PRIVACY, DATA PROTECTION & SURVEILLANCE

XVIth INTERDISCIPLINARY WORKSHOP
12 DECEMBER 2023

PROGRAM

12:00 **Welcome and introduction round**

12:30 *Dennis Redeker (ZeMKI, Zentrum für Medien-, Kommunikations- und Informationsforschung, Universität Bremen), Sebastian Kuhnke (Universität Bremen)*
Social Media Privacy Concerns in the Majority World: A New Dataset

13:30 *Daniel Guagnin und Volkan Sayman (nexus Institut, Berlin)*
Sicher im Datenverkehr – Narrative zu gesellschaftlichen und sozialen Datenschutzrisiken

14:30 **Coffee break**

15:00 *Corbinian Ruckerbauer (Stiftung Neue Verantwortung, Berlin)*
Surveillance by the Bundeswehr – Without Legal Basis and Control

16:00 *Sakyi Mannah (Selbstregulierung Informationswirtschaft e.V.)*
Der Widerruf der Einwilligung im Kontext der Anonymisierung

17:00 **Conclusion and outlook**

17:15 **End**

Location:

Alexander von Humboldt Institute for Internet and Society
Französische Straße 9
10117 Berlin
Room »Kosmos«
https://www.openstreetmap.org/#map=19/52.51452/13.38679

Social Media Privacy Concerns in the Majority World: A New Dataset

Dennis Redeker (ZeMKI, Zentrum für Medien-, Kommunikations- und Informationsforschung, Universität Bremen), Sebastian Kuhnke (Universität Bremen)

Through legislation in the Global North, such as GDPR, and the ensuing 'Brussels effect' (Bradford), globalized digital privacy rules are geared to serve the preferences of users in richer countries. Comparative privacy research can provide an important impetus for privacy policy around the world, taking into account also voices from developing countries. The present research project aims to better understand social media privacy perceptions and concerns outside of the OECD world. For this we conducted a comparative survey study of social media users (Facebook and Instagram), collecting data from 14,179 respondents from 30 countries, primarily in the Global South and Eastern Europe. The nature of this survey allows us to ask the same questions to respondents around the world, rather than to piece together smaller studies to better understand attitudes in the majority world.

Research Framework

The current project aims to provide a strong empirical base for further research, analysis and normative discussion. It is hence more descriptive in nature, aiming at exploration rather than causal inference. Consequently, four main research questions are the following:

- How do digital technologies affect the exercise of privacy as a human right (UDHR, Art 12) (as compared to freedom of expression, freedom of information, equality before the law or the right to life, liberty and security of person)?
- How concerned are users that specific actors know things about them, based on what they post and what they do on social media platforms? Here we propose four different groups, including friends and family, employers and schools, the platforms themselves (and connected to them: advertising firms) and the users' respective government.
- How do users perceive privacy concerns in terms of magnitude, especially also in comparison with other concerns they have, such as concerns about hate speech, bullying or bots.
- How are these questions mediated by age, education and gender?

Research Methods

Data collection occurred between November 2022 and March 2023 as part of the Platform Governance Survey, conducted at the University of Bremen and funded by the Federal Office of Communications (OFCOM) of Switzerland and by the State of Bremen. Respondents were recruited using paid advertisements that appeared on two of Meta Inc.'s social media platforms: Facebook and Instagram. Ads allowed to quota sample respon-

dents reasonably well, applying quotas for gender and age, based on relevant census data from the study countries. The following countries have been included in the study: Algeria, Argentina, Belarus, Bolivia, Bosnia and Herzegovina, Brazil, Cameroon, Colombia, Croatia, Democratic Republic of Congo, Georgia, Ghana, Haiti, Hungary, Indonesia, Kenya, Madagascar, Mexico, Nicaragua, Nigeria, Paraguay, Philippines, Poland, Romania, Serbia, Switzerland, Tunisia, Turkey, Uruguay and Venezuela. Eleven additional countries were included in the full sample of the Platform Governance Survey but they performed comparatively worse terms of recruitment, leading to lower sample sizes.

