** in den neu entstehenden Forschungsrichtungen im Bereich „Verbraucherinformatik" allgemein sowie speziell im Bereich des Verbraucher-Empowerment durch Künstliche Intelligenz. Meist sind es Praxisprojekte; besonders relevante und innovative Projekte waren beim Workshop vertreten[16].

In der Forschung befassen sich mehrere Disziplinen - meist in disziplinärer Sichtweise - mit diesen Themen. Das Forschungsfeld wird von diesen Disziplinen und Richtungen gegenwärtig vielfältig beschrieben und sucht seinen Namen: **Verbraucherinformatik**, Verbraucherempowerment, Consumer informatics, the digital consumer, VerbraucherTech, legal tech, Algorithms for good, machine learning etc. haben Schnittstellen, unterscheiden sich aber auch. Hier besteht **grundlegender konzeptioneller Klärungsbedarf** bezüglich des Inhalts, der Abgrenzung sowie der Schlüsselthemen.

Die Zusammenarbeit mehrerer Disziplinen und Subdisziplinen in dieser Art von Forschung ist notwendig. Interdisziplinäre und **transdisziplinäre** Herangehensweisen sorgen für den Anschluss und die Nutzbarkeit an die Verbraucher(politk)praxis. Eine besondere Rolle spielen: Verbraucherrecht und -politik, Informatik / Data Science (AI, ML), (Daten-)Ethik, (Daten-)Politik und Verhaltensforschung, Designforschung und sozial-digitale Partizipation. Aber auch andere Disziplinen können bei speziellen Fragen hochrelevant sein.

16 DATENSCHUTZscanner (Dr. Sara Kettner), PrivacyScore (Prof. Dominik Herrmann), SaToS (Prof. Florian Matthes), AVARE (Dr. Gunther Schiefer), Claudette II (Prof. Hans-W. Micklitz und Dr. Kasper Drążewski). Aber auch andere Disziplinen

Der Themenbereich ist bislang systematisch unterforscht. Wichtig wären einige **größere Calls** bzw. ein **Forschungsprogramm Verbraucherinformatik**. Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) hat vor kurzem eine einschlägige Projektausschreibung publiziert. Wichtig wäre es, systematisch Budget aus der Strategie Künstliche Intelligenz und der Digitalstrategie des Bundes für Verbraucherforschung abzustellen.

Die digitale Welt endet nicht an Landesgrenzen. Sowohl in Forschung als auch in der Verbraucherpolitik sollten internationale, vor allem **europäisch wirksame Projekte** gefördert werden. Dies ist besonders relevant, weil die systematisch unterfinanzierte Verbraucherpolitik thematische Schwerpunkte

bilden muss und sich weitgehend im europäischen Raum bewegt. Zudem sollte es möglich sein, Konsortien auch grenzüberschreitend zu organisieren.

Dabei kann es sehr sinnvoll sein, wenn **Bundesländer (wie Baden-Württemberg)** mit besonderen Stärken hier Vorreiter sind und beispielsweise „proof of concept" Studien finanzieren.

Grundsätzlich sollten gemeinsam mit den jeweiligen politischen und subpolitischen Akteuren (Verbraucherzentralen, Europäische Verbraucherzentrum Deutschland in Kehl, Landeszentren für Datenschutz, BEUC etc.), Start-ups und Forschern **Verbundprojekte** geplant werden. Besonders interessant ist auch hier das Format der **Reallabore**[17].

