KOPIE

Der Bayerische Landesbeauftragte für den Datenschutz

Bayer. Datenschutzbeauftragter • PF 22 12 19 • 80502 München

An das
Bundesverfassungsgericht
Schlossbezirk 3
76131 Karlsruhe

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen	München, den 01.09.2020
1 BvR 2771/18 und 1 BvR 1552/19	DSB/2-622/2-336	Durchwahl: 089 212672 - 0

Stellungnahme zu den Verfahren 1 BvR 2771/18 und 1 BvR 1552/19

Anlage: 20 Abschriften der Stellungnahme des BayLfD

Sehr geehrter Herr Präsident,

für die Gelegenheit der Stellungnahme zu den bezeichneten Verfahren bedanke ich mich.

Zur konkreten polizeilichen Praxis der Polizei in Baden-Württemberg und in Hessen kann ich aufgrund meiner fehlenden örtlichen Zuständigkeit leider nichts beitragen. Gerne werde ich aber zunächst auf meine Prüferfahrungen zum polizeilichen Einsatz der Quellen-Telekommunikationsüberwachung in Bayern eingehen. In den dann folgenden Ausführungen werde ich mich auf die vom Senat aufgeworfene Frage konzentrieren, ob eine verfassungsrechtliche Notwendigkeit staatlicher Maßnahmen zum Schutz informationstechnischer Systeme gegen Dritte gesehen wird, ob solche Schutzvorschriften bestehen und ob in diesem Zusammenhang der VO (EU) Nr. 2016/679 (DSGVO), der Richtlinie (EU) 2016/680 (JI-DSRL) und den diesbezüglichen Vorschriften des deutschen Rechts Bedeutung beigemessen wird.

./.

Wagmüllerstraße 18
80538 München
Postfach 22 12 19
80502 München

Telefon: 089 212672-0
Telefax: 089 212672-50
https://www.datenschutz-bayern.de
poststelle@datenschutz-bayern.de

1. Rechtstatsächliche Bemerkungen

Die bayerische Polizei hat Maßnahmen der „Quellen-Telekommunikationsüberwachung" (Quellen-TKÜ) in den Jahren 2008 bis 2011 auf Grundlage der Befugnis zur Durchführung von Telekommunikationsüberwachungen durchgeführt. 23 dieser Maßnahmen habe ich im Jahr 2012 umfänglich geprüft.

> Der Bayerische Landesbeauftragte für den Datenschutz,
> Prüfbericht Quellen-TKÜ, vom 31.07.2012
> (abrufbar unter www.datenschutz-bayern.de unter Themengebiete/Polizei).

Seinerzeit habe ich in Ansehung der Entscheidung des Bundesverfassungsgerichts vom 27.02.2008 – 1 BvR 370, 595/07 (BVerfGE 120, S. 274 ff.) dringend empfohlen, fortan Quellen-TKÜ-Maßnahmen nur noch auf ausdrücklicher gesetzlicher Grundlage durchzuführen. Dieser Empfehlung ist der bayerische Gesetzgeber im Jahr 2017 nachgekommen.

> Gesetz zur effektiveren Überwachung gefährlicher Personen vom
> 24.07.2017, BayGVBl. 2017, S. 388.

Die Befugnis zur Quellen-TKÜ in Art. 34a Abs. 1a Polizeiaufgabengesetz (PAG) wurde im Rahmen des PAG-Neuordnungsgesetzes im Jahr 2018 ohne beabsichtigte inhaltliche Änderungen in Artikel 42 Abs. 2 PAG überführt. Diese Vorschrift wird durch die Art. 48 ff. BayPAG, insbesondere im Hinblick auf den Schutz des Kernbereichs privater Lebensgestaltung, um Betroffenenrechte und technisch-organisatorische Vorgaben ergänzt.

> PAG-Neuordnungsgesetz vom 18.05.2018,
> BayGVBl. 2018, S. 301.

Ebenso wie die von den Beschwerdeführern angegriffenen hessischen und baden-württembergischen Vorschriften orientiert sich die Befugnis in Art. 42 Abs. 2 PAG dem Wortlaut nach eng an der vom Ersten Senat getroffenen Abgrenzung zwischen dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informations-

technischer Systeme und dem Fernmeldegeheimnis aus Art. 10 Abs. 1 Grundgesetz (GG) (BVerfG, Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 120, 274, 309).