Der Widerruf der Einwilligung im Kontext der Anonymisierung

Sakyi Mannah (Selbstregulierung Informationswirtschaft e.V.)

Aktuelle Umweltkatastrophen, Konflikte und sonstige Krisen zeigen, dass Unternehmen (insbesondere kleine und mittlere Unternehmen) immer häufiger wirtschaftlichen Herausforderungen in Krisensituationen ausgesetzt sind. Genau dieses Problem wird durch sog. Krisenresilienzplattformen wie z.B. Cognitive Economy Intelligence Plattform für die Resilienz wirtschaftlicher Ökosysteme (CoyPu) adressiert, wobei mittels KI-Methoden ganz und/oder auch teilautomatisiert große Mengen an personen- und nichtpersonenbezogenen Daten aus verschiedenen Datenquellen verarbeitet werden.

Die Verarbeitung personenbezogener Daten untersteht den Vorschriften der Datenschutzgrundverordnung (EU) 2016/679 (DSGVO), welche den Zweck des Schutzes natürlicher Personen bei der Verarbeitung ihrer Daten erstrebt. Besonders die Anonymisierung, welche bislang für Unternehmen eine attraktive Art der Verarbeitung von Daten darstellt, stellt eine Methode zur Erreichung dieses Schutzzweckes dar. Hierbei wird zum Schutz der betroffenen Person der Personenbezug der Daten durch den Datenverarbeiter derart aufgehoben, sodass eine einzelne Person anhand dieser Daten nicht mehr identifizierbar ist. Allerdings besteht nach wie vor weder Einigkeit darüber was unter einer „korrekten Anonymisierung" zu verstehen ist noch wie die Vorschriften und Anforderungen der Datenschutzgrundverordnung bei derartigen Anonymisierungen Anwendung finden.

Diese Forschungsarbeit befasst sich insbesondere mit den Anforderungen der Datenschutzgrundverordnung betreffend die Einwilligung nach Artikel 6 Absatz 1 Buchstabe a und dessen Widerruf im Rahmen einer Anonymisierung. Denn hierbei erscheint es auf den ersten Blick fraglich, ob die Vorschriften zum Widerrufsrecht auch auf bereits anonymisierte Daten Anwendung finden. Zwar wäre es naheliegend anzunehmen, dass der Widerruf bei anonymisierten Daten, mangels Identifizierbarkeit einzelner Personen, ausgeschlossen wäre. Denn ein ausdrücklicher Bezug der Verordnung wird gemäß Artikel 2 Absatz 2 Datenschutzgrundverordnung lediglich auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten und nicht auf nichtpersonenbezogene Daten genommen. Mit Blick auf die immer schneller wachsende und komplexer werdenden Sektor der Informationstechnologie wird jedoch deutlich, dass aufgrund des derzeitigen technischen Standes die Wahrscheinlichkeit einer Re-Identifizierung bei anonymen Daten nicht ganz ausgeschlossen werden könnte und ein Widerruf im Falle einer sog. faktischen Anonymisierung durchaus denkbar wäre. Ziel dieser Arbeit ist es mithin zu beantworten welche Anforderungen an die Einwilligung betreffend die Anonymisierung zu stellen sind. Dazu werden die folgenden Forschungsfragen aufgestellt: Ist der Widerruf der Einwilligung in eine Anonymisierung nach der Datenschutzgrundverordnung möglich? Und wenn nein, kann die Einwilligung nach Artikel 6 Absatz 1 Buchstabe a Daten-

schutzgrundverordnung überhaupt als Rechtsgrundlage für eine Anonymisierung herangezogen werden?

Um diese Forschungsfragen zu beantworten, wurden die einschlägigen Vorschriften der Verordnung und die dem zugrundeliegenden Erwägungsgründe auf ihren Wortlaut und ihrer systematischen Stellung untersucht. Betreffend die einschlägigen Vorschriften der Datenschutzgrundverordnung wurde spezifisch auf die Artikel 7, Artikel 2 und den Artikel 1 Bezug genommen.

