Datenschutz gegen digitalen Autoritarismus

VB verfassungsblog.de/datenschutz-gegen-digitalen-autoritarismus/

Paul Friedl

Louis Rolfes

21 August 2024

Die Datenmacht des Staates stellt für Bürger*innen und ihre Rechte im heutigen Zeitalter eine zentrale Gefahr dar. Unabhängige Datenschutzbehörden sollen Missbräuche dieser Datenmacht verhindern. Autoritäre Kräfte, die nach den anstehenden Landtagswahlen auch in deutschen Landesregierungen beteiligt sein könnten, könnten allerdings versuchen, diese Kontrolle zu neutralisieren. Welche Risiken drohen und wie diesen entgegnet werden kann, behandelt der folgende Beitrag.

Staatliche Datenmacht und digitaler Autoritarismus

Um zu veranschaulichen, welche Gefahren von der Datenmacht des Staates ausgehen, bedarf es keines Blickes in literarische Dystopien; Beispiele staatlichen Datenmissbrauchs traten in den letzten Jahren und Jahrzehnten auch in real-existierenden (europäischen) Gesellschaften im Überfluss auf. In Deutschland ist hier insbesondere an die nicht enden wollende Serie an Missbräuchen von Datenbanken durch Polizei- und Sicherheitsbehörden zu denken. In Mecklenburg-Vorpommern etwa haben Polizeibeamte nachweislich mehrmals Polizeidatenbanken missbraucht, um rechtswidrig Minderjährige zu kontaktieren; teils kam es dabei auch zu sexuellen Belästigungen. Ebenfalls in Mecklenburg-Vorpommern soll die neonazistische Gruppierung „Nordkreuz“ mithilfe polizeilicher Dienstcomputer Listen mit rund 25.000

Namen und Daten politischer Gegner*innen erstellt haben. Seit 2018 wurden außerdem dutzende, mehrheitlich migrantisierte Personen durch Mails des sogenannten „NSU 2.0“ bedroht; oftmals wurden ihre Personendaten kurz zuvor von (teils nachweislich rechtsextremen) Polizeibeamten abgefragt. Die schiere Masse derartiger Fälle weist darauf hin, dass rechtswidrige polizeiliche Datenabfragen ein Alltagsphänomen darstellen, das nur ob der bestehenden strukturellen Intransparenz größtenteils unentdeckt bleibt.

Nicht nur polizeiliche Informationssysteme bergen Missbrauchspotenzial. Spätestens seit den Enthüllungen zur Spyware „Pegasus“ ist bekannt, dass auch in Europa Überwachungssoftware gezielt zur Ausspähung, Repression und Verleumdung regierungskritischer Stimmen eingesetzt wurde und wird. In Ungarn wurde *Pegasus* beispielsweise zur Überwachung hunderter Journalist*innen, Menschenrechtsaktivist*innen und oppositioneller Politiker*innen eingesetzt. Auch in Polen wurden im Rahmen der autoritären Wende hunderte Oppositionelle – vorgeblich ausnahmslos nach richterlicher Autorisierung – mit *Pegasus* überwacht. Ausspionierte private Nachrichten wurden anschließend im Staatsfernsehen veröffentlicht. Spanien und Griechenland haben *Pegasus* ebenfalls eingesetzt und auch das BKA und der BND haben die mächtige Überwachungssoftware erworben. Zu der Frage, ob weitere deutsche Nachrichtendienste oder Sicherheitsbehörden *Pegasus* verwenden, schweigt sich die Bundesregierung weiter aus. Der Fall *Pegasus*veranschaulicht auch die Rolle privatwirtschaftlicher Unternehmen bei der Einrichtung staatlicher Überwachungssysteme.

