INSTITUTE FOR PARLAMENTARISM, SECURITY AND SCIENCE

FORUM ZUR FÖRDERUNG DES ÖFFENTLICHEN UND WISSENSCHAFTLICHEN DIALOGS ZU DEN THEMEN PARLAMENTARISMUS, SICHERHEIT UND GESELLSCHAFTSPOLITIK

Stellungnahme zu den beiden Regierungsvorlagen 15 und 17 d.B. betreffend das Überwachungspaket.

„*Darin zeigt sich eine wesentliche Funktion von **Privatheit**: In einer von individuellen Entscheidungen geprägten Gesellschaft muss die Privatsphäre gegen Einblicke Dritter geschützt werden, damit das individuelle öffentliche Handeln überhaupt möglich ist*“, so PETER SCHAAR im Vorwort zur angesehenen Publikation „Das Ende der Privatsphäre“ aus dem Jahr 2007.

Und weiter: „*Während staatliche Stellen – von der Polizei bis zur Finanzverwaltung – immer mehr über uns wissen wollen, bleiben die Bürger ohne angemessenen Schutz gegen Ausspionieren, Missbrauch, Manipulation und Verfälschung ihrer Daten.*“

Wer hätte gedacht, welche hohe Aktualität diese Aussagen über die Regierungspläne zukommen wird.

Die Bundesregierung hat zum von ihr genannten Sicherheitspaket am 21. Februar 2018 diese beiden Regierungsvorlagen im Ministerrat beschlossen. Hinzuweisen sei darauf, dass dieses Paket nicht voll inhaltlich dem Paket entspricht, welches im Vorjahr in Begutachtung geschickt wurde. Es ist daher nicht verständlich, wieso nicht wie üblich eine Begutachtung zu den Ministerialentwürfen vorgenommen wurde. Nunmehr muss dies durch die Beschlussfassung von zwei Ausschussbegutachtungen korrigiert werden, wofür dem Nationalrat bzw. seinen Ausschüssen zu danken ist. Es ist zu hoffen, dass die Zivilgesellschaft und Expertinnen sowie Experten sich umfänglich daran beteiligen werden.

Der Inhalt dieser Vorlagen setzt die Prognosen von Peter Schaar nunmehr um. Aus datenschutzrechtlicher Sicht sind dabei zwei Maßnahmen hervorzuheben:

Eine **verstärkte Videoüberwachung des öffentlichen Raums** führt dazu, dass **Privatheit im öffentlichen Raum kaum mehr möglich ist**, da die Sicherheitsbehörden Zugriff zu allen von Rechtsträgern des öffentlichen oder des privaten Bereichs, sofern letzteren ein öffentlicher Versorgungsbereich zukommt, gespeicherten Ton- und Bilddaten erhalten (§ 53 Abs. 5 SPG). Ergänzend dazu erhalten die Behörden aber auch direkten Zugang zu den Aufnahmezentren und dürfen an Ort und

Stelle diese Daten in Echtzeit streamen. Für den Datenzugriff genügt schon der Zweck der Vorbeugung wahrscheinlicher Angriffe.

Diese Maßnahmen kombiniert mit Gesichtserkennungsprogrammen führen zu einer beinahe **lückenlosen Überwachung jeder Person im öffentlichen Raum und damit zu einer maßlosen Einschränkung des Grundrechts auf Privatheit**.

Im Rahmen eines Interviews mit dem Tagesspiegel am 3. März 2018 führte die deutsche Bundesdatenschutzbeauftragte Andrea Voßhoff über die Entwicklungen folgendes aus:

*Am Berliner Bahnhof Südkreuz laufen Tests zur Gesichtserkennung mit Überwachungskameras. Lässt sich solche Technik mit Datenschutzrichtlinien vereinbaren**?***

Diese neue Dimension der biometrischen Gesichtserkennung bringt neue datenschutzrechtliche Herausforderungen mit sich. Mit dieser Technologie wird noch viel tiefer in die Grundrechte des Einzelnen eingegriffen, als es bei einer herkömmlichen Videoüberwachung der Fall ist. Sollten Verfahren wie die am Südkreuz getesteten in den Echtbetrieb gehen, bedarf es dazu in jedem Fall einer gesetzlichen Grundlage. Hier stellen sich auch verfassungsrechtliche Fragen.