Erste Erkenntnisse ergaben sich bereits bei der Betrachtung des Artikel 7 insbesondere des Absatzes 3. Demnach hat jede von der Datenverarbeitung betroffene Person das Recht ihre Einwilligung in die Datenverarbeitung zu widerrufen. Der herrschenden Ansicht nach stellt der Vorgang der Anonymisierung rechtlich gesehen ein „Verwenden" im Sinne einer Verarbeitung nach Artikel 4 Nummer 2 Datenschutzgrundverordnung dar, sodass diese auf eine Einwilligung entsprechend der Ermächtigungsgrundlage aus Artikel 6 Absatz 1 Buchstabe a Datenschutzgrundverordnung gestützt werden kann. Problematisch erscheint hierbei allerdings, dass im Kontext anonymer Daten der Widerruf durch den Betroffenen in der Regel erst dann erfolgt, wenn die Daten infolge der aufgrund der Einwilligung durchgeführten De-Identifizierungsmaßnahme keinen Personenbezug mehr aufweisen. Dies hätte zur Folge, dass der Artikel 7 Absatz 3 mangels Personenbezug oder „Betroffenheit der Person" keine Anwendung auf die bereits anonymisierten Daten findet und mithin auch kein Widerrufsrecht des Betroffenen besteht.

Dennoch ist diese Erkenntnis eher nicht befriedigender Natur. Zwar gibt sie auf dem ersten Blick beiden aufgestellten Forschungsfragen eine eindeutige Antwort, was eine weitere Untersuchung überflüssig machen würde. Allerdings lässt diese Ansicht vollkommen außer Betracht, dass bei einer Verarbeitung personenbezogener Daten entsprechend des in der Datenschutzgrundverordnung geltenden Verbotsprinzips mit Erlaubnisvorbehalt die Einwilligung nach Artikel 6 Absatz 1 Buchstabe a stets als Ermächtigungsgrundlage herangezogen werden kann. Dies hätte dann auch zur Folge, dass bereits im Vorfeld nie in einen Vorgang der Anonymisierung eingewilligt werden kann.

Auch der Wortlaut des Artikel 2 Datenschutzgrundverordnung könnte für ein Widerrufsrecht des Betroffenen bei bereits anonymisierten Daten sprechen. Ihrer systematischen Stellung nach regelt der Artikel 2 Absatz 1 den sachlichen Anwendungsbereich der Datenschutzgrundverordnung. Dar-über hinaus wird im Absatz 2 des Artikel 2 in einem abschließenden Katalog geregelt in welchen Fällen die Vorschriften der Datenschutzgrundverordnung keine Anwendung findet. Deutlich wird, dass der Vorgang der Anonymisierung im Absatz 2 nicht genannt ist. Dies und die Nennung der Anonymisierung in den Erwägungsgründen bieten Grund zur Annahme, dass Kenntnis von der Anonymisierung bei der Erstellung der Datenschutzgrundvorordnung bestand und dieser bewusst nicht vom Katalog des Artikel 2 Absatz 2 erfasst werden soll.

Anhand der bisherigen Erkenntnisse wird deutlich, dass eine eindeutige Beantwortung der Forschungsfragen zum jetzigen Zeitpunkt noch nicht möglich erscheint. Mithin bleibt es im Weiteren zu eruieren, ob und inwiefern einschlägige Vorschriften der Datenschutzgrundverordnung konkretisiert werden müssten, um so eine genauere Antwort auf die Forschungsfragen zu geben. An dieser Stelle empfiehlt es sich auch hervorzuheben, dass von zuständigen Datenschutzbehörden genehmigte Verhaltensregeln oder auch sogenannte Codes of Conduct gemäß Artikel 40 Datenschutzgrundverordnung ebenfalls zu einer weiteren Konkretisierung der Anwendung der Vorschriften zur Einwilligung und dem Widerruf der Einwilligung beitragen könnte. Das solche Verhaltensregeln für regulatorische Klarheit sorgen können zeigt von SCOPE Europe betreute EU Cloud Code of Conduct welcher entwickelt wurde, um die Anforderungen der Datenschutzgrundverordnung betreffend Cloud-Dienste abzudecken.