17 Siehe dazu https://mwk.baden-wuerttemberg.de/fileadmin/redaktion/m-mwk/intern/dateien/pdf/Aktuelle_Ausschreibungen/Reallabor_KI/2019-05-16_Ausschreibung_Reallabor_KI.pdf

Im Rahmen des Verbraucherforschungsforums wurden folgende Themenfelder für eine Forschungsagenda genannt:

AGB und Datenschutz

- Vereinfachte AGB Kontrolle und Datenschutz-Scanner
- Vereinfachte Prüfung der Qualität von Online-Angeboten (fake shops, fake labels etc.)
- Verbraucherfreundliche Architektur von Webseiten

Empowerment: Digitale Unterstützung von Verbraucherbildung, - beratung, -information

- Bessere, „smarte" Verbraucherinformation
- Personalisierung, Apps, real time feedback
- Dialogplattformen mit diversen Stakeholdern, um die Bedürfnisse zu erfahren

Vereinfachte Rechtsdurchsetzung

- legal tech
- smart contracts

Datensouveränität

- Bessere Kontrolle und Datenmanagement durch Daten-Dashbords oder Data-Wallets
- Blockchain zur Datensicherung
- KI zur Förderung von Nachhaltiger Entwicklung

Autorinnen und Autoren

Dr. Kasper Drążewski

Europäische Hochschulinstitut Florenz

Dr. Kasper Drążewski ist wissenschaftlicher Mitarbeiter am Europäischen Hochschulinstitut (EUI) in Florenz. Seine aktuelle Forschungsarbeit konzentriert sich auf die Anwendung künstlicher Intelligenz im Bereich des Verbraucherschutzes. Dr. Drążewski hat sich neben seiner Doktorarbeit auch dem Thema der modernen Herausforderungen an Urheberrecht und Softwareinnovation gewidmet. Neben einem LL.M. und einem Ph.D. in Rechtswissenschaften an der EUI hält er einen MA in Rechtswissenschaften an der European School of Law and Administration und in Journalismus an der Universität Warschau. Dr. Drążewski ist außerdem Senior Editor beim European Journal of Legal Studies.

Daniel Braun

Lehrstuhl für Software Engineering betrieblicher Informationssysteme, Technische Universität München

Daniel Braun ist seit Mai 2016 wissenschaftlicher Mitarbeiter am Lehrstuhl für Software Engineering betrieblicher Informationssysteme (sebis) an der Technischen Universität München. Sein Forschungsschwerpunkt liegt im Bereich der Generierung und Verarbeitung natürlicher Sprache (NLG/NLP) für juristische Anwendungen und Sprachinterfaces. Zuvor studierte er Informatik an der University of Aberdeen und der Universität des Saarlandes.

Prof. Dr. Dominik Herrmann

Lehrstuhl Privatsphäre und Sicherheit in Informationssystemen, Universität Bamberg

Prof. Dr. Dominik Herrmann hält seit 2017 eine Professur für Privatsphäre und Sicherheit in Informationssystemen an der Universität Bamberg inne. Die Absicherung von Informationssystemen und der Schutz der Privatsphäre mit technischen Mechanismen steht im Fokus seiner Arbeit. In diesem Rahmen analysiert und evaluiert sein Team an der Universität Bamberg existierende Informationssysteme und entwickelt Schutzmechanismen. 2014 wurde seine Promotion über die Überwachung im Internet und datenschutzfreundliche Techniken von der Gesellschaft für Informatik e.V. (GI) ausgezeichnet.

Dr. Micha Kaiser

Forschungszentrum Verbraucher, Markt und Politik | CCMP, Zeppelin Universität Friedrichshafen

Dr. Micha Kaiser ist akademischer Mitarbeiter am Forschungszentrum Verbraucher, Markt und Politik und unterstützt das Team insbesondere bei der Durchführung und Auswertung von quantitativen Studien. Seine Forschungsbereiche umfassen Gesundheitsökonomie und Konsumentenverhalten, zu denen er bereits an der Universität Hohenheim und im Rahmen eines Aufenthalts an der Universität Oxford forschte. Sein methodischer Schwerpunkt liegt dabei auf der Ökonometrie, Statistik und „Machine Learning".