Neben den Gefahren, die durch schwer kontrollierbare Überwachungs-Tools drohen, können Staaten ihre Datenmacht aber auch in anderen Bereichen ausspielen. Insbesondere autoritäre Regierungen nutzen ihren staatlichen Informationsvorteil teilweise auch gezielt zur Festigung der eigenen Herrschaft. Nachweislich hat etwa Viktor Orbáns *Fidesz*-Partei Daten, die ungarische Bürger*innen dem Staat für Covid-Impfungen und Steuervergünstigungen bereitgestellt hatten, genutzt, um gezielte Wahlwerbung zu schalten. Ganz grundsätzlich lässt sich konstatieren, dass es zum Standardrepertoire autoritärer Regierungen gehört, über Eingriffe in die Privatsphäre ihrer Bürger*innen Räume privater Freiheit auszutrocknen. Bereits marginalisierte und vulnerabilisierte Gruppen, etwa Flüchtlinge (durch GPS-Tracking), sexuelle Minderheiten(durch erzwungene Outings) oder armutsbetroffene Menschen (durch Überwachung im Sozialwesen), geraten hier oft zuerst ins Visier. Unter dem Begriff des digitalen Autoritarismus (*digital authoritarianism*) werden diese Strategien seit einiger Zeit verstärkt auch akademisch aufgearbeitet.

Unabhängiger Datenschutz gegen den digitalen Autoritarismus

Es ist Grund- und Gründungseinsicht des Datenschutzrechts, dass die Datenmacht des Staates rechtlich eingehegt werden muss. Insofern fungiert das Datenschutzrecht als Garantie digital mediatisierter Freiheitsrechte und der Beschränkung informationeller staatlicher Herrschaft. Zentral für diese Garantie ist jedenfalls nach der Vorstellung des

europäischen Datenschutzrechts, dass *unabhängige* Aufsichtsbehörden (sog. Data Protection Authorities; DPAs) die Einhaltung des Datenschutzrechts überwachen. Diese sogar unionsverfassungsrechtlich verbürgte Unabhängigkeit der DPAs soll sicherstellen, dass die Kontrollstellen bei der Überwachung und Durchsetzung des Datenschutzrechts keiner politisch-opportunistischen Einflussnahme ausgesetzt werden und dadurch ihre Kontrollfunktion insbesondere auch der Exekutive gegenüber effektiv ausüben können. Die Notwendigkeit einer politisch unabhängigen Datenschutzaufsicht veranschaulicht etwa der Fall des baden-württembergischen Datenschutzbeauftragten, der es der Stadt Tübingen nach einer öffentlichen Auseinandersetzung mit dem Oberbürgermeister Palmer verbot, aus Polizeidaten eine Liste angeblich "auffälliger Asylbewerber" zu kompilieren und diese anderen Behörden zur Verfügung zu stellen.

Das Vorgehen der ungarischen Aufsichtsbehörde, die im Anschluss an die *Pegasus*-Veröffentlichungen nicht nur zu dem zweifelhaften Ergebnis kam, dass sicherheitspolitische Gesichtspunkte die Überwachungsmaßnahmen ausnahmslos rechtfertigen konnten, sondern zudem auch ein Verfahren gegen das die Missstände aufdeckende Medienportal einleitete, veranschaulicht hingegen, welche Folgen es haben kann, wenn DPAs ihre Unabhängigkeit verlieren und als Kontrollinstanz ausfallen.

(Soll-?)Bruchstellen der Unabhängigkeit: *threat modelling* für die Datenschutzaufsicht

Das wirft die Frage auf, ob und wie autoritäre Kräfte, etwa eine rechtsautoritäre Regierung in Thüringen, die Unabhängigkeit der Datenschutzaufsicht unterminieren könnten. Insoweit sind verschiedene Manöver denkbar, derer sich eine repressive Regierung bedienen könnte, um die unabhängige Datenschutzaufsicht zu neutralisieren.

