Systematische und schwerwiegende Überwachung und Privatheit: Ein Kommentar aus datenwissenschaftlicher Sicht

Delphine Reinhardt

Die zentrale Frage des Symposiums bezieht sich auf einen möglichen Bedarf an einem Strafrecht gegen schwerwiegende systematische Datenschutzverletzungen durch Staat und Wirtschaft. Schon bei der Betrachtung der Adjektive „schwerwiegende" und „systematische" bei Datenschutzverletzungen entstehen weitere Fragen, die sich zurzeit schwierig beantworten lassen. Im Folgenden werden diese Fragen einzeln erläutert und mögliche Antworten skizziert, die dennoch nicht als Endlösungen betrachtet werden sollten. Im Gegenteil sollten sie als Grundlage für weitere Diskussionen dienen.

Die erste Frage, die sich stellt, ist, wann eine „systematische Überwachung" anfängt. Das Thema des Symposiums ist um die „Überwachung" durch den Staat und Unternehmen artikuliert. Mit der Benutzung des Begriffs „Überwachung" könnte man jedoch schnell tendieren, sich auf staatliche Akteure zu fokussieren, da diese in den meisten Fällen in Verbindung gebracht werden. Solcher voreilige Fokus könnte jedoch gefährlich sein, da „Überwachung" im Sinne von „Beobachtungen" sich nicht nur auf staatliche Akteure beschränken. Betrachtet man dabei besonders die „Systematik" der Überwachung als eine methodische Vorgehensweise statt durch ein politisches System, werden nicht nur z.B. kriminelle Aktivitäten und deren Täter als Ziel dieser Überwachung, sondern auch jeder Bürger*in. Diese flächendeckende Überwachung fängt zum Beispiel bei unseren täglichen (wenn nicht minutenweisen) Interaktionen mit herkömmlichen Geräten wie Handys, Tablets oder Computern an. Dabei kann unser Verhalten überwacht werden: Welche Webseiten wir besuchen, wann, wie lange und in welcher Reihenfolge, welche Klicks wir betätigen, wie wir unsere Maus bewegen. Diese flächendeckende und damit systematische Überwachung hört jedoch nicht auf, wenn wir etwa unsere Laptops zu klappen oder unsere Handys zur Seite legen. Daten über uns werden stätig durch neue intelligente Geräte wie smarte Uhren, smarte Lautsprecher oder vernetzte Geräte, die zur Realisierung der Vision von Smart Homes und zukünftigen

Smart Cities beitragen, gesammelt. Damit können mögliche Schlussfolgerungen ohne unsere Kenntnisse gezogen werden. Zum Beispiel können Stimmungen und Emotionen sowie sozio-wirtschaftlicher Status durch die Analyse von Sprachbefehlen an smarten Lautsprechern erkannt werden.[1] Basierend auf Sensordaten, die durch Handys und smart Uhren, getragen von Fahrradfahrer*innen, gesammelt werden, konnten wir in einer unserer jüngsten Arbeiten zeigen,[2] dass die Art des Fahrrads, der Gang, die Höhe des Sattels sowie die Art des Geländes erkannt werden können. Diese gesammelten sensor-basierten Informationen betreffen nicht nur die Hauptnutzer*innen, das heißt die Personen, die das Gerät angeschafft und hauptsächlich nutzen, sondern auch deren Umfeld inklusive Drittpersonen, die z.B. zum Besuch sind. Ohne den Einsatz dedizierter Schutzmechanismen ist eine „systematische Überwachung" im Sinne der Beobachtung deswegen schon Teil unseres Alltags.

In diesem Kontext stellt sich die weitere Frage, in welchen Fällen solcher Überwachung es sich um eine „schwerwiegende" Verletzung der Privatheit handelt. Diese Frage zu beantworten ist wegen verschiedener Faktoren besonders schwierig. Einerseits ist es bekannt, dass menschliche Privatheitseinstellungen individuell und komplex abzubilden sind (auch für die Individuen selbst). Die Personen müssen oft Verletzungen ihrer Privatheit gegen andere mögliche Vorteile wie Komfort durch Personalisierung, physische Sicherheit durch Überwachung gesundheitlicher Werte mittels z.B. smart Uhren, oder weitere Einbindung in deren sozialen Kreisen durch Sofortnachrichtendienste abwägen. Ihre Entscheidungen sind dabei bekanntermaßen abhängig von dem Kontext,[3] das heißt, z.B. wer sammelt die Daten für welchen Zweck und in welchem Umfang, sowie der Hintergründe der Person selbst (Gender, Alter, Kultur, Vorerfahrungen, technische Kenntnisse usw.). Durch diese Individualität und Komplexität erscheint es schwierig, eine gemeinsame Antwort für eine Gesellschaft zu skizzieren. Außerdem decken die verschiedenen existierenden Definitionen der Privatheit verschiedenen Dimension, die über die informationelle Selbstbestimmung

1 *Hernández Acosta/Reinhardt*, A Survey on Privacy Issues and Solutions for Voice-controlled Digital Assistants. Pervasive and Mobile Computing (PMC), 2022.

2 *Hernández Acosta/Rahe/Reinhardt*, Does Cycling Reveal Insights about You? Investigation of User and Environmental Characteristics during Cycling. Proceedings of the 19th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous), 2022.

