ArGe Digitale Transformation: Safety, Security and Privacy

Online-Meeting: Digitale Souveränität

27. Juni 2022, 16:00-18:00 Uhr, remote

Digitale Souveränität – ein an sich nicht neues Konzept – sollte einer der Grundsteine der Digitalen Transformation sein und hat in der jüngeren Vergangenheit wieder an Brisanz gewonnen. Die Vorträge und Diskussionen des Online-Meetings der ÖFG ArGe Digitale Transformation am 28.6.2022 zeigten auf, dass im Hinblick auf Digitale Souveränität noch längst nicht alle Grundsatzfragen diskutiert bzw. praktischen Probleme gelöst sind. Als Fallbeispiele dienten der österreichische Umgang mit Gesundheitsdaten während der COVID-Krise sowie die Produktion und Verbreitung von Inhalten rund um den Ukraine-Krieg auf der Plattform Reddit.

In seinem Vortrag „Was lernen aus Covid?“ führte Univ.-Prof. Dr. Nikolaus Forgó (Universität Wien) einleitend aus, dass bereits seit den 1990ern bestehende Erkenntnisse und Entscheidungen zu Themen wie der Unabhängigkeit des Cyberspace auch heute noch Gültigkeit haben. Die in diesem Zeitraum enorm gewachsene Technologie- und Internetlandschaft besteht jedoch mittlerweile aus einzelnen großen Akteuren, von denen nur wenige in Europa angesiedelt sind. Dieser Umstand wurde von der Europäischen Kommission schon lange vor der COVID-Krise und dem Ukraine-Krieg als ein Sicherheitsrisiko identifiziert, dem man mit technologischer und digitaler Souveränität begegnen möchte. Im Kontext der EU bedeutet dies meist, Regulatorien zu erarbeiten und zu implementieren – im Hinblick auf Informationssicherheit ist die DSGVO wohl eines der bekanntesten. Das Ziel, den individuellen Bürger:innen die Souveränität über ihre persönlichen Daten zu garantieren, wird jedoch in der Praxis nicht unbedingt erreicht. Dies lässt sich zum Beispiel anhand der österreichischen Verordnungspraxis im Rahmen der COVID-Krise veranschaulichen, in der die Übermittlung von Gesundheits- und genetischen Daten in einer Form erlaubt wird, die (1) eine Einhaltung der DSGVO verunmöglichen und (2) natürliche Personen (z.B. Bürgermeister:innen) plötzlich persönlich für informationssicherheitstechnische Belange haftbar machen. Inwiefern die DSGVO als europäische Erfolgsgeschichte gelten kann, ist daher fraglich – sie ist nicht nur in die Jahre gekommen (die erste Fassung geht auf 2012 zurück), sondern steht auch stellvertretend für zahlreiche Normtexte, die grundsätzliche Fragen weder adäquat abbilden noch praxisgerecht beantworten. Laut Prof. Forgó sind in Zukunft Normen gefragt, bei denen „nicht nur Jurist:innen gewinnen“ (da diese Regulatorien über Jahre interpretiert und ausjudiziert werden müssen), sondern die Innovationsbildung in Europa nachhaltig voranbringen. Dafür ist es auch nötig, weiterreichende Themen wie die zugrundeliegenden Werte sowie die Schaffung digitaler Kompetenzen – in Schulen und an Universitäten – zu diskutieren resp. zu ermöglichen.

In der folgenden Diskussion steuerten die Teilnehmenden Sichtweisen und Erfahrungswerte aus ihren Fachgebieten und beruflichen Hintergründen bei. Es wurde festgehalten, dass EU-Regulierungen eine starke Profilierungs-Komponente haben – eine Regulierung auf EU-Ebene zu verankern gilt als Erfolgskriterium für Institutionen und die sie leitenden Personen – was zu langen Entwicklungs- und Umsetzungsprozessen sowie enormen Detaillierungsgraden führt. In diesem komplexen Prozedere scheint das eigentliche Ziel einer Regulierung verloren zu gehen, und die operativen Bereiche (oft auf nationaler Ebene) stehen vor der schwierigen Aufgabe, solche Richtlinien in praktisch anwendbare Gesetze und Prozesse zu „übersetzen“. Diese Herausforderung trifft zusätzlich auf einen Ressourcenmangel auf den darunterliegenden operativen Ebenen, wo Zeit und Personal für