Eine erste offene Flanke stellen die Möglichkeiten zur Absetzung des*der Datenschutzbeauftragten dar. Eine autoritäre Thüringer Landesregierung könnte den Versuch unternehmen, eine*n unliebsame*n Beauftragte*n vorzeitig abzusetzen. Die Entscheidung hierüber liegt jedenfalls in Thüringen in der Verantwortung des*der Landtagspräsident*in – ein Amt, das etwa in Thüringen sogar ohne Regierungsbeteiligung in autoritäre Hände fallen könnte. Nach Art. 53 Abs. 4 DSGVO, § 3 Abs. 8 S. 2 ThürDS setzt dies voraus, dass der*die Beauftragte eine schwere Verfehlung begangen hat oder aber die Voraussetzungen für die Wahrnehmung seiner*ihrer Aufgaben nicht mehr erfüllt. Objektiv handelt es sich hierbei um strenge Anforderungen. Es ist aber denkbar, dass ein solcher Grund vorgeschoben wird, um eine vorzeitige Neubesetzung zu erzwingen. Problematisch ist hier insbesondere, dass die DSGVO nicht vorsieht, dass über eine solche Enthebung gerichtlich entschieden werden kann oder muss; eine entsprechende Regelung im DSGVO-Kommissionsentwurf wurde im Laufe des Gesetzgebungsverfahrens gestrichen.

Auch das Verfahren zur Besetzung des*der Datenschutzbeauftragten bietet Potenzial für Missbrauch. Um die persönliche Unabhängigkeit des*der Beauftragten abzusichern, sieht Art. 53 Abs. 1 DSGVO vor, dass die Datenschutzbeauftragten in einem „transparenten" Auswahlverfahren ernannt werden. In der politischen Praxis sind diese Auswahlverfahren

– jedenfalls in Deutschland – jedoch für gewöhnlich alles andere als transparent: Vielmehr einigt sich in der Regel die Regierung oder eine an ihr beteiligte Fraktion im Hinterzimmer auf eine*n Kandidat*in und schlägt diese*n dem Landtag vor, der sie*ihn mit der absoluten Mehrheit seiner gesetzlichen Mitglieder wählt. Ein offenes Bewerbungsverfahren findet nicht statt. Ist die parteiische Auswahl der eigenen Kandidat*in aber schon heute der Normalfall, müsste auch eine autoritäre Thüringer Landesregierung keinen argumentativen Mehraufwand betreiben, um eine*n linientreue*n eigene*n Kandidat*in ins Amt zu heben, der*dem mehr an politischem Einfluss denn an der Durchsetzung des geltenden Rechts liegt.

Schließlich sind auch Angriffe auf die budgetäre Unabhängigkeit des*der Thüringer Landesbeauftragten für Datenschutz denkbar. Artikel 52 Abs. 4 DSGVO, § 4 Abs. 6 ThürDSG garantieren zwar, dass der Datenschutzaufsicht ausreichende personelle, technische und finanzielle Ressourcen bereitgestellt werden müssen. Mit einer Mehrheit im Landtag hätte eine autoritäre Landesregierung allerdings die Möglichkeit, dem*der Landesbeauftragten finanzielle und personelle Ressourcen vorzuenthalten und dadurch dessen Arbeit zu erschweren oder sogar praktisch zum Erliegen zu bringen – ganz ohne (ohnehin schwer vorstellbarer) formeller Auflösung des Amtes. Da die Arbeit der Datenschutzaufsicht im Ganzen recht ressourcenintensiv ist, könnten substanzielle Kürzungen das Arbeitsvermögen der Aufsicht in allen Bereichen kritisch mindern.

Resilienz des Datenschutzes stärken

Die eben diskutierten Szenarien verdeutlichen, dass reflektiert werden muss, ob und wie der Gesetzgeber den Bestand und die Arbeits- und Durchsetzungsfähigkeit der Datenschutzaufsicht institutionell besser absichern könnte.

Zunächst scheint hier dringend geboten, transparente Verfahren zur Ernennung der DPAs zu schaffen, um die Datenschutzaufsicht stärker vor politischer Einflussnahme zu schützen. Neben einer öffentlichen Stellenausschreibung wäre zumindest auch eine öffentliche Anhörung der Bewerber*innen im Vorfeld der Auswahlentscheidung erforderlich.