Die bayerische Regelung enthält allerdings in Art. 42 Abs. 2 Satz 2 PAG die polizeiliche Befugnis, auch visualisierte Darstellungen der Telekommunikation auszuleiten und zu erheben („soweit zu Zwecken des Satzes 1 unerlässlich"). Diese zusätzliche Regelung betrifft die Anfertigung von sog. „Application-Shots", die zumindest zum Zeitpunkt meiner Prüfung im Jahr 2012 und wohl auch noch im Jahr 2017 als notwendig erachtet wurde, um eine Quellen-TKÜ bei Messenger-Diensten und E-Mail-Verkehr technisch realisieren zu können.

Bayerischer Landtag, LT-Drs. 17/16299, S. 15 (zu Nr. 13).

Es ist diskussionswürdig, ob diese Form der Ausleitung die vom Bundesverfassungsgericht definierten Grenzen einer Quellen-TKÜ hin zu einer Onlinedurchsuchung überschreitet – unabhängig davon, ob sie wie in Bayern gesetzlich legitimiert wird oder ohne ausdrückliche gesetzliche Regelung praktiziert wird. Die bayerische Polizei kann damit de lege lata gegenüber der baden-württembergischen und hessischen Polizei eine Art „Quellen-TKÜ-Plus" durchführen, ohne dass sie wie eine Online-Durchsuchung Zugriff auf den gesamten Datenbestand des Zielinformationssystems nimmt.

Gleichwohl hat die Quellen-TKÜ bei der bayerischen Polizei seit 2012 nur eine begrenzte praktische Bedeutung. Auch seit der ausdrücklichen Regelung der Befugnis im PAG im Jahr 2017 macht die Polizei von der Befugnis bislang nur sehr zurückhaltend *bzw. gar keinen* Gebrauch.

Bayerischer Landtag, LT-Drs. 17/23554, S. 2 zu Frage 5.

Zwar wurde zur Evaluierung des Gesetzesvollzugs des PAG-Neuordnungsgesetzes eine unabhängige Kommission zur Begleitung des neuen Polizeiaufgabengesetzes eingesetzt. Eine Gesetzesevaluierung des Art. 42 Abs. 2 PAG wurde vor dem Hintergrund mangelnder tatsächlicher Relevanz durch diese Kommission jedoch nicht vorgenommen.

./.

Kommission zur Begleitung des neuen bayerischen Polizeiaufgabengesetzes, Abschlussbericht vom 30.08.2019, S. 11
(abrufbar unter www.polizeiaufgabengesetz.bayern.de).

Seit der Veröffentlichung des Prüfberichts Quellen-TKÜ vom 31.07.2012 sind mir in Bayern keine einschlägigen präventivpolizeilichen Maßnahmen bekannt geworden, sodass sich Folgeprüfungen erübrigt haben. Dementsprechend wurde mir mit Schreiben des Bayerischen Staatsministeriums des Innern, für Sport und Integration vom 19. August 2020 mitgeteilt, dass im Zeitraum vom 1. August 2012 bis 1. August 2020 seitens der bayerischen Polizei keine Maßnahmen der Quellen-TKÜ durchgeführt wurden.

Allerdings führe ich die begrenzte Anzahl von Maßnahmen in erster Linie darauf zurück, dass der mit der Maßnahme verbundene Angriff auf die Integrität und Vertraulichkeit des Zielsystems gegenwärtig noch technisch aufwändig ist oder aufwändige Begleitmaßnahmen erfordert.

Erfolgt der Eingriff beispielsweise wie bei den meisten polizeilichen Maßnahmen in Bayern in den Jahren 2008 bis 2011 nicht per remote, besteht ein gesteigertes Risiko, dass die Maßnahme von der betroffenen Person entdeckt wird.

