Stellungnahme zum Ministerialentwurf 326/ME betreffend Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden

der Fachschaft Informatik der TU Wien im Sinne des HSG § 20 Abs. 4
21. August 2017

Obwohl sich Europa in der nachweislich längsten friedlichen bzw. kriegsfreien Ära seiner Geschichte befindet [1], versuchen politische Gruppierungen und Strömungen seit Jahren, die Bevölkerung immer stärker zu überwachen. Anstatt Ursachen für (kriminelles) Verhalten zu beseitigen - etwa Armut als Ursache für Beschaffungskriminalität, Gesetzeslücken als Ursachen für Steuerhinterziehung, soziale und ökonomische Unsicherheit als Ursache für Radikalisierung - werden überzogene Sicherheits- und Überwachungsinstrumente implementiert.

Resultat sind Gewöhnungseffekte, Selbstzensur, und Umgehungsverhalten. Der französische Philosoph Michel Foucault hat dafür den Begriff „Panoptismus“ geprägt: Unabhängig davon, ob eine Überwachung tatsächlich stattfindet, diszipliniert sich das womöglich unter Beobachtung stehende Individuum selbst. Es passt sein Verhalten an die gestellten normativen Erwartungen an. Hält der Zustand über einen längeren Zeitraum an, führt dieser Mechanismus zu einer Verinnerlichung der Normen. Aus einem (für den_die Normaufsteller_in) kostenintensiven Fremdzwang wird ein kostengünstiger Selbstzwang (Selbstdisziplinierung).[2]

Insgesamt sind uns bei der Durchsicht der Unterlagen - Gesetzesentwurf, Textgegenüberstellung, Vorblatt Folgenabschätzung sowie Erläuterungen - einige problematische Stellen aufgefallen. Es gibt undefinierte Begriffe (Accessprovider vs. Serviceprovider; Zugangsdaten), nicht messbare und somit nicht umsetzbare Zielsetzungen (Stärkung des Sicherheitsgefühls)[3], und sogar eindeutige Widersprüche (Mindestspeicherdauer - in der Erläuterung, aber nicht im Entwurf - vs. zwei Wochen nicht überschreitende Aufbewahrungsverpflichtung für Videoaufzeichnungen).

Empfehlung: Aufgrund massiver Bedenken datenschutzrechtlicher, gesellschaftlicher, menschenrechtlicher, ethischer sowie technischer Natur empfehlen wir das komplette Verwerfen des vorliegenden Entwurfs. Zielsetzungen, die dermaßen vage formuliert und unmessbar sind wie im Regierungsprogramm, das an mehreren Stellen in den Unterlagen zitiert wird, haben im Pflichtenheft einer Regierung bzw. eines Projektes mit solchen Ausmaßen und Auswirkungen nichts verloren.

Außerdem empfehlen wir den für den Entwurf verantwortlichen Personen die Lektüre von Cory Doctorow's „Little Brother“ im Speziellen sowie seine Arbeit im Allgemeinen. Der Autor macht seine Werke selbst auf seiner Website [4](kostenlos bzw. gegen Spende) zugänglich.

Sicherheits-Foren, SPG § 56

Mit Einführung der „Sicherheits-Foren“ werden willkürlich ausgewählte Bürger_innen (Sicherheitspartner_innen) mit bisher der Exekutive vorbehaltenen Kompetenzen ausgestattet.

Es ist unbekannt, wie die Sicherheitspartner_innen ausgewählt werden, es ist kein Mechanismus angeführt, der die Arbeit der Sicherheitspartner_innen kontrolliert. Es sind keine Konsequenzen bei Fehlverhalten oder Möglichkeiten zum Rücktritt von bzw. Verlust der Position als Sicherheitspartner_in im Entwurf zu finden.

Eine Kontrolle der Auswahl der Sicherheitspartner_innen ist dringend notwendig, um homosoziale Kooptation (siehe z.B. [5]) und damit Diskriminierung von nicht einbezogenen Gruppen zu verhindern. Dies ist insbesondere zum Schutz von religiösen und ethnischen Minderheiten sowie anderen Angehörigen marginalisierter Gruppen als auch Mitgliedern von politischen Organisationen, Gewerkschaften etc. dringend notwendig.

Bereits jetzt gibt es regelmäßig Fälle von Polizist_innen, die den ihnen anvertrauten Zugang zu sensiblen Daten missbräuchlich nutzen - und das, obwohl sie von Kontrollmechanismen und angedrohten Konsequenzen wissen [6].

Zweckmäßigkeit und Verhältnismäßigkeit der Weitergabe von teilweise hoch sensiblen Daten an Sicherheitspartner_innen unterliegen keiner unabhängigen Kontrolle. Betroffene werden nicht über die Weitergabe ihrer Daten informiert. Die §§ 8 und 9 DSG 2000 [7] werden komplett außer Kraft gesetzt, es sind keine Sanktionen für eine Verletzung der Verschwiegenheit durch Sicherheitspartner_innen vorgesehen.

Empfehlung: Diese Maßnahme ist zur Gänze unverhältnismäßig und sollte ersatzlos aus dem Entwurf gestrichen werden.

