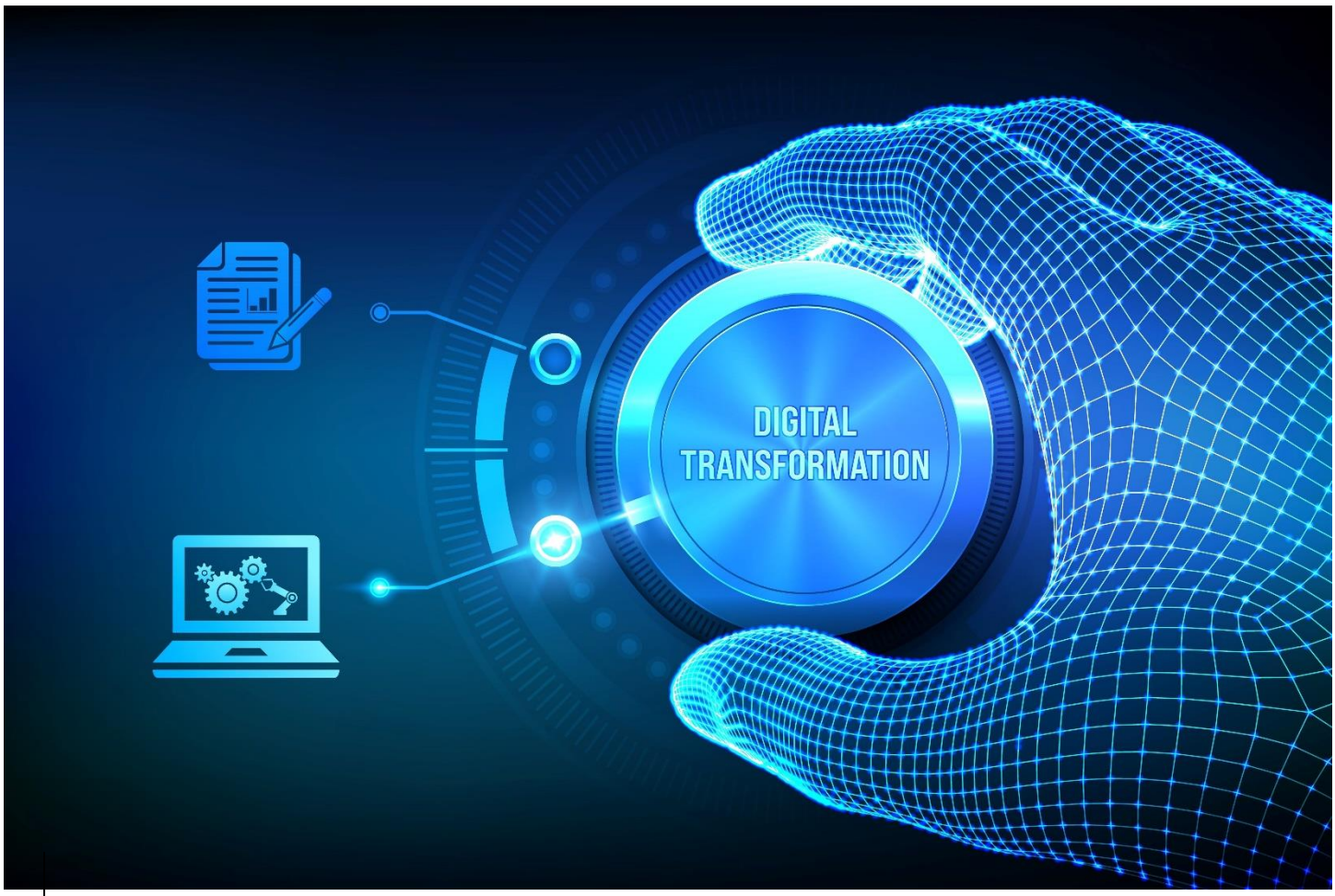
Hessische Staatskanzlei
Ministerin für Digitale Strategie und Entwicklung