Ein verdeckter polizeilicher remote-Zugriff ist hingegen deutlich aufwändiger und anspruchsvoller zu realisieren: Zunächst muss die Polizei vorab das Zielinformationssystem sicher identifizieren, um eine versehentliche Infiltration eines nichtpolizeirelevanten informationstechnischen Systems zu vermeiden. Bevor der eigentliche Angriff auf die Integrität des Zielsystems erfolgt, wird es notwendig sein, die auf dem Zielsystem vorhandenen Anwendungen und Programme auszukundschaften, um Kenntnis über mögliche Schwachstellen des Zielsystems erlangen. Missachtet die Zielperson die gebotenen IT-Sicherheitsanforderungen, etwa indem sie Administratorenrecht und Nutzerrechte nicht getrennt hält, kann die Polizei einen remote-Angriff auch ohne bislang unbekannte Sicherheitslücken von Anwendungen erfolgreich durchführen.

./.

Allerdings werden Zielpersonen – gerade im Bereich der organisierten Kriminalität – häufig gängige IT-Sicherheitsstandards beachten. In solchen Fällen kann ein remote-Zugriff letztlich nur über die Ausnutzung von bislang allgemein unbekannten Sicherheitslücken von Anwendungen und Programmen erfolgen, die auf dem Zielsystem eingesetzt werden. Die von den Beschwerdeführern sinngemäß geäußerte Vermutung, dass die Polizei jedenfalls teilweise auf bislang unbekannte Sicherheitslücken angewiesen sein wird, um ihren remote-Zugriff auf ein Zielsystem erfolgreich durchzuführen, ist vor diesem Hintergrund durchaus nachzuvollziehen.

Nur der Vollständigkeit halber möchte ich darauf hinweisen, dass bei einer technischen Weiterentwicklung der Überwachungstechnologie oder bei entsprechender Kooperation der Anbieter von Telekommunikationsdienstleistungen die Anzahl der Maßnahmen deutlich anwachsen kann. Aufmerksam machen möchte ich hierbei auf das Bemühen der Bundesregierung, Anbieter von Telekommunikationsdienstleistungen auf die Mitwirkung bei der Quellen-TKÜ der Verfassungsschutzbehörden gesetzlich zu verpflichten.

> Bundesministerium des Innern, für Bau und für Heimat (BMI), Referentenentwurf vom 16.06.2020, Entwurf eines Gesetzes zur Harmonisierung des Verfassungsschutzrechts, S. 8 zu Artikel 10 Gesetz, § 2 Abs. 1a (abrufbar unter www.bmi.bund.de, unter Ministerium / Gesetzgebungsverfahren).

2. Verfassungsrechtliche Notwendigkeit staatlicher Maßnahmen zum Schutz informationstechnischer Systeme gegen Dritte?

Im Kern lege ich die Kritik der Beschwerdeführer als Rüge aus, dass die angegriffenen Vorschriften es unklar lassen, mit *welchen* technischen Mitteln die Polizei in die von der betroffenen Person genutzten informationstechnischen Systeme eingreifen will. Diese Rüge halte ich im Ergebnis für berechtigt.

Aus datenschutzrechtlicher Sicht sehe ich es ebenso wie die Beschwerdeführer als entscheidend an, ob und inwieweit staatliche Maßnahmen zum Schutz informations-

technischer Systeme gegen Angriffe Dritter verfassungsrechtlich geboten sind. Dies möchte ich nachfolgend begründen, wobei bei der vorliegenden Sach- und Gesetzeslage die herkömmliche Zuordnung zu grundrechtsdogmatischen Funktionen (Abwehrfunktion, Schutzpflicht usw.) ein anspruchsvolles Unterfangen darstellt.

2.1 Grundrechtlich begründete staatliche Schutzpflicht

In seiner bisherigen Rechtsprechung hat das Bundesverfassungsgericht noch nicht ausdrücklich Feststellungen dazu getroffen, ob aus dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme staatliche Schutzpflichten abzuleiten sind.

Allerdings hat das Bundesverfassungsgericht in seiner Entscheidung vom 27.02.2008 folgenden Zielkonflikt beschrieben, der eine staatliche Schutzpflicht zumindest nahe legt:

> „Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolgreichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben. Der Zielkonflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist." (BVerfG, Urt. v. 27.02.2008 – 1 BvR 370, 595/07, BVerfGE 120, 274, 325 f.).

