



in Kooperation mit



DiDaT STAKEHOLDER KONFERENZEN KONSORTIUM



2. Stakeholderkonferenz am 22.01.2020



Vertrauenswürdigkeit digitaler Informationen - VR 06

1. Gegenstand, Ziele und Leitfragen

- Digitalisierung ermöglicht neue Manipulation von Informationen, deren diskursive Verhandlung politisch, sozial, wirtschaftlich und juristisch wirksam ist
- Entwicklung der Informationstechnik hat die generelle Zeugenschafts- und Vertrauensproblematik verschärft

AG-Mitglieder: Markus Breuer, Martin Fuchs, Sebastian Hallensleben, Andreas Kaminski, Julio Lambing, Sabine Thürmel, Malte Reißig, Christian Reuter, Deborah Ryszka

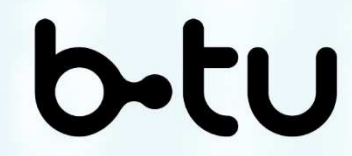
Inhaltlich verantwortlich für den vorliegenden Entwurf: S. Hallensleben, A. Kaminski, J. Lambing

Leitfrage

Wie können IT-gestützte Vertrauensinfrastrukturen so gestaltet werden, dass ein fakten- und wertebasierter öffentlicher, wissenschaftlicher und politischer Diskurs möglich bleibt, um eine Disruption der Grundlagen von Demokratie und Rechtsstaat zu verhindern?

2. Unseens, Ursachen und Maßnahmen zu sozial robusten Orientierungen im VR06

	1. Unseens	2. Ursachen / Kausalitäten / Entstehungsprozesse der Unseens	3. Maßnahmen möglicher sozio-technologischer Innovationen zur Mitigation	4. Sozial robuste Orientierungen zum Umgang mit Unseens
			Erste Ideen / Vorschläge zur Diskussion	
1	Herkunft & Vertrauenswürdigkeit von Information nicht mehr klar	Erweiterte technische Möglichkeiten zur Fälschung Schwere Erkennbarkeit von Fälschungen; nur mit immer ausgefeilteren Tools (Wettrüsten Erkennung ↔ Fälschung)	Standards für die 1zu1-Zuordnung v. Informationen zu Person / Organisation als Urheber: -> Normungsprozesse in etablierten Foren -> Gesetzliche Unterstützung der Standards -> Öffentlichkeitsarbeit - Nutzung kryptograf. Funktionen in ID-Cards - Erforschung Blockchain-basierter Lösungen, wo staatlicher Vertrauensanker unakzeptabel	Gesellschaftlich verfügbare und verbreitete Instrumente zur Rückverfolgung von Informationsquellen etablieren Nachrichtenquellen müssen eine Identität tragen, ohne Quellenanonymität zu gefährden
2	Misstrauen & Rückzug aus dem konstruktiven demokratischen Diskurs	Überflutung & Schnelligkeitsdrang von Informationen	Entwicklung / Verbreitung von Alternativen zum "Gefällt mir"; Beispiele: - "Gefällt mir" für erfolgreiche Dialoge - Online-Reputationsgewinne durch erfolgreiche Kompromissbildung	Aufbau und Verbreitung soziotechnischer Strukturen zur Förderung von Konsens und Kompromiss
3	Desorientierung & erzwungene Unmündigkeit des Einzelnen (Vertrauensverlust, Reality Apathy, Zynismus)	Erweiterte techn. Möglichkeiten zur schnellen Verbreitung von Informationen Kommerzielle Anreize, skandalisierende, extreme und/oder emotional erschütternde Nachrichten zu verbreiten	Protokolle & Reputationstools zur Visualisierung der Vertrauenswürdigkeit eines Online-Akteurs - Implementierung Pilotprojekte - Entwicklung/Erforschung theoretischer Modelle für Online-Verhalten Leuchtturmprojekte (für Demonstration Vorteile & Optimierungsanalyse)	
4	Beeinträchtigung oder sogar Zusammenbruch review-basierter Plattformen, insb. in der Sharing Economy	Staatliche & nichtstaatliche Akteure, die bürgerliche Öffentlichkeit, Politikbetrieb und Medienwelt destabilisieren wollen	Bildungsprogramme zur Identifizierung von Erkenntnisbarrieren & Perspektivverzerrungen sowie zu Know-How, sich Informationen umsichtig & kritisch zu beschaffen	Stärkung der Urteilsfähigkeit des mündigen Bürgers
5	Öffentlichkeit vertraut dem staatlichen Rechtssystem nicht mehr	Politische bzw. soziokulturelle Polarisierung in den liberalen Demokratien Zahlreiche Menschen, die aus privaten, malignen Intentionen Falschinformationen verbreiten	? Strafbarkeit für die absichtliche Erstellung und Verbreitung von Fälschungen, die nicht als Satire oder Fiktion erkennbar sind Etablierung von für Nichttechniker plausiblen Notariatsmechanismen	? Rechtswesen, den Bedingungen des digitalen Zeitalters anpassen