Echtzeitstreaming & Speicherverpflichtung bei Videoüberwachung im öffentlichen Raum, SPG §§ 93a, 94, 96

Videoüberwachung des öffentlichen Raums ist grundsätzlich eine sehr heikle Angelegenheit, nicht ohne Grund ist diese für private Auftraggeber_innen weitestgehend unzulässig [8]. Eine Ausweitung dieser Möglichkeiten ist daher rein prinzipiell kritisch zu sehen.

Die im Entwurf vorgesehene „unverzügliche Bereitstellung“ der Bilddaten „auf Verlangen der Sicherheitsbehörde“ bedeutet Echtzeitstreaming ohne jegliche Kontrolle etwa durch Richter_innen und Staatsanwält_innen. Diese unkontrollierten Möglichkeiten zur Videoüberwachung wurden auch schon in der Vergangenheit (am Schwedenplatz) von der Polizei missbraucht (“Wenn nix los ist, schauen die Polizisten halt in fremde Zimmer“[9]) und sollten daher eingedämmt, nicht ausgeweitet, werden.

Die geplante Aufbewahrungsverpflichtung (bis zu 2 Wochen durch Bescheid) für Betreiber_innen, die „zulässigerweise“ öffentlichen Raum überwachen, widerspricht dem

Datenschutz-Grundsatz, dass Daten nur so lange wie notwendig gespeichert werden sollen (DSG 2000 § 6 Abs. 1 [10]). Auch für die Anordnung dieser Speicherverpflichtung fehlt jegliche Kontrollinstanz.

Empfehlung: Die Maßnahme ist insgesamt als unverhältnismäßig und missbrauchsgefährdet einzustufen. Wir empfehlen, sie ersatzlos aus dem Entwurf zu streichen.

Mautüberwachung, BStMG § 19a bzw. StVO § 98a

Die Daten, die laut der Novelle erfasst werden sollen, „sind der Sicherheitsbehörde auf Ersuchen [...] zu übermitteln". Jegliche gerichtliche Kontrolle fehlt. Die bei der automatischen Mautkontrolle anfallenden Daten systematisch für den Zweck der Rasterfahndung zu verwenden widerspricht dem Datenschutz-Grundsatz (DSG § 6 Abs. 1), dass Daten nur für den Zweck verwendet werden dürfen, für den sie gesammelt wurden (explizit in BStMG §93a „Verfolgung der Mautprellerei"). Das selbe Problem gilt für die Änderung der Straßenverkehrsordnung. Dort dürfen die Daten derzeit „ausschließlich zum Zwecke eines Verwaltungsstrafverfahrens" verwendet werden. Die mit der vorliegenden Novellierung erlaubte Verwendung für den Zweck der Strafrechtspflege öffnet Tür und Tor für Rasterfahndungen.

Die Lenker_innen-Erkennung, die mit StVO § 98a eingeführt werden soll, ist technisch (Gesichtserkennungssoftware) extrem schwierig und zudem ethisch höchst problematisch.

Generell gilt: eine zu große Menge an Daten wird unauswertbar und erhöht die Wahrscheinlichkeit von falsch positiven Ausschlägen. Diese dann auch noch auszufiltern bedeutet einen weiteren personellen Aufwand. In der Folgenabschätzung ist die Rede von verschiedenen Varianten, die zur Auswertung von Videoaufnahmen überprüft wird - es ist unklar, von welchen Techniken/Technologien hier die Rede ist.

„Für den Aufbau der Videoauswertungssysteme" ist, laut Folgenabschätzung, die „Unterstützung externer Dienstleister" notwendig, für die „70 Dienstleistungstage zu je 1.000 veranschlagt werden". Bei Verrechnung handelsüblicher Stundensätze (ca. 150 Euro/Personenstunde) bedeutet das, dass das Projekt von 1 Person in 70 Tagen abgearbeitet werden soll. Für ein Projekt solchen Ausmaßes ist das komplett unterdimensioniert. Des weiteren soll zuerst nur ein Testbetrieb gefahren werden, um zu erheben, wie das System funktioniert - allerdings wurde bereits ein EU-Forschungsprojekt (INDECT [11]) mit österreichischen Steuermitteln finanziert, das genau die Machbarkeit von solchen Projekten erheben soll.

In diesem Bereich ergibt sich neben den Bedenken datenschutzrechtlicher, technischer, ethischer und menschenrechtlicher Art zusätzlich ein Bedenken in Bezug auf die verhältnismäßige und sparsame Verwendung von Budgetmitteln.

Empfehlung: Diese Maßnahme ist unverhältnismäßig, schlecht geplant und zeigt teilweise Doppelgleisigkeiten mit existierenden Projekten (INDECT). Sie sollte ersatzlos

gestrichen werden.