HESSEN

# Herausforderungen der digitalen Transformation für die Stabilität von Demokratie






digitales.hessen

## 1. Zur Einführung

Der Rat für Digitalethik hat sich im Jahr 2022 in seinen Sitzungen mit der Frage befasst, inwieweit der im Gang befindliche Prozess der digitalen Transformation Auswirkungen auf unser demokratisches, auf Partizipation angelegtes Gemeinwesen hat. Entsprechend seinem Auftrag, die Hessische Landesregierung bei der Umsetzung und Steuerung der digitalen Transformation zu beraten, hat er drei Themenfelder identifiziert, denen bei der politischen Willensbildung und Rahmensetzung auf der Ebene des Landes hohe Priorität einzuräumen ist: Informations- und Kommunikationsverhalten, Finanzsektor und Kryptowerte sowie IT-Sicherheit für Unternehmen und Behörden. Der Rat für Digitalethik ist sich bewusst, dass sich die angesprochenen Herausforderungen nicht allein innerhalb eines einzelnen Bundeslandes klären lassen, geht aber davon aus, dass der Landespolitik politische Handlungsspielräume zur Verfügung stehen, die unbedingt zu nutzen sind.

## 2. Informations- und Kommunikationsverhalten

Besonders deutlich verändert die digitale Transformation das Informations- und Kommunikationsverhalten unserer Gesellschaft. Nach der ARD-ZDF-Onlinestudie 2021 sind täglich 54 Millionen Deutsche über vier Stunden im Internet. Dabei nutzen über 70 % täglich Messenger-Dienste wie WhatsApp. Soziale Netzwerke wie Facebook, Instagram und Twitter, Kommentarspalten von Videoplattformen wie YouTube und TikTok oder auch journalistische Onlinepublikationen werden täglich von 50 % der Deutschen genutzt – unter den 14 bis 29-Jährigen sogar von fast 90 %. Dies bedeutet jedoch nicht, dass wichtige Werte wie etwa Barrierefreiheit und digitale Teilhabe aller Bürgerinnen und Bürger im Netz bereits verwirklicht wären.

Digitalisierung vervielfältigt Informationszugänge, sie bietet aber auch zuvor unbekannte Verbreitungspfade für nicht qualitätsgesicherte Mitteilungen. Von daher kann man die basisdemokratischen Potentiale von Netzkommunikation loben: Sie hat die klassische Pressearbeit bereichert und die Zahl der – schnellen, authentischen, multimedialen, international verbreitungsfähigen – Formate erheblich anwachsen lassen. Zugleich stellt aber die digitalisierte Kommunikation unsere Gesellschaft wie auch die Medienlandschaft vor große Herausforderungen: Falschinformationen, Deep Fakes, gezielte Desinformationen und staatliche Propaganda sind für demokratische Gesellschaften eine reale Gefahr. Auch sogenannte Fake Science – also vorgetäuschte Wissenschaftlichkeit – führt zu einer Unterminierung der Glaubwürdigkeit von Presse und Wissenschaft. Medienpolitik, einschlägig forschende Wissenschaft und eine mündige Gesellschaft müssen sich diesen Herausforderungen stellen. Ertragreiche und gesellschaftsfördernde Debatten sind nur möglich, wo für das, was Nachrichtenwert hat, Mindeststandards existieren und wo

auch die automatisierten Verbreitungswege von Informationen nicht einen (vermeintlichen) Sensationswert zusätzlich überhöhen.