Surveillance by the Bundeswehr – Without Legal Basis and Control

Corbinian Ruckerbauer (Stiftung Neue Verantwortung)

The current government coalition in Germany according to its coalition agreement, aims to expand and strengthen the control of "all intelligence activities of the federal government" during the current legislative period. However, a central question remains entirely unanswered: To what activities precisely are the parties referring to, and who carries out those activities? Does this exclusively refer to the actions of the three federal intelligence services, namely, the Bundesnachrichtendienst (BND), the Bundesamt für Verfassungsschutz (BfV), and the Bundesamt für den Militärischen Abschirmdienst (BAMAD)? Or should, like in other democracies, the focus of the legal framework and oversight also be extended to intelligence activities of the federal government that are not conducted by the intelligence services themselves? A central example of the latter are the intelligence activities of the Bundeswehr.

The government has not yet made a firm decision on this issue, despite currently initiating far-reaching reforms. Initial proposals by the federal government for the further development of legal oversight have been internally debated (Flade, 2023; UK-Rat, 2023; Wetzling & Vieth-Ditlmann, 2023) and ultimately not included in the first reform of intelligence law (Federal Government, 2023b), which was introduced in the Bundestag in early October 2023 (Federal Government, 2023b; Federal Government, 2023c). In a second part of the reform, by 2024, "a value-consistent systematization of regulations for information acquisition should follow, and the intelligence law should be made future-proof as a whole" (Federal Government, 2023b). In our view, it is urgently necessary to consider the intelligence activities of the Bundeswehr in this process. If a reform of this growing part of state surveillance is neglected once again, the following deficits regarding the rule of law would continue to be accepted:

Lack of a legal framework: Unlike for intelligence services or law enforcement agencies, there is no sufficient legal basis for the collection and processing of data in the context of military intelligence. The Constitutional Court has clearly defined a series of requirements and procedures for the constitutional safeguarding and limitation of fundamental rights infringements within the framework of state surveillance. In the field of military intelligence, these requirements, if at all, are only implemented in internal regulations, stipulated by the Federal Ministry of Defense (BMVg) – not by the Parliament.

Inadequate oversight: Important guidelines and structures for effective independent control of government actions in this area are missing. To this day, there is no permanent parliamentary oversight, let alone an independent oversight body that is executing effective control of those intelligence activities in a way that is meeting the standards of the Constitutional Court. The only independent institution reviewing the intelligence ac-

tivities of the Bundeswehr, the Federal Commissioner for Data Protection and Freedom of Information (BfDI), is , at least as far as is publicly discernible, limited in effectiveness.

The federal government and its majority in the Bundestag would be ill-advised to exclude the surveillance activities of the Bundeswehr and its independent oversight from the planned reform in 2024. Based on several case examples, this study demonstrates that measures of military intelligence deeply interfere with fundamental rights and human rights. To ensure their legal and constitutional implementation and control, the Bundestag should urgently:

- Mandate the essential surveillance activities of military intelligence in a law, clearly indicating when these activities infringe on fundamental rights.
- Ensure that the entire spectrum of military intelligence is subject to continuous parliamentary oversight, and that activities relevant to fundamental rights are reviewed by independent oversight for their legality and necessity.

The federal government and the government majority in the Bundestag could develop a standalone Bundeswehr Act or a Military Intelligence Act (MilNWG) for this purpose. However, in order to consistently ensure the required standards for control and legal framework in state surveillance, our opinion is that a new and unified legal framework should be established for all intelligence activities of the federal government. This would align with the federal government's goal of regulating intelligence methods of information acquisition consistently. Crucially, this new legal foundation should clearly specify legitimate purposes, thresholds for interferences, authorization requirements and procedures, as well as redress mechanisms, also for military intelligence, to prevent disproportionate surveillance and address shortcomings.