Auch Univ. Prof. Dr. Walter Berka hat schon am 18. Österreichischen Juristentag im Jahr 2012 festgehalten: **„Für mich beginnt die Schwelle zum Eingriff dort, wo Verhalten in der Öffentlichkeit zum Gegenstand einer systematischen Beobachtung und Erfassung gemacht wird.“**

Und genau diese Grenze wird mit dem von der Bundesregierung vorgelegten Gesetzesentwurf überschritten.

Darüber hinaus werden in Zukunft aber **auch Fahrzeuge und deren Lenker sowie die Beifahrer** großflächig durch beispielsweise die Kameras der ASFINAG erfasst und die dabei entstandenen Daten gespeichert (§ 54 Abs. 4b SPG). Auch diese Daten stehen in Zukunft den Sicherheitsbehörden unter denselben Voraussetzungen zur Verfügung. An diesem Beispiel lässt sich deutlich zeigen, dass eine positive Überwachungsmaßnahme im Sinne der Verkehrssicherheit und des Schutzes von Menschenleben nunmehr auch für völlig andere Zwecke – nämlich die umfassende Überwachung der Bürgerinnen und Bürger - verwendet werden sollen.

Interessant ist in diesem Zusammenhang auch die Stellungnahme der ASFINAG vom 18. August 2017, in der ausgeführt wird, dass ein Großteil der Kameras nicht für die Speicherung von Daten ausgerüstet ist und diese systemisch nicht dafür ausgerichtet sind, Kennzeichen systematisch zu erfassen.

Auch die **sogenannte Section Control** wurde nur unter strengen Datenverwendungsbeschränkungen vom Datenschutzrat befürwortet und in Folge vom Gesetzgeber beschlossen. Nunmehr sollen diese Daten dennoch zu anderen Zwecken (wieder für die Vorbeugung, aber auch die Strafrechtspflege) in Zukunft verwendet werden (§ 98a Abs. 2 StVO).

Diese Vorlagen führen daher neben der generellen Einschränkung des Rechts auf Privatheit auch dazu, dass bisher nur für einen ganz bestimmten Zweck gespeicherte Daten auch für Überwachungszwecke verwendet werden sollen. Dies alles um eine angebliche Kriminalitätsbedrohung von der österreichischen Bevölkerung abzuwehren, obwohl diese laut Kriminalstatistik des BMI nicht vorhanden ist und die angezeigten Fälle mit Ausnahme der Computerkriminalität deutlich zurückgehen.

Darüber hinaus hat der VfGH in seiner Entscheidung zur Section Control genau diese beschränkte und enge Zweckwidmung der Datenverwendung als Grundlage für die Genehmigung der Section Control gesehen. Es stellt sich daher die zusätzliche Frage, ob die vorgesehene Übermittlungsverpflichtung an die Sicherheitsbehörden dieses Instrument nicht im Nachhinein verfassungswidrig macht.

Ein zweiter Schwerpunkt entsteht durch den Einsatz eines **Bundestrojaners** zur Überwachung verschlüsselter Nachrichten, dessen konkrete technische Entwicklung noch nicht feststeht (§ 135a StPO). Klar ist jedoch, dass es sich dabei um **Schadsoftware** handelt, die notwendig ist, um unbekannte Sicherheitslücken in IT-Systemen auszunützen. Bei einer solchen Schadsoftware ist jedoch systemisch, dass diese auch für andere Zwecke missbraucht werden kann, um beispielsweise Fremddaten auf ein System zu laden und dadurch das Ansehen einer Person zu schädigen (Kinderpornographisches Material).