Mit der Transformation des Informations- und Kommunikationsverhaltens entstehen zudem völlig neue Räume für anonyme, herabwürdigende und bedrohliche Äußerungen. Bislang ist jede oder jeder Dritte von mindestens einer Form von Hass im Netz betroffen gewesen; besonders im Fokus stehen dabei politisch und journalistisch tätige Personen. Die schnelle Verbreitung, die Beteiligung und Kenntnisnahme anderer Personen sowie die damit verbundene Perpetuierung und nahezu unbegrenzte Reichweite digitaler Massenkommunikation hat zur Folge, dass Menschen sich in Reaktion auf solche Angriffe seltener zu ihrer Meinung bekennen und sich seltener an Diskussionen im Netz beteiligen (sogenannter Silencing-Effekt). Der Effekt, dass Personen, Positionen und Berichterstattung aus dem öffentlichen Diskurs verdrängt werden, stellt daher eine Bedrohung für den freien und offenen Meinungsaustausch und damit für die Stabilität von Demokratie insgesamt dar.

Der Rat für Digitalethik spricht sich dafür aus, im Hinblick auf digitale Kommunikationsräume und plattformgebundene Öffentlichkeiten keine Kluft zwischen Anspruch und Wirklichkeit des den demokratischen Meinungsaustausch aller und die Pressefreiheit garantierenden Art. 5 des Grundgesetzes zu dulden: Ethische und (presse)rechtliche Standards – etwa das Prinzip der Zeichnung von politischen Botschaften mit dem eigenen Klarnamen – müssen analog wie digital Grundlage der politischen Diskussionen sein. Anonymität von Hasskommunikation darf es nicht geben. Verpixelung von Bildern kann zwar im Einzelfall geboten sein. Dennoch müssen der Öffentlichkeit – wo es um faktengetreue Berichterstattung geht – grundsätzlich unverpixelte Bilder zugemutet werden können. Auch müssen die öffentlich-rechtlichen Medien in die Lage versetzt werden, innerhalb der Grenzen ihres gesetzlichen Auftrags ihr Programmangebot um hinreichend vielfältige digitale Formate zu erweitern. Innovative Formen der Zusammenarbeit zwischen öffentlich-rechtlichen und privaten Qualitätsmedien sollten, gerade im Bereich von Infrastrukturen, gefunden werden. Eine vielschichtige und diverse Presselandschaft der Autorinnen und Autoren – mit einer funktionierenden Rückkopplung in Wissenschaft und Gesellschaft – ist Voraussetzung für eine funktionierende Demokratie.

Der Rat für Digitalethik erkennt an, dass die Hessische Landesregierung der gesellschaftlichen Erwartung an ein verstärktes Vorgehen staatlicher Institutionen gegen Hassrede im Internet bereits im Jahr 2019 durch das Aktionsprogramm „Hessen gegen Hetze“ nachgekommen ist. Dazu ist u.a. eine zentrale staatliche Meldeplattform für Bürgerinnen und Bürger, Unternehmen, Medi-

enhäuser, Behörden, Kommunen etc. eingerichtet worden, über die Hasskommentare nutzerfreundlich und auf Wunsch auch den Sicherheitsbehörden anonym gemeldet werden können. Ebenso ist eine Kooperation von staatlichen und zivilgesellschaftlichen Organisationen zur Prävention von Hass und Hetze im Internet und zur Opferberatung beschlossen worden. Es ist zu wünschen, dass derartige Programme auch über Strafverfolgung hinaus zu einem Kulturwandel beitragen.

Gleichwohl regt der Rat für Digitalethik an, dass die Hessische Landesregierung durch geeignete Maßnahmen (z.B. Konsultationen und Anhörungen) eine offene und partizipative Diskussion über das Spannungsfeld zwischen Anonymität und Verantwortlichkeit bei der Internetkommunikation in Gang setzt. Einerseits sichert Anonymität im Netz die Informationsfreiheit sowie die freie Meinungsäußerung und kann Personen davor schützen, auch im analogen Leben zur Zielscheibe von Hass und Aggression zu werden. Andererseits kann Anonymität im Netz zu einer Enthemmung und Verrohung des öffentlichen Diskurses beitragen und den Rechtsgüterschutz sowie die Rechtsdurchsetzung erschweren.