Netzsperren, TKG § 17

Die in Artikel 3 der EU Verordnung 2015/2120 [12] erwähnten Verkehrsmanagementmaßnahmen sind explizit nur bei „objektiv unterschiedlichen technischen Anforderungen an die Dienstqualität bestimmter Datenverkehrskategorien“ anwendbar - eine Anwendung bei strafrechtlichen Inhalten ist dabei nicht vorgesehen. Des weiteren müssen diese Verkehrsmanagementregeln „transparent, nichtdiskriminierend und verhältnismäßig“ sein - eine Kontrolle dieser Punkte ist im vorliegenden Gesetzesentwurf nicht vorgesehen. Der Zweck der „Vermeidung von strafrechtlichen Handlungen“ ist auch unangemessen breit definiert, die Auflistung sollte taxativ (vollständig) sein.

Der Zweck der erlaubten Verkehrsmanagementmaßnahmen ist nicht klar und geht auch aus der Erläuterung nicht hervor. Sollte der Zweck der Änderung sein, es Providern zu erlauben Internet-Pakete mit Jugendschutz-Optionen anzubieten, stellt dies einen nicht zulässigen Eingriff in die Netzneutralität dar, sofern keine genaueren Regelungen für die Provider erlassen werden. Es sind zumindest Vorkehrungen zu treffen, die Provider dazu zu verpflichten Pakete mit nicht eingeschränktem Internetzugang zu den selben Konditionen anzubieten.

Laut EuGH sind Netzsperren nur nach richterlicher Anordnung zulässig. [13]

Empfehlung: Diese Maßnahme ist unverhältnismäßig, unkontrolliert und wenig durchdacht. Sie sollte ersatzlos gestrichen werden.

Registrierung bei SIM-Karten, TKG §§ 92, 97

Aus rechtlicher Sicht gilt auch der Kauf von Guthaben für Prepaid-SIM-Karten als Vertragsabschluss - entsprechend muss die Erfassung der Stammdaten bzw. Identitätsfeststellung des_der Käufers_Käuferin auch beim Kauf von Guthaben passieren. Es ergibt sich durch Kassensysteme der Händler_innen und Buchungssysteme der Provider die Möglichkeit genau nachzuverfolgen wer, wann, für wen Guthaben gekauft hat. Mangels einer definierten Speicherfrist sollten diese anfallenden Daten gelöscht werden, sobald diese nicht mehr benötigt werden (DSG § 6 Abs. 1). Sowohl bei Prepaid SIM-Karten, als auch bei Guthaben wäre das sofort - weil diese für die Diensterbringung nicht erforderlich sind.

Die Überprüfung der Identität der Teilnehmer_in muss „durch oder für den Anbieter“ erledigt werden - für den Handel bedeutet das einen organisatorischen Mehraufwand, der wohl in den meisten Fällen dazu führen wird, dass entsprechende Produkte nicht mehr angeboten werden.

Empfehlung: Die vorgeschlagenen Änderungen sind überzogen und stellen unserer Mei-

nung nach bei korrekter Durchführung ein Handelshindernis dar. Es scheint, als wären Auswirkungen dieser Maßnahmen nicht ausreichend bedacht worden. Wir empfehlen die ersatzlose Streichung aus dem Entwurf.

Quick-Freeze Vorratsdatenspeicherung, TKG § 99

Es ist unklar, was „Zugangsdaten“ sind, die (laut Folgenabschätzung) abgespeichert werden sollen. Im umgangssprachlichen Gebrauch ist dies die Kombination aus Benutzer_innenname und Passwort, die üblicherweise zur Authentifzierung und Identifikation von Benutzer_innen dient. Diese Daten zu speichern kommt einer Komplettüberwachung gleich.

Aus den Erfahrungen der wieder aufgehobenen Vorratsdatenspeicherung in Österreich und Deutschland wissen wir bereits, dass Verkehrsdaten rapide ihren Wert für Ermittlungsarbeit verlieren. Die Speicherfrist von 12 Monaten ist daher unverhältnismäßig lang und sollte auf 1 Monat gekürzt werden.

Empfehlung: Die Maßnahme setzt laut Folgenabschätzung kein Ziel aus dem Regierungsprogramm um. Sie ist unzureichend ausformuliert (fehlende Definitionen) und eine unnötige Maßnahme. Sie sollte ersatzlos gestrichen werden.

Fachschaft Informatik
Technische Universität Wien

Literatur

[1] `https://ec.europa.eu/germany/eu60/frieden_de`

[2] Michel Foucault: Überwachen und Strafen – Die Geburt des Gefängnisses. Frankfurt/M. 1992

[3] `http://derstandard.at/2000062428318`

[4] `http://craphound.com/littlebrother/download/`

[5] `http://www.tu-dortmund.de/cms/berufung/de/home/Geschlechtergerechtigkeit_in_Berufungsverfahren/index.html`

[6] `http://www.tt.com/panorama/verbrechen/11038710-91/private-nachforschungen-polizisten-in-der-datenfalle.csp`

[7] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597

[8] https://www.dsb.gv.at/fragen-und-antworten#Videoueberwachung_auf_oeffentlichen_Grund_

[9] http://www.spiegel.de/netzwelt/web/a-392649.html

[10] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597

[11] https://en.wikipedia.org/wiki/INDECT

[12] http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R2120&from=DE

[13] http://curia.europa.eu/juris/document/document.jsf?text=&docid=149924&pageIndex=0&doclang=de&mode=req&dir=&occ=first&part=1&cid=515352