Aus diesen Feststellungen lässt sich ableiten, dass eine möglichst große Sicherheit informationstechnischer Systeme im öffentlichen Interesse liegt. Auch in sprachlicher Hinsicht scheint das Bundesverfassungsgericht im Jahr 2008 bei der Ableitung des Grundrechts *auf Gewährleistung* der Integrität und Vertraulichkeit informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht auch im Sinne einer Gewährleistungsverantwortung ausgegangen zu sein. Vor diesem Hintergrund meine

./.

ich, dass das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme auch einen objektiven Auftrag an den Staat richtet, einen hinreichenden Schutz des Grundrechts sicherzustellen.

> Vgl. u.a. Papier, Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft, NJW 2017, 3025, 3027, zuvor bereits Hömig, Neues Grundrecht, neue Fragen? Zum Urteil des BVerfG zur Online-Durchsuchung, JurA 2009, 207 ff. sowie Petri, Das Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung", DuD 2008, 443, 447 f.

Die bisherige Rechtsprechung des Bundesverfassungsgerichts zu grundrechtlich begründeten staatlichen Schutzpflichten verstehe ich allerdings so, dass die staatlichen Organe grundsätzlich in eigener Verantwortung entscheiden können, wie sie ihre Verpflichtung zu einem effektiven Schutz eines Grundrechts erfüllen. Eine Verengung dieser Einschätzungsprärogative kommt wohl nur in besonders gelagerten Fällen in Betracht, wenn ein effektiver Grundrechtsschutz nicht anderweitig zu erreichen ist. Dieses Regel-Ausnahme-Verhältnis gilt wohl auch dann, wenn der Staat zum Schutz hochrangiger Grundrechtsgewährleistungen verpflichtet ist.

> Grundlegend BVerfG, Urt. v. 16.10.1977 – 1 BvQ 5/77, BVerfGE 46, 160, 164 f.

Anerkannt ist, dass eine Verletzung einer Schutzpflicht jedenfalls dann vorliegt, „wenn Schutzvorkehrungen entweder überhaupt nicht getroffen sind, wenn die getroffenen Regelungen und Maßnahmen offensichtlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder wenn sie erheblich hinter dem Schutzziel zurückbleiben."

> BVerfG, Urt. v. 01.12.2009 – 1 BvR 2857, 2858/07, BVerfGE 125, 39, 78 f., Rn. 135; vgl. auch BVerfG, Urt. v. 10.01.1995 – 1 BvF 1/90, 1BvR 342, 348/90, BVerfGE 92, 26, 46, Rn. 74.

Nach meinem Eindruck bekennen sich die Gesetzgeber des Bundes und der Länder

in zahlreichen Vorschriften und in unterschiedlicher Weise auch zu der staatlichen Schutzpflicht in Bezug auf die Integrität und Vertraulichkeit informationstechnischer Systeme. Auch staatliche Vollzugsorgane nehmen diese Verantwortung wahr. Prominentes Beispiel auf Bundesebene ist das Bundesamt für Sicherheit in der Informationstechnik (BSI), das auf Grundlage des BSI-Gesetzes (BSIG) agiert. Aber auch auf Landesebene wird aus dem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen ein objektiver Handlungsauftrag staatlicher Organe abgeleitet, z.B. bei der Zusammenarbeit verschiedener Behörden im Rahmen sog. Cyberabwehren (vgl. ausführlich unten Ziff. 2.2.2).

2.2 Schutzvorschriften, Bedeutung von EU-Datenschutzvorschriften

Die Vorschriften der DSGVO und der JI-DSRL sehen keine ausdrücklichen Schutzpflichten der Mitgliedstaaten vor, die Grundsätze der Integrität und Vertraulichkeit in der Informationstechnik zu fördern. Gleichwohl haben aus meiner Sicht mehrere Vorschriften für die hier zu entscheidende Frage des Senats eine nicht unerhebliche Bedeutung.

2.2.1 Gesamtverantwortung des Landes für technisch-organisatorische Maßnahmen landeseigener öffentlicher Stellen, die personenbezogene Daten verarbeiten

Zunächst gehört es nach Art. 5 Abs. 1 Buchst. f) DSGVO zu den zentralen Grundsätzen für die Verarbeitung personenbezogener Daten, dass sie in einer Weise verarbeitet werden, die ihre angemessene Sicherheit gewährleistet. Dieser Datenschutzgrundsatz wird in den Art. 24, 25 und 32 DSGVO sowie in Art. 19, 20 und 29 JI-DSRL konkretisiert, die den Verantwortlichen und (in Art. 32 DSGVO, Art. 29 JI-DSRL) die Auftragsverarbeiter zu geeigneten technischen und organisatorischen Maßnahmen verpflichten.