sinnstiftende Schritte in Sachen Informationssicherheit und Digitaler Souveränität oft nicht vorhanden sind. Folglich büßen an sich gut gemeinte Richtlinien – sh. DSGVO – am Ende an Wirksamkeit ein. Unschärfe bei Begriffsdefinitionen und lange Implementierungszeiträume führen weiters dazu, dass eine Regulierung mit der (technischen) Realität meist nicht Schritt hält – so löst der ursprünglich geographisch verankerte Begriff der Souveränität im Kontext digitaler Daten das Bild örtlich fixierter Datencenter aus, während heutzutage eigentlich die Frage nach der Hoheit über Datenströme zu beantworten wäre.

Der zweite Vortrag des Treffens, „Visuelles Gatekeeping vor und inmitten des Ukraine-Russland-Krieges" von Univ.-Prof. Dr. Andreas Eckhardt (Universität Innsbruck), widmete sich einem weiteren hochaktuellen Thema des Internetzeitalters: die Produktion und Verbreitung von News in Online-Netzwerken, in diesem Fall der Plattform Reddit. Am Beispiel des Subreddits r/Russia, dessen Inhalte aus dem Zeitraum 10.2. bis 10.4.2022 ausgewertet wurden, wird veranschaulicht, wie sich die „Berichterstattung" mit Kriegsbeginn Ende Februar 2022 wandelt – nicht nur die Inhalte wechseln von u.a. der Bewunderung Russlands und der Verspottung des Westens zu militärischen Themen und Bildmaterial aus dem Kriegsgebiet, sondern auch die Gruppe der Beitragenden ändert sich von einer Vielzahl an User:innen auf primär wenige Reddit-Moderator:innen (deren Identität nicht herauszufinden ist). Diese Fallstudie dient der Illustration eines größeren Phänomens, das mit Online-Plattformen entstanden ist: (visual) audience gatekeeping. Gatekeeper verwalten Informationen und deren Weitergabe; ursprünglich eine Funktion, die von Institutionen und Personen wie Zeitungen, öffentlichem Rundfunk und Journalist:innen wahrgenommen wurde, sind es in Zeiten von Online-Netzwerken die User:innen, die Inhalte produzieren und verbreiten. Im Hinblick auf Bilder und Videos wird dies besonders brisant, sagt doch ein Bild mehr als tausend Worte und ist leicht zu manipulieren und/oder in beliebigen Kontext zu setzen. Prof. Eckhardt und sein Team werteten unter Anwendung von Critical Visual Content Analysis über 2.000 visuelle Elemente aus mehr als 1.600 r/Russia-Posts aus, um ein theoretisches Modell zu „visual audience gatekeeping" zu entwickeln.[1] Im Kontext der Digitalen Souveränität ist die Frage visueller Inhalte – die immer seltener von zentralen Gatekeepern verwaltet und oft dennoch zur Beweisführung herangezogen werden – eine zentrale. Anknüpfend an Prof. Forgós Vortrag stellt sich auch hier einerseits die Frage nach Regulatorien, während es andererseits Bewusstseinsschaffung (u.a. durch digitale Grundbildung) brauchen wird, um den individuellen Nutzer:innen Souveränität im Umgang mit visuellen und anderen Inhalten zu ermöglichen.