Sicher im Datenverkehr – Narrative zu gesellschaftlichen und sozialen Datenschutzrisiken

Daniel Guagnin und Volkan Sayman (nexus Institut, Berlin)

Die stetige Verbesserung und Personalisierung kommerzieller Dienste im Internet – allen voran von Werbung – durch die Verarbeitung personenbezogener Daten bildet das technisch-ökonomische Rückgrat des heutigen Internets (Zuboff 2019). Jeden Tag hinterlassen wir über verschiedene Webseiten, Geräte und Internetbesuche hinweg Informationen über unsere alltäglichen Aktivitäten, sei es unser Kaufverhalten, unseren Musikgeschmack oder unsere Lesegewohnheiten. Die hierbei entstehenden Datenspuren repräsentieren gleichsam den Ausgangspunkt einer digitalen Wertschöpfungskette: Ein komplexes Netzwerk aus Datenverarbeitern nutzt eine Vielzahl von Technologien um sie zu speichern, hinsichtlich unserer möglichen Interessen und Vorlieben zu analysieren und gegebenenfalls weiter zu vermarkten (vgl. Roßnagel 2007). Teils werden hierfür Informationen über Verhalten, Interessen und Präferenzen vieler Nutzer:innen aggregiert und statistisch korreliert, teils mehr oder weniger detaillierte Einzelprofile gebildet, oftmals werden beide Maßnahmen miteinander kombiniert (Degeling 2016). Diese gezielte Sammlung und Verarbeitung persönlicher Daten ist trotz ihrer Alltäglichkeit für die Nutzer:innen von Online-Diensten weitgehend unsichtbar (Christl 2017).

Die EU-Datenschutzgrundverordnung (DSGVO) erkennt in den so beschriebenen Charakteristika von Komplexität, Alltäglichkeit und relativer Unsichtbarkeit zu Recht signifikante Risiken für die Garantie bürgerlicher Grundrechte. Sie reagiert darauf mit zahlreichen rechtlich bindenden Vorschriften für die Verarbeiter personenbezogener Daten, allen voran solche der Zweckbindung, Transparenz und Intervenierbarkeit (insbes. der Einwilligungserfordernis) von Datenerhebung und -verarbeitung.

Den Nutzer:innen begegnet im Online-Alltag gleichwohl zumeist eine formalistische, ritualisierte und materiell unzureichende Umsetzung der vorgenannten Datenschutzprinzipien: Das Cookie-Banner. Es klärt die Nutzer:innen weder wirksam darüber auf, was mit ihren Daten geschieht, noch bietet es ihnen eine wirksame Kontrolle über die mit der Datenverarbeitung verbundenen Risiken (Utz et al. 2019). Die defizitäre Übersetzung der DSGVO in ein niedrigschwelliges Interface hat drei wesentliche Gründe:

Erstens besteht ein eklatanter Mangel an alltagstauglichen Narrativen, entlang derer Nutzer:innen eventuelle Risiken für die Ausübung ihrer Grundrechte verbildlichen und so gedanklich durchdringen können (vgl. Gaycken 2011). Zweitens fehlen Metriken, Methoden und Verfahren, anhand derer die Umsetzung entsprechender Transparenz- und Kontrollmaßnahmen an den jeweiligen Benutzer:innenschnittstellen entwickelt, evaluiert, getestet und bestenfalls zertifiziert werden können (Jakobi et al. 2022). Hiermit fehlen drittens auch entsprechend entwickelte grafische Interfaces, die im Hinblick auf Risi-

koverständnis und -kontrolle aus Nutzer:innensicht funktionieren, d.h. gemäß der DSGVO wirksam sind.