Soweit die Polizei ihre Erkenntnisse über bislang nicht bekannt gewordene Sicherheitslücken zurückhält, verletzt sie zwar nicht unmittelbar ihre eigenen Pflichten aus Art. 19, 20 und 29 JI-DSRL, in tatsächlicher Hinsicht beeinträchtigt sie aber die Mög-

lichkeiten anderer Stellen, ihre Pflichten zu technisch-organisatorischen Maßnahmen wahrzunehmen. Dies berührt nicht nur die Schutzpflicht des Staates gegenüber Privaten, sondern auch insbesondere die Sicherheit der Datenverarbeitung eigener staatlicher oder kommunaler Einrichtungen, soweit diese ihrerseits personenbezogene Daten verarbeiten und so in die Grundrechte Dritter eingreifen.

So gibt es auf nationaler Ebene zahlreiche Vorschriften, die Behörden zu technisch-organisatorischen Schutzmaßnahmen für eine integre und vertrauliche Verarbeitung personenbezogener Daten verpflichten. In Umsetzung der Dienstleistungsrichtlinie 2006/123/EG sieht beispielsweise § 2 Abs. 1, Abs. 2 E-Government-Gesetz Baden-Württemberg vom 17.12.2015 (EGovG BW, BaWüGBl. 2015, 1191) vor, dass die dortigen Behörden den Zugang zur elektronischen Kommunikation zu eröffnen haben. Mindestens einen solchen Zugang müssen sie durch „angemessene Sicherungsmaßnahmen gegen den unberechtigten Zugriff Dritter" schützen. Die Behörden haben diesen gesicherten Zugang grundsätzlich bei der Kommunikation in Verwaltungsverfahren zu nutzen. Nach § 3 Abs. 1 Hessisches E-Government-Gesetz vom 12.09.2018 (HEGovG, HEGVBl 2018, 570) ist jede Behörde verpflichtet, einen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifizierten elektronischen Signatur versehen sind, zu eröffnen. Die Pflicht zu technisch-organisatorischen Maßnahmen ist in verschiedenen Vorschriften des Gesetzes verankert.

Hessen und Baden-Württemberg sind zudem durch § 1 Abs. 1 Onlinezugangsgesetz (OZG) verpflichtet, bis spätestens Ende 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Die dabei zu beachtenden IT-Sicherheitsstandards richten sich nach § 5 OZG. Das für die Festlegung der Sicherheitsstandards zuständige BMI bezeichnet in Auslegung des OZG die „Zuverlässigkeit, Ausfallsicherheit und *IT-Sicherheit* der digitalen Angebote" als „integralen Bestandteil der Entwicklung und im kontinuierlichen Betrieb".

BMI, https://www.onlinezugangsgesetz.de unter Suchbegriff IT-Sicherheit, FAQ vom 24.06.2020: IT-Sicherheit und Support (Abruf am 13.08.2020)

./.

Diese beispielhaft vorgestellten Regelungen sind meines Erachtens nicht nur aus EU-rechtlichen Vorgaben ableitbar, sondern auch verfassungsrechtlich geboten. Denn Behörden greifen auch im Rahmen der Leistungsverwaltung regelmäßig in das grundrechtlich geschützte Persönlichkeitsrecht ein, insbesondere wenn sie ohne Einwilligung der betroffenen Person sie betreffende personenbezogene Daten verarbeiten. Es ist daher ein Gebot der Verhältnismäßigkeit, dass die negativen Auswirkungen der Verarbeitung durch technisch-organisatorische Maßnahmen auf das Nötigste beschränkt werden.

> Grundlegend BVerfG, Urt. v. 15.12.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1, 44, Rn. 151 m.w.N.; BVerwG, Urt. v. 23.06.2004 – 3 C 41/03, BVerwGE 121, 115, Rn. 40; OVG Lüneburg, Urt. v. 10.10.2019,– 11 LC 148/15, juris Rn. 74; BayVGH, Beschl. v. 25.03.2015 – 11 ZB 14.2601, juris Rn. 12.