## 3. Finanzsektor, Kryptowerte und Demokratie

Die Welt des Geldes ist durch Digitalisierung deutlich abstrakter und unübersichtlicher geworden. Global tätige Internetkonzerne planen eigene Zahlungsmittel und treten damit in eine Art Konkurrenz zum Staat. Digitale Finanzprodukte, dezentrale Kreditvergabe und andere dezentrale Finanzprodukte („De-Fi“) boomen. Krypto-Werte („Krypto-Währungen“) wie Bitcoin oder Ether erfreuen sich als staatsferne Zahlungsmittel sowie als Spekulationsgegenstände mit zeitweilig hohen Renditen einer wachsenden Beliebtheit. Zahlreiche alternative Anlage- und Investitionsangebote knüpfen ebenso an die Idee eines gänzlich dem staatlichen Einfluss entzogenen Wirtschaftens an. Solche Angebote sind oft komplex, schwer durchschaubar und nicht selten unseriös. Kryptowerte unterliegen enormen Schwankungen, was deren Verwendung riskant macht. In Zeiten hoher Inflation könnte die Risikobereitschaft dennoch weiter steigen – und auch die Anziehungskraft von auf Gewinnmaximierung angelegten, libertär-anarchistischer Internet-Ideologien ist beträchtlich. Krypto-Communities grenzen sich nicht selten von demokratischer (Rechts) Staatlichkeit mehr oder weniger offen ab. Technik soll Recht und demokratische Diskurse ersetzen. Frustration über „den Staat“ kann hier Existenzkrisen und Verschuldung nach sich ziehen.

Das Wissen der Bevölkerung über Geldanlagen und Finanzmarktmechanismen generell ist in Deutschland gering und ungleich verteilt. Erst recht gilt dies für das Wissen über die digitale Transformation des Finanzsektors, die ein globales Phänomen ist, den europäischen Alltag jetzt aber erreicht hat. Zugleich drängen digitale Bezahlverfahren in Europa ganz generell die Nutzung

von Bargeld zurück. Die Covid-19-Pandemie hat diese Entwicklung auch in Deutschland – einem relativ bargeldfreundlichen Land – verstärkt. Digitales Bezahlen ist oft bequem. Es ist aber niemals anonym, was Befürchtungen vor gläsernen Kundinnen und Kunden und womöglich einem Überwachungsstaat weckt. Welcher Mix einer künftigen Geldnutzung passt also zu einer Demokratie?

Digitale Finanzkompetenzen stellen eine wichtige – und unterschätzte – Dimension derjenigen digitalen Kompetenzen dar, an denen es in der Gesellschaft aktuell fehlt. Eine auf Befähigung aller Beteiligten ausgerichtete Bildungspolitik muss dafür sorgen, dass Bürgerinnen und Bürger aller Altersgruppen digitale Finanzkompetenzen erlangen. Benötigt wird ein digitaler Verbraucherschutz, der sich in verstärktem Maße auf komplexe Finanzprodukte erstreckt. Gerade für das Land Hessen mit dem herausragenden Finanzplatz Frankfurt/Rhein-Main ist vor einem pauschalen Hype rund um neue Finanzprodukte zu warnen. Eine leistungsfähige Strafverfolgung sollte auch dem Schutz vor digitaler Finanzkriminalität und digitalen Betrugsformen dienen.

Ergänzend schlägt der Rat für Digitalethik der Hessischen Landesregierung vor, eine breite, öffentliche und partizipative Diskussion über den „Digitalen Euro“ zu initiieren, also über digitales Zentralbankgeld, dessen Einführung die Europäische Zentralbank derzeit erwägt. Das erforderliche Maß an Wissen, um dieses für die Demokratie wichtige Projekt zu verstehen und zu bewerten, fehlt derzeit weitgehend – denn Geld ist etwas, das alle angeht. Selbst in den verantwortlichen Institutionen ist digitales Zentralbankgeld ein Thema, mit dem sich Fachleute intensiv befassen müssen. Veränderungen der Währung stellen eine Schlüsselfrage für das Vertrauen der Bürgerinnen und Bürger in ihren Staat dar. Die Hessische Landesregierung sollte daher die zu erwartende Diskussion über die Einführung und Ausgestaltung eines „Digitalen Euro“ (als einer Art anonymes digitales Bargeld) nicht nur passiv abwarten, sondern das Gespräch mit den Bürgerinnen und Bürgern eröffnen. Durch derartige partizipative Diskurse kann das Land Hessen ein Vorreiter bei der demokratischen Ausgestaltung einer künftigen digitalen Zentralbankwährung für Europa sein.