Bestehende Methoden zur Messung und Ansätze zur Verbesserung von Lesbarkeit und Verständlichkeit zielen vor allem auf die Beschreibung der Datenverarbeitungspraktiken der Verantwortlichen (z.B. Bui et al. 2021) und der verwendeten personenbezogenen Daten (z. B. Bhatia, Breaux 2015), nicht aber auf die dabei betroffenen Grundrechte und -freiheiten oder auf die damit einhergehenden Risiken. Aufgrund dieses Mangels an Transparenz wird letztlich den Nutzer:innen selbst abverlangt, aus der Auflistung der verarbeiteten Daten und der Beschreibung der Datenverarbeitungszwecke und -praktiken auf die entsprechenden Grundrechtsrisiken zu schließen. Die Nutzer:innen ziehen diese Schlüsse jeweils anhand eigener Erfahrungen – etwa mit digitalen Technologien, medial thematisierten Schadensereignissen oder der eigenen Verwundbarkeit – sowie Vorstellungen bzw. mentalen Modellen der zu erwartenden Risiken.

Es gibt eine große Zahl an auch empirischen Arbeiten zu Privatheitsrisiken und deren subjektiven gedanklichen Repräsentationen (Kang et al. 2015), jedoch finden sich keine empirischen Untersuchungen über die spezifisch grundrechtsbezogenen Risikovorstellungen von Nutzer:innen – insbesondere in Bezug auf personalisierte Werbung und sonstige personalisierte Inhalte. Stattdessen sind die Vorstellungen von sowohl Nutzer:innen als auch Expert:innen (Friedewald et al. 2022) geprägt von den Privatsphäre- und Datenschutznarrativen, die in der öffentlichen wie der fachlichen Debatte dominieren und die sich durch drei wesentliche Charakteristika auszeichnen: Erstens kommt es in den Bereichen Datenschutz, Privacy und Surveillance zu einer Überbetonung von Problemen der individuellen Privatheit (Pohle 2022), während die genuin sozialen Risiken der Datenverarbeitung vernachlässigt werden (vgl. Viljoen 2021, 600f.). Zweitens ist die Debatte stark von negativ aufgeladenen Begriffen wie „Missbrauch", „Überwachung" oder „Angriff" geprägt. Schließlich sind drittens exzeptionalistische, also gerade nicht alltagstaugliche bzw. -relevante Risikovorstellungen weit verbreitet, etwa von Geheimdiensten oder „Hackern" als omnipotente Akteure oder dem chinesischen Sozialkreditsystem als Dystopie. Es fehlen somit Narrative, die anschlussfähig sind an juristische Diskurse zu Grundrechten und Grundrechtsrisiken, der Alltäglichkeit der Verarbeitung und den dabei entstehenden Risiken angemessen und zugleich alltagstauglich – die also keine übermäßigen Anforderungen an „digital literacy" bzw. „data literacy" stellen und trotzdem praktisch handhabbar bleiben.

Die Verständlichkeit von und Informierung über Risiken stellt hierbei eine wesentliche Grundlage für die Rechtmäßigkeit des „informed consent" der Nutzer:innen dar, nicht zuletzt, weil die Art der Darstellung einen signifikanten Einfluss auf deren Einwilligungsentscheidung hat. Während in der Literatur häufig von „Dark Patterns" und „Nudging" die Rede ist (Grafenstein et al. 2018), stellt sich hier aus soziologischer Betrachtung zunächst die Frage der generellen Handlungsbeeinflussung über die Bereitstellung von In-

formation und erst darauffolgend die Frage nach Sanktionierung bzw. Verunmöglichung bestimmter Verhaltensweisen (Gläser et al. 2018). Doch während zu den Auswirkungen von Zweckspezifizierungen auf die Einwilligungshandlungen und die Wahrnehmung von Betroffenenrechten (Grafenstein et al. in review) oder von Android-Berechtigungsdialogen auf die Gewährung derselben (Smith, Muszynska 2019) bereits Vorarbeiten bestehen, bedarf es dringend weitergehender Forschung zu den Auswirkungen des jeweiligen Designs auf die Verständlichkeit von Datenschutzrisiken und dafür geeigneter Wirksamkeitsmetriken sowie Nachweismethoden.

Basierend auf den empirisch zu erhebenden Grundrechtsrisiken, wie sie sich aus verschiedenen Perspektiven darstellen, gilt es, Risikonarrative zu entwickeln, die nicht nur die individuellen, sondern auch die gesellschaftlichen Risiken veranschaulichen können.