Auch ist beim Einsatz von Schadsoftware nicht vorhersehbar, ob diese nicht weiteren Schaden in vernetzten Systemen anrichten kann, wie dies

im Fall eines Hackerangriffs auf das britische Gesundheitsministerium passierte, wo bei einer Reihe von Krankenhäusern die EDV-Systeme ausfielen, was zu lebensbedrohlichen Situationen führten.

Erschwerend kommt noch dazu, dass eine solche Software natürlich nicht auf dem freien Markt zu erhalten ist und jedenfalls die Republik mit zwielichtigen Unternehmen Geschäfte eingehen muss, die normalerweise Diktaturen oder Verbrechersyndikate unterstützen.

Bei dem Abhören von internetunterstützten Gesprächen ist zusätzlich zu berücksichtigen, dass eben diese Gefahren auch gegenüber dem Kommunikationspartner entstehen können, der möglicherweise mit dem Verfolgungsgrund überhaupt nichts zu tun hat.

Wozu gegenwärtig Schadsoftware wirklich verwendet wird, zeigt sich am eben bekanntgeworden erfolgreichen Hackerangriff auf das deutsche Regierungsnetz (Informationsverbund Berlin-Bonn (IVBB)).

„*Laut dpa sollen mittels Schadsoftware Daten des Außen- und des Verteidigungsministeriums kopiert worden sein. Nach Informationen aus Sicherheitskreisen gegenüber dem SPIEGEL könnte sich der Datenabfluss aber womöglich auch nur auf das Außenministerium beschränken. Um welche Datenmenge es geht - einzelne Dateien oder die Inhalte mehrerer Festplatten - ist ebenfalls unklar*“ (Das steckt hinter dem Hackerangriff aufs Regierungsnetz, spiegel online).

Vorgebeugt soll diesen Bedenken wohl mit § 135a Abs. 2 StPO werden, wonach eine Überwachung verschlüsselter Nachrichten überdies nur dann zulässig ist, wenn das Programm

1. nach Beendigung der Ermittlungsmaßnahme funktionsunfähig ist oder ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems, in dem es installiert wurde, und der in ihm gespeicherten Daten entfernt wird, und

2. keine Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme, in denen kein Programm zur Überwachung verschlüsselter Nachrichten installiert wird, bewirkt.

Genau eine solche Prognose vor dem Eingriff zu treffen, ist aber nach allen Experteneinschätzungen unmöglich.

Eine Genehmigung des Gesetzgebers zur Beschaffung und Einsatz einer solchen nicht näher detaillierten äußerst sensiblen Technologie ist daher grob fahrlässig und unverantwortlich, eine Art legistisches russisches Roulette.

Den Charakter dieser Entwürfe zeigt sich auch an dem Umstand, dass es 2018 notwendig erscheint, das Briefgeheimnis massiv einzuschränken. Jahrzehntelang sind die zuständigen Behörden mit der Voraussetzung ausgekommen, dass die Beschlagnahme von Briefen nur gegenüber Personen angewandt werden darf, die sich wegen einer solchen Tat in Haft befinden oder deren Vorführung deswegen angeordnet wurde. Nunmehr soll diese Voraussetzung ersatzlos gestrichen werden. Begründet wird diese Maßnahme mit der Versendung von Drogen aus dem Darknet. Auch hier wird ein völlig unpassendes Einzelfallbeispiel herangezogen, um eines der ältesten Grundrechte weitgehend einzuschränken.

Apropos: Mit dem Datenschutzanpassungsgesetz – Inneres soll das nach der DSGVO gewährleistete Widerspruchsrecht in den Sicherheitsbereichen für die Bürgerinnen und Bürger generell ausgeschlossen werden. Wie formulierte voraussehend Peter Schaar so treffend:

„*Während staatliche Stellen – von der Polizei bis zur Finanzverwaltung – immer mehr über uns wissen wollen,* ***bleiben die Bürger ohne angemessenen Schutz gegen Ausspionieren, Missbrauch, Manipulation und Verfälschung ihrer Daten****.*“

Dr. Peter Pointner, Mitglied des Vorstandes des InstPSS sowie Mitglied des Datenschutzrates

23. März 2018