## 4. IT-Sicherheit für Unternehmen und Behörden

Durch die zunehmende Digitalisierung sämtlicher Lebens-, Arbeits- und Geschäftsbereiche ist die IT-Sicherheit (englisch Cybersecurity) als zentraler Bestandteil der Informationssicherheit mittlerweile zu einer Top-Priorität von Unternehmen und Behörden, zum Beispiel aber auch von Kommunen, Hochschulen, gesellschaftlichen Akteuren wie Vereinen etc. (im Folgenden gemeinsam „Organisationen“) geworden.

Die IT-Sicherheit richtet sich primär gegen Cyberkriminalität. Hierunter lassen sich zahlreiche und immer vielfältiger werdende Bedrohungsformen subsumieren, angefangen vom einfachen Computervirus über Cyberkriminalität und Cyberspionage bis hin zu Cyberterror und Cyberware. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt in seinem jüngsten Bericht zur Lage der IT-Sicherheit in Deutschland fest, dass die Gefährdungslage im Cyber-Raum so hoch wie nie zuvor ist. Ein effektives Cybersecurity-Management – im besten Falle als Bestandteil eines Informationssicherheits-Managementsystems – verringert unter Nutzung geeigneter Technologien, Prozesse und Maßnahmen das Risiko, d.h. die Wahrscheinlichkeit und die möglichen Auswirkungen erfolgreicher Cyberangriffe.

Schutzgut der Informationssicherheit sind generell Informationen. Aufgrund der hohen Bedeutung von Informationen als Unternehmenswerte sollen Informationen jeglicher Art und Herkunft in Bezug auf die primären Ziele Vertraulichkeit, Integrität und Verfügbarkeit geschützt werden.

Die Digitalisierung fordert Organisationen damit auch im Hinblick auf ihre IT-Sicherheit in mehrfacher Hinsicht heraus: Auf der Ebene des reinen Kerngeschäfts sind die Organisationen gezwungen, ihre IT-Sicherheit ständig zu erhöhen. Es müssen Prozesse implementiert werden, die den hohen und dynamischen Anforderungen an organisatorische, technische, personelle und infrastrukturelle Implikationen gerecht werden und eine stetige Überprüfung und Verbesserung der Sicherheitsmaßnahmen ermöglichen.

Unter ethischer Perspektive stellen sich allerdings für Organisationen im Kontext der IT-Sicherheitstechnik noch deutlich größere Herausforderungen als die, die aus dem reinen Kerngeschäft resultieren. Sie werden im Bereich von Unternehmen unter dem Begriff der „Corporate Digital Responsibility“ diskutiert. Überwiegend verstanden als ein Bestandteil oder zumindest angelehnt an den Begriff und das Verständnis der „Corporate Social Responsibility“ wird Entscheidungsträgerinnen und Entscheidungsträgern hiermit ein hohes Maß an gesellschaftlicher Verantwortung zugeschrieben. Diese geht über die eigene klassische unternehmerische Verantwortung für den ökonomischen Erfolg deutlich hinaus: Gefordert ist das Etablieren von Kernwerten, also einer Werteorientierung innerhalb der jeweiligen Organisation und damit im Ergebnis um einen verantwortungsbewussten Umgang mit der Digitalisierung generell.