In der Diskussion wurde thematisiert, inwieweit Regulatorien – zum Beispiel der europäische Digital Services Act (Juni 2022 noch nicht in Kraft) – die Digitale Souveränität individueller Nutzer:innen einschränken können; gleichzeitig wurde darauf aufmerksam gemacht, dass Online-Plattformen unter dem Privileg arbeiten, im Gegensatz zu natürlichen Personen oder traditionellen Medien nicht für die geposteten Inhalte haftbar zu sein (was ihre derzeitige Marktposition überhaupt erst ermöglicht hat). Es gab darüber hinaus großes Interesse an der präsentierten Fallstudie, z.B. den Kriterien für die Auswahl des Subreddits sowie den Zeitraum, für den die Daten erhoben wurden. Zwei weitere Datenquellen – ein Ukraine-Subreddit sowie einer zu EU-Themen – warten hierbei noch auf die Analyse, die ein äußerst aufwändiges Unterfangen ist, für das entsprechend zeitliche und personelle Ressourcen zur Verfügung stehen müssen. Es lässt sich aber jetzt schon sagen, dass die Dynamiken in den geposteten Inhalten im Subreddit r/Ukraine ähnlich zu r/Russia sind, nur sozusagen „gespiegelt". Nachdem Krieg ein extremes Ereignis ist, das sich entsprechend auf berichtete Inhalte auswirkt, stellte

[1] Publikation in Begutachtung, Juni 2022.

sich die Frage nach der Gültigkeit der Studienergebnisse für andere gesellschaftliche Themen. Prof. Eckhardt wies darauf hin, dass „Krieg anschauen“ nicht das Ziel gewesen sei (wie sich auch am Zeitraum der Datenerhebung ablesen lässt); nichtsdestotrotz lässt sich vermuten, dass überall dort ähnliche Dynamiken beobachtet werden können, wo es soziale Spannungen gibt. Die Überlegung, was man als Nutzer:in hier – abgesehen davon, offline zu gehen – tun kann, führte wie schon im Nachklang des ersten Vortrags zu einem Konsens darüber, dass Bewusstseinsbildung, digitale Grundbildung und ausreichend zeitliche und personelle Ressourcen nötig sind, um nicht erst im Anlassfall auf z.B. Kampagnen in Social Media zu reagieren.

Die beiden Vorträge mögen unterschiedliche Ecken unseres digitalen Zeitalters beleuchtet haben, lassen jedoch ein gemeinsames Fazit zu:

(1) Die Schaffung von Bewusstsein in allen Gesellschaftsgruppen ist eine Grundlage für Digitale Souveränität. Dazu wird es u.a. nötig sein, das vorhandene Wissen aus den „echo chambers“ der Universitäten, Fachhochschulen und Expertenrunden herauszuholen und der Öffentlichkeit zugänglich zu machen.

(2) Um Bewegung in die derzeit doch etwas verfahrene Situation aus technischer Entwicklung vs. komplexer, unpraktikabler Regulatorien vs. Souveränität der Nutzer:innen zu bringen, sollten drei Strategien kombiniert werden:
   - „Marsch durch die Institutionen“ und aktives Einbringen in politische Gremien
   - Gang auf die Straße, einschließlich zivilgesellschaftlicher Kampagnen auf YouTube
   - Aufbau von Bereitschaft für und Vertrauen in die Wissenschaft seitens der Politik, um hier in Zukunft gemeinsam an z.B. guten, d.h. tatsächlich wirksamen Richtlinien zu arbeiten

(3) Um obiges nachhaltig erreichen zu können, sind zwei Dinge von zentraler Bedeutung:
   - digitale Bildung, so früh wie möglich
   - interdisziplinäres Einflechten von IT und Digitalem an den Universitäten

   Beides sind hochkomplexe und weitreichende Unterfangen, für die – wie so oft – die Ressourcen und, im Falle der vielgewünschten und wenig gelebten Interdisziplinarität, das Know-how fehlen.

Der Weg zu einer umfassenden und nachhaltig in der Praxis implementierten Digitalen Souveränität ist wohl noch ein langer. Umso wichtiger ist es, via Fallstudien, Analysen und weiteren kleinen Schritten dieses Thema beharrlich zu verfolgen und präsent zu halten.

Weiterführende Links (YouTube)

Ars Boni spezial 268: Cyberwarfare: https://www.youtube.com/watch?app=desktop&v=n0AJdhIFOb8

Ars Boni 279: Überwachen, Blocken, Delisten – Zur Reichweite der EU-Sanktionen gegen RT und Sputnik: https://www.youtube.com/watch?app=desktop&v=oX7QwnFJse0

Ars Boni 297 Spezial: Der Digital Services Act aus österreichischer Perspektive: https://www.youtube.com/watch?app=desktop&v=cexHkW1b2VU