Halten Sicherheitsbehörden Erkenntnisse über unbekannte Sicherheitslücken zurück, beeinflussen sie damit nicht nur die Selbstschutzmöglichkeiten privater Datenverarbeitungen. Vielmehr tragen sie mittelbar auch dazu bei, dass andere Behörden nicht effektiv ihren eigenen gesetzlichen Verpflichtungen bei der Ergreifung organisatorischer und verfahrensrechtlicher Vorkehrungen nachkommen können, welche der Gefahr einer Verletzung des Persönlichkeitsrechts gerade entgegenwirken sollen. Sinnbildlich gesprochen würde nicht nur die linke Hand des Staates nicht wissen, was die rechte tut. Vielmehr würde die Polizei als rechte Hand des Staats dazu beitragen, dass andere Behörden als linke Hand des Staats nicht grundrechtsschonend in die Grundrechte von Personen eingreifen können.

Die E-Government-Gesetze des Bundes und der Länder verdeutlichen ebenso wie das OZG, dass Bund und Länder nahezu sämtliche öffentlich-rechtliche Dienstleistungen in eine vernetzte elektronische Kommunikationsinfrastruktur überführen. Meines Erachtens kann eine solche Zentralisierung von Verwaltungstätigkeiten nur gerechtfertigt sein, wenn der jeweilige Gesetzgeber auch eine Gesamtverantwortung für die IT-Sicherheit der bei den Behörden verarbeiteten personenbezogenen Daten übernimmt – unabhängig von der hier nicht zu entscheidenden Frage, inwieweit eine

./.

solche Zusammenführung im Einklang mit dem datenschutzrechtlichen Prinzip der informationellen Trennung von Verwaltungsdienstleistungen steht. Will der Gesetzgeber in einem angenommenen übergeordneten Interesse der öffentlichen Sicherheit Abstriche an der IT-Sicherheit der landeseigenen Behörden zulassen, so muss er deshalb schon in *Wahrnehmung seiner Gesamtverantwortung* die Voraussetzungen hierfür ausdrücklich, normenklar und normbestimmt regeln.

2.2.2 Einwirkung auf öffentliche und nichtöffentliche Stellen durch staatlich veranlasste Standardisierungen

Weiterhin ergibt sich die verfassungsrechtliche Notwendigkeit von Schutzmaßnahmen auch daraus, dass die öffentliche Hand selbst mit Vorgaben auf das Sicherheitsniveau informationstechnischer Systeme nichtöffentlicher Stellen einwirkt.

Bund und Länder nehmen die unter 2.1 skizzierte Schutzpflicht zunächst wahr, indem sie Behörden und sonstige öffentliche Stellen mit der Aufgabe betrauen, datenschutzrechtlich Verantwortliche und Auftragsverarbeiter über die wesentliche Themen der Sicherheit in der Informationstechnik zu beraten und zu informieren.

Beispielsweise hat der Bundesgesetzgeber mit dem BSI eine Bundesoberbehörde geschaffen, deren Aufgabe nach § 3 Abs. 1 Satz 1 BSIG ausdrücklich darin besteht, die Sicherheit in der Informationstechnik zu fördern. Die Aufzählung von wichtigen im öffentlichen Interesse liegenden Aufgaben nach Satz 2 schließt auch private Interessen an IT-Sicherheit ein. Das BSI verfolgt als Cyber-Sicherheitsbehörde des Bundes das Leitbild, Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, *Wirtschaft und Gesellschaft* zu gestalten. Als „Kunden" werden nicht nur staatliche Einrichtungen, sondern auch Unternehmen und Privatanwender bezeichnet. Zwei zentrale Aufgabenbereiche bestehen in der Information zu *allen* wichtigen Themen der IT-Sicherheit sowie in der Beratung zu Fragen der IT-Sicherheit.

BSI, Leitbild, abrufbar unter
https://www.bsi.bund.de/DE/DasBSI/Leitbild/leitbild_node.html.

./.

Ohne dies gesetzlich zu verankern, hat Baden-Württemberg eine „Cyberwehr Baden-Württemberg" initiiert. Als Kontakt- und Beratungsstelle für kleine und mittlere Unternehmen sowie als Koordinierungsstelle bei Hackerangriffen vernetzt die Cyberwehr sich mit Sicherheitsbehörden, Wirtschaft und Wissenschaft. Dazu ist eine „Zentrale Ansprechstelle Cybercrime" (ZAC) eingerichtet worden, die beim Landeskriminalamt angesiedelt ist.

https://cyberwehr-bw.de.