Daneben stellen sich Fragen der Überwachung, zum Schutz von Eigentum im digitalen Zeitalter, zum ständigen Konflikt Vertraulichkeit versus Verfügbarkeit bzw. Privacy versus Security oder auch zum ethischen Hacken. Die Balance zwischen einem angemessenen, an die konkreten

Bedürfnisse der jeweiligen Organisation angepassten Niveau an IT-Sicherheit und der Berücksichtigung anderer Werte – etwa von Privatsphäre, Fairness oder auch Autonomie – ist eine tägliche Herausforderung für das Management von Organisationen aller Art. Dies gilt umso mehr, als Unternehmen auch bei der Produktentwicklung Sicherheitsaspekte nicht vernachlässigen dürfen („Security by Design“). Die IT-Sicherheit bewegt sich regelmäßig in einem komplexen Geflecht von Werten, die je nach Kontext neu austariert und gegeneinander abgewogen werden müssen und immer wieder zu neuen Dilemmata bei der Entscheidungsfindung führen können. Aufgrund bislang fehlender Ausdifferenzierung dieser Werte, die sich als Richtschnur für unternehmerisches Handeln eignen könnten, bewegen sich die Akteure oftmals in einem großen Graubereich, der sie bei der Auswahl vielfältiger Handlungsoptionen überfordern kann und sich nachteilig im Unternehmensalltag auswirkt.

Der Rat für Digitalethik ist davon überzeugt, dass ein vertrauenswürdiger Umgang mit der Digitalisierung im Alltag alle angeht. Wir stehen vor der Aufgabe, unsere Gesellschaft im Kontext der Komplexität und Geschwindigkeit der technologischen Entwicklungen verantwortungsvoll zu strukturieren und zukunftsfähig zu halten. Eine dementsprechend effektive und verantwortungsvolle IT-Sicherheit ist hierfür unabdingbar.

Um Organisationen bei dieser wichtigen Aufgabe nicht alleine zu lassen oder gar zu überfordern, tritt der Rat für Digitalethik dafür ein, den politischen Diskurs zu verstärken. Ziel der Verständigung sollte es sein, festzulegen in welcher konkreten Art und Weise der Schutzgedanke umgesetzt werden soll. Eine klare Verortung und ein Ausloten der Cybersecurity mit ihren zugrundeliegenden digitalen Technologien und ihrer Verantwortlichkeit sind in den Organisationen und für unsere Gesellschaft unabdingbar. Es geht damit nicht zuletzt darum, welche Normen und Regeln wir uns auferlegen, um unsere Verantwortung zu definieren.

Da bereits der Fokus auf dem erfolgreichen Verfolgen des Kerngeschäfts für eine Vielzahl kleiner und mittlerer Unternehmen oftmals Herausforderung genug ist, tritt der Rat für Digitalethik dafür ein, diesen Organisationen seitens der Hessischen Landesregierung neben bestehenden Angeboten wie bspw. des CyperCompetenzCenter (Hessen3C) durch eine gezielte Förderung von Schulungsmaßnahmen zu unterstützen, um eigenes Know-how aufzubauen. Daneben sollten Förderprogramme, die den Aufbau und die Investition in IT-Infrastrukturen honorieren, intensiviert werden. Zudem regt der Rat für Digitalethik an, für Unternehmen allgemein Anreize zu schaffen, um ein hohes Niveau an Informationssicherheit zu erreichen, etwa durch die Installation eines eigenen Informationssicherheits-Managementsystem (z.B. Zertifizierung nach BSI-Grundschutz

oder ISO 27001). Denkbar wäre hier eine gezieltere Ermessensausübung im Rahmen der Auftragsvergabe.