Dr. Sara Elisa Kettner

ConPolicy-Institut für Verbraucherpolitik Berlin

Dr. Sara Elisa Kettner ist Projektmanagerin im Bereich der Verbraucherforschung bei ConPolicy, dem Institut für Verbraucherpolitik. Sie ist zuständig für Beratungsprojekte und Studien im Bereich Verbraucherpolitik und Behavioral Insights. Ihre Themenschwerpunkte sind dabei Digitalisierung, Datenschutz und Corporate Digital Responsibility. Im Rahmen Ihrer bisherigen Tätigkeit hat sie unter anderem Projekte für die Europäische Kommission, das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) und das Bundesministerium für Bildung und Forschung (BMBF) umgesetzt sowie Unternehmen im Bereich der digitalen Verantwortung beraten. Als PostDoc forschte sie an der Quadriga Hochschule Berlin im Rahmen des Privacy Guard Projekts zu Nutzerverhalten und Datenschutz im Bereich von Smartphone-Apps.

Prof. Dr. Florian Matthes

Lehrstuhl für Software Engineering betrieblicher Informationssysteme | Technische Universität München

Prof. Dr. Florian Matthes ist seit 2002 Inhaber des Lehrstuhls für Software Engineering betrieblicher Informationssysteme (sebis) an der Fakultät für Informatik der Technischen Universität München. Seine Forschung fokussiert sich auf Technologien und Methoden, um die digitale Transformation von Unternehmen und Gesellschaften zu unterstützen. Als Beiratsmitglied der Ernst Denert-Stiftung für Software Engineering, Gründer von Blockchain Bayern e.V. und Organisator internationaler Fachveranstaltungen fördert er die Zusammenarbeit zwischen Praktikern und Wissenschaftlern in der Informatik und Wirtschaftsinformatik. Neben seinen Tätigkeiten in Forschung und Lehre ist er Mitgründer und Aufsichtsratsvorsitzender der CoreMedia AG und infoAsset AG, Mitgründer der Tr8cy Ltd. Und Gründungsbotschafter der UnternehmerTUM.

Prof. Dr. Hans-W. Micklitz

Europäische Hochschulinstitut Florenz

Prof. Dr. Hans-W. Micklitz war bis September 2019 Professor für Wirtschaftsrecht am European University Institute (EUI). Ab Oktober 2019 ist er Finland Distinguished Professor an der Universität in Helsinki sowie Part-Time Professor am Robert Schuman Centre for Advanced Studies am European University Institute in Florenz. Seine Forschungsschwerpunkte sind Europäisches und Deutsches Privat- und Wirtschaftsrecht zu Themen des Vertrags und Deliktsrechts, der technischen Normung und Zertifizierung, der Produktsicherheit, des Anlegerschutzes, der unlauteren Geschäftspraktiken, der Haftung für unsichere Dienste, der regulierten Märke (Telekommunikation, Energie, Finanzen und Verkehr) sowie der Rechtsdurchsetzung. Er ist Herausgeber des Journal of Consumer Policy und Experte in zahlreichen Fachgremien, wie zum Beispiel dem Sachverständigenrat für Verbraucherfragen des Bundesministeriums der Justiz und für Verbraucherschutz.

Grit Puchan

Ministerium für Ländlichen Raum und Verbraucherschutz Baden-Württemberg

Frau Puchan ist seit dem 1. Juni 2016 Ministerialdirektorin im Ministerium für Ländlichen Raum und Verbraucherschutz Baden-Württemberg. Im Jahr 1988 legte Frau Puchan ihr 2. Juristisches Staatsexamen an der Julius-Maximilians-Universität Würzburg ab und war dann als Rechtsanwältin tätig. Seit 1990 ist Frau Puchan Landesbeamtin in Baden-Württemberg mit verschiedenen Stationen in der Landesverwaltung, davon unter anderem Referentin im Umweltministerium, Dezernentin im Landratsamt Main-Tauber-Kreis, Leiterin des Rechts- und Planfeststellungsreferats im Regierungspräsidium Tübingen, Pressesprecherin des Regierungspräsidiums Tübingen und Leiterin der Abteilung Umwelt im Regierungspräsidium Tübingen. Von 2009 bis 2015 war sie Regierungsvizepräsidentin des Regierungspräsidiums Tübingen. Es folgte ab November 2015 bis Mai 2016 das Amt als Leiterin der Abteilung II Landtag von Baden-Württemberg.