Das Land Hessen hat mit dem „Hessen Cyber Competence Center (Hessen3C)" eine zentrale Kompetenzstelle zur interdisziplinären Zusammenarbeit und institutionalisierten Kooperation staatlicher Behörden im Bereich der IT-Sicherheit eingerichtet. Auch Hessen3C verfolgt u.a. die Aufgabe, nichtöffentliche Stellen in IT-Sicherheitsfragen zu beraten.

https://innen.hessen.de/sicherheit/hessen3c/hessen-cyber-competence-center.

Staatliche Stellen wirken auch im Rahmen von Zertifizierungen auf die IT-Sicherheitsstandards von Unternehmen ein. Aus datenschutzrechtlicher Sicht sind Mitgliedstaaten nach Maßgabe der Art. 42, 43 DSGVO verpflichtet, datenschutzspezifische Zertifizierungsverfahren sowie Datenschutz-Gütesiegel und -Prüfzeichen zu fördern. Als Mittel zur regulierten Selbstregulierung dienen derartige Verfahren dazu, einen Verantwortlichen zu dem Nachweis zu befähigen, dass er die Datenschutzgrundsätze der DSGVO – darunter den Grundsatz der Integrität und Vertraulichkeit im Sinne des Art. 5 Abs. 1 Buchst. f) DSGVO – einhält. Zertifizierungen sind in der DSGVO zudem an verschiedenen Stellen als Mittel zum Nachweis für eine rechtskonforme Ausgestaltung der personenbezogenen Datenverarbeitung vorgesehen, vgl. Art. 24 Abs. 3, Art. 25 Abs. 3, Art. 28 Abs. 5 und 6, Art. 32 Abs. 3 DSGVO.

Eine besondere Bedeutung haben standardisierte Vorgaben der IT-Sicherheit allerdings bei kritischen Infrastrukturen im Sinne der Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung

./.

der Notwendigkeit, ihren Schutz zu verbessern. Nach Art. 5 dieser Richtlinie haben die Mitgliedstaaten für Sicherheitslösungen für diese kritischen Infrastrukturen zu sorgen. Zudem verpflichtet Art. 7 der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union die Mitgliedstaaten dazu, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen. Diese Vorgaben hat der Bundesgesetzgeber mit dem IT-Sicherheitsgesetz vom 17.07.2015 (BGBl. 2015 I S. 1324) umgesetzt, in dem er Betreibern kritischer Infrastrukturen nach Maßgabe der §§ 8a, 8b BSIG den Nachweis der Erfüllung eines Mindestniveaus an IT-Sicherheit gegenüber dem BSI etwa durch Sicherheitsaudits auferlegt.

Ähnlich wie bei dem in 2.2.1 beschriebenen behördenübergreifenden Betrieb von elektronischen Kommunikationsinfrastrukturen kann aus rechtsstaatlicher, aber vor allem auch aus Sicht der Bürgerinnen und Bürger ein Widerspruch entstehen, wenn staatliche Stellen einerseits ein hinreichendes Sicherheitsniveau bei informationstechnischen Systemen bescheinigen, die von der Polizei anschließend durch Ausnutzung unbekannter Sicherheitslücken infiltriert werden. Unabhängig davon, ob der Staat bei mängelbehafteten Zertifizierungen von Sicherheitsanwendungen haftet, sehe ich aus verfassungsrechtlicher Sicht hier zwar keine Vollzugs- sehr wohl aber eine Gewährleistungsverantwortung des Staates. Sie begründet meines Erachtens die verfassungsrechtliche Notwendigkeit, das angedeutete Spannungsverhältnis zwischen zertifizierten Sicherheitsstandards einerseits und polizeilichen Ermittlungsmaßnahmen andererseits durch hinreichend klare und bestimmte Regelungen aufzulösen.