## 5. Aktiv werden – Demokratie stärken

Der Prozess der digitalen Transformation schreitet mit großer Geschwindigkeit voran. Noch sind manche seiner Folgen nicht vollends absehbar. Umso wichtiger ist es, diesen Prozess nicht sich selbst zu überlassen, sondern um der Stabilität von Demokratie willen in den drei spezifischen Bereichen Informations- und Kommunikationsverhalten, Finanzsektor und Kryptowerte sowie IT-Sicherheit für Unternehmen und Behörden politisch tätig zu werden – sei es durch die Initiierung gesellschaftlicher Debatten, sei es durch gesetzgeberische Rahmensetzungen oder durch Initiativen im Bundesrat. Der Rat für Digitalethik hofft daher, dass seine Vorschläge innerhalb der politischen Gremien des Landes Hessen und darüber hinaus Beachtung finden und zu einer sachgemäßen, kompetenzgeleiteten öffentlichen Debatte beitragen.

## 6. Weiterführende Hinweise


- ARD/ZDF, „Onlinestudie 2021“, abrufbar unter www.ard-zdf-onlinestudie.de
- Bundesamt für Sicherheit in der Informationstechnik (BSI), Informationssicherheit mit System - Der IT-Grundschutz des BSI, 2020, aufrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/sonstiges/Informationssicherheit_mit_System.pdf?__blob=publicationFile&v=3
- Bundesamt für Sicherheit in der Informationstechnik (BSI), Die L age der I T-Sicherheit in Deutschland 2022, 2022, aufrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6
- Christen, Markus/ Gordijn, Bert/ Loi, Michele (Herausgeber), The Ethics of Cybersecurity, Springer Open, Cham, Schweiz 2020.
- FORSA, „Befragung zur Wahrnehmung von Hassrede“, 2021, abrufbar unter https://www.medienanstalt-nrw.de/themen/hass/forsa-befragung-zur-wahrnehmung-von-hassrede.html
- FORSA, „Umfrage Hass und Gewalt gegen Kommunalpolitiker/innen“, 2021, abrufbar unter https://koerberstiftung.de/site/assets/files/16886/umfrage_hass_und_gewalt_gegen_kommunalpolitiker.pdf
- Hessen CyberCompetenceCenter Hessen3C, Hessisches Ministerium des Innern und für Sport, https://innen.hessen.de/Sicherheit/Cyber-und-IT-Sicherheit/Cybersicherheit
- Hessisches Cyberabwehrausbildungszentrum, Hessisches Ministerium des Innern und für Sport, https://innen.hessen.de/sicherheit/cyber-und-it-sicherheit/cybersicherheit/hessisches-cyberabwehrausbildungszentrum
- Hessisches Ministerium des Innern und für Sport, „Broschüre 2 Jahre Meldestelle HessenGegenHetze“, 2022, abrufbar unter https://hessengegenhetze.de/sites/hessengegenhetze.hessen.de/files/2_broschuere_2_jahre_meldestelle_hessengegenhetze_0.pdf
- Hoven, Elisa/Forschungsgruppe g/d/p, „Hass im Netz: Ergebnisse einer Studie“, 2022, abrufbar unter https://www.jura.uni-leipzig.de/fileadmin/prins_import/dokumente/dok_20220829123452_ae0b27c451.pdf

- Krause, Benjamin, Hate Speech - Strafbarkeit und Strafverfolgung von Hasspostings, C.H.Beck Verlag, München 2022
- Papendick Michael/ Rees Yann/ Wäschle Franziska/ Zick Andreas, Hass und Angriffe auf Medienschaffende - Eine Studie zur Wahrnehmung von und Erfahrungen mit Angriffen auf Journalist*innen, 2020, abrufbar unter https://pub.uni-bielefeld.de/download/2943243/2943245/Studie_Hass_und_Angriffe_auf_Medienschaffende.pdf
- Schmidt, Matthias, Ethik in der IT-Sicherheit. Eine Einführung, UVG-Verlag, Berlin 2021
- Zentrum verantwortungsbewusste Digtalisierung ZEVEDI, Projekt „Demokratiefragen des digitalisierten Finanzsektors“ des Zentrums Verantwortungsbewusste Digitalisierung und der Stiftung Mercator