Gesetzt, dass auch unter einer autoritären Regierung eine unabhängige Datenschutzaufsicht fortbesteht, sollte weiter gerade im Bereich der Polizei- und Sicherheitsbehörden über eine Stärkung der Durchsetzungsbefugnisse der Datenschutzaufsicht nachgedacht werden. Derzeit steht vielen Datenschutzaufsichten gegenüber Polizei- und Verfassungsschutzbehörden als „schärfstes Schwert“ nur ein Beanstandungsrecht zu (bspw. § 7 Abs. 6 ThürDSG). Rechtsverbindliche Anordnungen können sie diesen Behörden gegenüber oftmals nicht treffen. Dies ist nicht zuletzt europarechtlich problematisch, da Art. 47 Abs. 2 JI-RL eine Ausstattung der behördlichen Datenschutzbeauftragten mit „wirksamen Rechtsbehelfen“ fordert, und sollte deswegen überdacht werden. Ähnlich steht es mit den vielen Ausnahmeregelungen, nach denen Datenschutzbeauftragte staatliche Behörden nicht mit Bußgeldern sanktionieren dürfen und auch keine sofortige Vollziehbarkeit von Maßnahmen anordnen dürfen. Der Umstand, dass sich der Datenschutzbeauftragte des Bundes kürzlich sogar gezwungen

sah, Klage gegen den Bundesnachrichtendienst zu erheben, da dieser der Kontrollstelle trotz Beanstandung wiederholt die ihr zustehende Akteneinsicht verwehrt hatte, zeigt, dass es sich bei diesen Problemen nicht um Fantasiegebilde handelt.

Neben einer stärkeren institutionellen Absicherung der Datenschutzaufsicht gibt es freilich eine Vielzahl möglicher materiell-rechtlicher Anpassungen, die gefährliche Datennutzungbefugnisse des Staates einhegen könnten bzw. müssten. Besonders Datenbestände, die bereits vulnerabilisierte Gruppen betreffen, etwa das Ausländerzentralregister, sollten hier in den Blick genommen werden. In Bezug auf das Ausländerzentralregister kommt etwa in Betracht, die Zugriffsmöglichkeiten von Polizei und Geheimdiensten einzuschränken oder das Register weitgehend abzuschaffen. Auch der Tendenz, den Polizeibehörden immer weitgehendere Überwachungsbefugnisse einzuräumen, muss entgegengewirkt werden. Das Verfassungsrecht wird hier weiterhin ein wichtiges Korrektiv bleiben. Schließlich sollten rechtliche Instrumente ausgeschöpft bzw. geschaffen werden, um die Produktion und den Handel von übermäßig eingriffsintensiver Überwachungssoftware stärker einzuschränken.

Insgesamt wird der Bedeutung der DPAs als unabhängige Kontrollinstanzen gegen die Datenmacht autoritärer Regime sowohl in der wissenschaftlichen als auch in der öffentlichen Debatte zu wenig Beachtung geschenkt. DPAs müssen besser gegen potenzielle Angriffe durch autoritäre Regime geschützt werden und das Datenschutzrecht schon jetzt fortentwickelt werden, um einen späteren Missbrauch der staatlichen Überwachungsinstrumente durch autoritäre Regime zu verhindern. Insbesondere bedarf es geeigneter rechtlicher Vorkehrungen zum Schutz vulnerabilisierte Gruppen, die nicht nur unter autoritären Regimen besonders stark von den Missbrauchspotenzialen staatlicher Datenmacht gefährdet sind.

- 

EXPORT METADATA
Marc21 XMLMODSDublin CoreOAI PMH 2.0
SUGGESTED CITATION Friedl, Paul; Rolfes, Louis: *Datenschutz gegen digitalen Autoritarismus, VerfBlog,* 2024/8/21, https://verfassungsblog.de/datenschutz-gegen-digitalen-autoritarismus/, DOI: 10.59704/e57030caf5e9fbe9.