3 *Nissenbaum*, Privacy as Contextual Integrity, Washington Law Review 79 (2004). S. 119 ff.

hinaus gehen. Beispielsweise spielen soziale sowie physische Privatheit eine Rolle. Ein Vergleich dieser verschiedenen Facetten im Sinne einer Priorisierung ist dennoch nach bestem Wissen und Gewissen nicht bekannt und gestaltet sich auch zukünftig als schwierig. Auch ein Blick in die technischeren Fächer bietet keine richtige Hilfestellung. Bei den Untersuchungen möglicher Angriffe auf die Anonymität der Betroffenen, der Entdeckung neuer Schlussfolgerungen über sie oder der Evaluierung der Performanz neuer Schutzmechanismen werden keine einheitlichen Metriken eingesetzt. Ein direkter Vergleich wird dann genauso problematisch. Deshalb erscheint es auch hier zurzeit schwierig, basierend auf diesen Beobachtungen eine gültige Quantifizierung der schwerwiegenden Grade vorzunehmen. Ein Ansatzpunkt, der schon in der Datenschutzgrundverordnung beinhaltet ist, bezieht sich auf die Natur der gesammelten Daten. Dennoch können in dem Kontext einer systematischen Überwachung weitere Kriterien eine Rolle spielen wie (1) die Anzahl der betroffenen Personen, (2) ob und wie die Opfer ausgewählt wurden sind im Sinne einer möglichen Diskriminierung und (3) die Möglichkeit, mit den gesammelten Daten weitere Informationen abzuleiten oder vorherzusehen. Eine Abschätzung Letzteres, ohne zu wissen, ob weitere Daten mitgesammelt wurden oder zur Verfügung stehen, ist besonders herausfordernd. Außerdem können Daten, die vielleicht heute als harmlos erscheinen, später möglicherweise durch technologische oder methodische Entwicklungen gravierende Informationen über die Bevölkerung ableiten lassen. In anderen Worten: wie kann diese zeitliche Komponente sinnvoll berücksichtigt werden?

Auch wenn für die obengenannten Fragen noch keine definitiven Antworten in diesem Rahmen gefunden wurden, sollte dennoch handeln werden. Die Einführung der DSGVO hat zwar zu einer theoretischen Verstärkung der individuellen Rechte geführt. Dennoch erscheint oft schon eine sogenannte „Privatheitsmüdigkeit" in der Praxis, die wir in unseren Benutzerstudien sowie Interaktionen mit einem breiteren Publikum beobachten können. Dabei kann sich der Schutz der eigenen Privatsphäre als eine sinnlose und aussichtslose Aufgabe anfühlen. Diese Wahrnehmung sollte jedoch nicht kritisiert werden, da sie mit vielen Lösungen konfrontiert werden, die nicht dediziert für die Nutzer*innen konzipiert worden sind, aber um trotzdem so viel Daten wie möglich zu sammeln. In der Praxis wird dennoch wenig getan, damit sich die Lage ändert, trotz einer Steigerung

der Bußgelder.[4] Ausnahmen sind z.B. die Aktion der CNIL wegen den Dark Patterns von Facebook und Google in Frankreich.[5] Eine Wirkung ist dennoch heutzutage noch nicht sichtbar. Mehr eigene Verantwortung an die Bevölkerung zu übertragen, besonders ohne nutzer-orientierte Lösungen zu implementieren und zu fördern, scheint ausweglos. Wie am Anfang dieses Beitrags schon erwähnt, können Entscheidungen mit Bezug auf die Privatheit komplex für die Benutzer*innen sein. Um diese Komplexität zu reduzieren, wird der Einsatz von Assistenten in der Forschung zurzeit verfolgt. Dabei werden verschiedene Ansätze untersucht, die auf Ähnlichkeiten mit anderem Benutzer*innen, Crowdsourcing, Expertenmeinungen oder basierend auf eigenen Daten setzen. Zum Beispiel haben wir in unserem DFG Projekt „Personalisierung von Datenschutzeinstellungen basierend auf der dynamischen Analyse von Inhalten und zwischenmenschlichen Beziehungen“[6] untersucht, ob es möglich ist, basierend auf schon vorhandenen Daten auf den Geräten der Nutzer*innen, zu helfen, das Teilen von möglichen sensitiven Informationen mit ihren sozialen Kreisen besser zu kontrollieren, um Privatheitsverletzungen zu verhindern. Bei der Entwicklung solcher Lösungen muss dennoch sichergestellt werden, dass diese keine zusätzliche Gefährdungen für die Privatheit der Nutzer*innen einführt. In der Tat ist deren Ziel, sich von der Überwachung zu entziehen und nicht zur weiteren Überwachung führen. Darüber hinaus adoptieren oft die durchgeführten Studien mit Bürger*innen, die entwickelten technischen Lösungen für sie, sowie die zurzeit verfügbare Gesetzgebung eine individuelle Perspektive ohne eine gemeinsame und gesellschaftliche Betrachtung.[7] Durch den resultierenden Individualismus lauert dennoch die Gefahr, dass die gemeinsame Erosion unserer Privatheit weiter voranschreitet. Wenn die einzelnen Nutzer*innen sich selbst nicht gegenüber Wirtschaft und Staat schützen können und Wirtschaft und Staat wenig Interesse daran haben, wer sonst sollte dann die Verantwortung übernehmen?

4 S. den Beitrag von *Dominik Brodowski*, in diesem Band, S. 70 ff.
5 S. www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance.
6 S. https://gepris.dfg.de/gepris/projekt/317687129.
7 S. den Beitrag von *Sebastian Golla* in diesem Band.