Prof. Dr. Lucia A. Reisch

Forschungszentrum Verbraucher, Markt und Politik | CCMP, Zeppelin Universität Friedrichshafen

Prof. Dr. Lucia A. Reisch gründete das Forschungszentrum Verbraucher, Markt und Politik (CCMP) im Januar 2012 an der Zeppelin Universität in Friedrichshafen. Sie ist Professorin für Konsumforschung und Verbraucherpolitik an der dänischen Copenhagen Business School und hält eine ständige Gastprofessur an der Zeppelin Universität. Im Rahmen ihrer Forschung widmet sie sich den Themen des Verbraucherschutzes, der Nachhaltigkeit, Verhaltensökonomk und Gesundheitswissenschaften. Sie ist Herausgeberin des Journal of Conusmer Policy und Expertin in zahlreichen Fachgremien, wie zum Beispiel dem Rat für Nachhaltige Entwicklung. Von 2015 bis 2018 war sie Vorsitzende des Sachverständigenrats für Verbraucherfragen des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV).

Dr. Gunther Schiefer

Karlsruher Institut für Technologie (KIT), Institut Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)

Dr.-Ing. Gunther Schiefer ist Teil der Forschungsgruppe für betriebliche Informationssysteme des Karlsruher Instituts für Technologie (KIT). Dort beschäftigt sich der Informatiker seit mehr als 15 Jahren mit der Erforschung und Entwicklung von Methoden und Verfahren für die sichere und vertrauenswürdige Nutzung von Daten mit mobilen Geräten und in der Cloud. Seine Schwerpunkte sind die digitale Souveränität des Anwenders, Privatheit von Daten und Informationen sowie die ganzheitliche Gestaltung von anforderungsadäquaten sicheren Prozessen. Er initiiert und koordiniert nationale und internationale Verbundforschungsprojekte mit Unternehmen und Forschungseinrichtungen.

Prof. Dr. Christian Thorun

ConPolicy-Institut für Verbraucherpolitik Berlin

Prof. Dr. Christian Thorun ist Gründer und Geschäftsführer des ConPolicy-Instituts für Verbraucherpolitik, das in einem breiten Spektrum der Verbraucherpolitik aktiv ist und evidenzbasierte Strategien und Instrumente für politische Entscheidungsträger, Verbände und Unternehmen entwickelt. Prof. Thorun ist als Beiratsmitglied im Verein für Selbstregulierung der Informationswirtschaft (SRIW) tätig. Darüber hinaus ist er Sprecher der Themenplattform Verbraucherbelange am Zentrum Digitalisierung.Bayern (ZD.B) und sitzt im unabhängigen ÖKOWORLD-Anlageausschuss. Als Mitglied des Think Tank 30, einer interdisziplinären Organisation unter dem Dach der Deutschen Gesellschaft des Club of Rome, ist er Teil eines Netzwerks junger Menschen, die sich mit Zukunftsfragen auseinandersetzen.

Impressum

1. Auflage September 2019

Herausgeber

Lucia A. Reisch, Christian Thorun
und Hans-W. Micklitz

Koordination

Zeppelin Universität gemeinnützige GmbH

Forschungszentrum Verbraucher, Markt
und Politik

Am Seemooser Horn 20

D-88045 Friedrichshafen

Gefördert
durch

Baden-Württemberg
MINISTERIUM FÜR LÄNDLICHEN RAUM
UND VERBRAUCHERSCHUTZ