Brandenburgische Technische Universität
Cottbus - Senftenberg

in Kooperation mit



DiDaT STAKEHOLDER KONFERENZEN KONSORTIUM



Universität Bremen

2. Stakeholderkonferenz am 22.01.2020



Vertrauenswürdigkeit digitaler Informationen - VR 06

3. Stakeholder

- Inhaltliche Eingrenzung: Angriffe durch gefälschte Informationen, die erst durch ihre Wahrnehmung und ihre diskursive Verhandlung in sozialen Räumen ihre schädliche Wirkung erhalten
- Beschränkung des Untersuchungsfelds auf Gefährdung von Demokratie und Rechtsstaat
- In Abgrenzung zu VR05 ist nicht die Funktion, Struktur und Akteurskonstellation spezifischer Bereiche des digitalen öffentlichen Raums (z.B. Social Media, klassische Medien etc.) im Blick
- Problemlage ist zwar international; aber diskursive verhandelte Informationen finden in national-staatlichen Kommunikationsgemeinschaften und Rechtsräumen; deshalb Stakeholder aus D-A-CH

Unseen x Stakeholder-Tabelle im VR06

	Unseens (Unintended Side Effects; unbeabsichtigte Nebenfolgender Nutzung digitaler Daten)	„Verursacher“	„Betroffene“	„Problemlöser / Regulatoren“
1	Herkunft & Vertrauenswürdigkeit von Information nicht mehr klar	Alt-Righter, Russian bots, 50 Cent Party, Maga Trolls; Astroturfer	Journalisten, Blogger, Influencer; Medieninhaber, Chefredakteure	Betreiber sozialer Netzwerke; Contentkuratoren und -aggregatoren, Suchmaschinen-betreiber; Medieninhaber, Chefredakteure; Anbieter u. Entwickler von Notariatslösungen; Vertrauenswürdige neutrale Instanzen (z.B. Prüfer, Zertifizierer);
2	Misstrauen & Rückzug aus dem konstruktiven demokratischen Diskurs	Journalisten, Blogger, Influencer; Alt-Righter, Russian bots, 50 Cent Party, Maga Trolls; Astroturfer, Hatemobs	Einzelne Wähler / Bürger	Journalisten, Blogger, Influencer; Entscheider aus Politik & Verwaltung
3	Desorientierung & erzwungene Unmündigkeit des Einzelnen (Vertrauensverlust, Reality Apathy, Zynismus)	Betreiber sozialer Netzwerke; Contentkuratoren und -aggregatoren, Suchmaschinen-betreiber; Revenge Porn, Cyber Stalker, Cyber Bullies, Incels; ScriptKiddies; Hatemobs	Betreiber sozialer Netzwerke	Medienpsychologen, Kommunikationsforscher; Betreiber sozialer Netzwerke; Contentkuratoren und -aggregatoren, Suchmaschinenbetreiber; Netzaktivisten, NGOs
4	Beeinträchtigung oder sogar Zusammenbruch review-basierter Plattformen, insb. in der Sharing Economy	Contentkuratoren und -aggregatoren, Suchmaschinenbetreiber; Review Faker, Shamazon Fakers	Contentkuratoren und -aggregatoren, Suchmaschinenbetreiber	Contentkuratoren und -aggregatoren, Suchmaschinenbetreiber;
5	Öffentlichkeit vertraut dem staatlichen Rechtssystem nicht mehr	möglicherweise mediale Akteure der Unrechtsverherrlichung?	Einzelne Wähler / Bürger; Polizei, Verfassungsschutz, Rechtsprechung	Polizei, Verfassungsschutz, Rechtsprechung; Internetjuristen; Entscheider aus Politik & Verwaltung; Anbieter u. Entwickler von Notariatslösungen; Vertrauenswürdige neutrale Instanzen (z.B. Prüfer, Zertifizierer); Betreiber sozialer Netzwerke
	Anforderungen an Repräsentanten von Stakeholdergruppen in DiDaT VR06	Target: ?	Beispiel: Politblogger, ECPMF, Truly Media, Traditionelle und neue Leitmedien; Rechtsexperten	Beispiel: VDE, TÜV, BSI, Richter, Blockchain-Anbieter, Zeitung, Netzpolitische Aktivisten wie #ichbinhier

4. Ergebnisse

- Breit konsensfähiger Lösungsansatz, aufbauend auf den skizzierten Arbeitshypothesen
- Abschätzung anhand von Test Cases, wie weit der Ansatz trägt und wo ggf. noch Schwächen sind
- Grundlagen für Pilotierung in der Vertiefungsforschung

5. Ausblick

- Grundlegende Transformation des Umgangs mit Vertrauen im digitalen Raum durch die Schaffung neuartiger Infrastrukturen und Werkzeuge
- Rückgewinnung des digitalen Raums als Ort des konstruktiven Diskurses und der gesellschaftlichen, politischen und wissenschaftlichen Innovation