2.2.3 Polizeiliche Verarbeitung nach Treu und Glauben

Aus meiner Sicht spricht auch die *Abwehrdimension* der Grundrechte für eine verfassungsrechtliche Notwendigkeit, den vorgenannten Zielkonflikt durch hinreichend klare und bestimmte Regelungen aufzulösen und entsprechende Schutzmaßnahmen in Bezug auf die betroffenen Personen zu ergreifen. Diese Notwendigkeit lässt sich aus der Verpflichtung der Polizei ableiten, ihre Datenverarbeitung am Grundsatz von Treu und Glauben auszurichten, vgl. Art. 4 Buchst. a) JI-DSRL.

./.

Der in der DSGVO und JI-DSRL gleichermaßen verankerte Grundsatz einer Datenverarbeitung nach Treu und Glauben wird aus Art. 8 Abs. 2 Satz 1 der Charta der Grundrechte der EU (EuGRCh) abgeleitet und ist nicht disponibel. Soweit ich dies nachvollziehen kann, gibt es zum Datenschutzgrundsatz der Verarbeitung nach Treu und Glauben allerdings bislang lediglich Entscheidungen, die sich auf die DSGVO bzw. auf die Vorgängerrichtlinie 95/46/EG beziehen.

Der Grundsatz der Verarbeitung nach Treu und Glauben wird in den Erläuterungen zu Art. 8 EuGRCh nicht näher definiert. Sie verweisen vielmehr ausdrücklich auf die Richtlinie 95/46/EG, die damit als Interpretationshilfe heranziehbar ist. Nach dem 38. Erwägungsgrund dieser Richtlinie setzt Datenverarbeitung nach Treu und Glauben voraus, dass die betroffenen Personen in der Lage sind, „das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden." Dementsprechend steht der Grundsatz der Verarbeitung nach Treu und Glauben zumindest in einer engen Beziehung zum Grundsatz der Transparenz in Art. 5 Abs. 1 Buchst. a) DSGVO.

Dem entspricht es, dass Entscheidungen, die sich unmittelbar mit dem Grundsatz der Verarbeitung personenbezogener Daten nach Treu und Glauben auseinandersetzen, rar sind. Die meisten veröffentlichten Entscheidungen beziehen sich auf die Frage, ob der Verantwortliche in bestimmten Fallkonstellationen aus Treu und Glauben dazu verpflichtet ist, über die allgemeinen Transparenzanforderungen hinaus die betroffene Person über Rahmenbedingungen einer Verarbeitung zu unterrichten. In aller Regel handelt es sich dabei um Fälle, in denen die betroffene Person nicht mit der geplanten Verarbeitung rechnen muss oder die Information benötigt, um die Folgen der Verarbeitung ansatzweise nachvollziehen zu können.

> EuGH, Urt. v. 01.10.2019 – C-673/17, Rn 78, 79 (Information über beabsichtigte Speicherdauer von Cookies); EuGH, Urt .v. 16.01.2019 – C-496/17 (Zollkodex), Rn. 59, 60 (Information über die Verwendung der Steueridentitätsnummer und weiterer Daten zu Zwecken der Zollverwaltung); EuGH, Urt. v. 01.10.2015 – C-201/14 (Bara), Rn. 34 (Information über gesetzlich nicht ausdrücklich vorgesehene Datenweitergabe von Behörde zu Behörde).

./.

Bei der Anwendung des Grundsatzes der Verarbeitung nach Treu und Glauben speziell auf die JI-DSRL sind Erwägungsgrund 26 JI-DSRL einige negative Hinweise zu entnehmen. Danach ist der Datenschutzgrundsatz der Verarbeitung nach Treu und Glauben *nicht* deckungsgleich mit dem Konzept eines fairen Verfahrens im Sinne des Art. 47 EuGRCh bzw. Art. 6 Europäische Menschenrechtskonvention (EMRK). Zugleich ist zu beachten, dass die JI-DSRL den in Art. 5 Abs. 1 Buchst. a) DSGVO verbrieften Grundsatz der Transparenz aus nachvollziehbaren Gründen *nicht* übernommen hat. Dementsprechend weist Satz 2 des 26. Erwägungsgrundes JI-DSRL sinngemäß darauf hin, dass die Durchführung von verdeckten Ermittlungen an sich *nicht* gegen den Grundsatz der Verarbeitung nach Treu und Glauben verstoßen. Zugleich weist Satz 3 ausdrücklich darauf hin, dass die Maßnahmen durch Rechtsvorschriften zu regeln sind, *dem Verhältnismäßigkeitsgrundsatz genügen und „die berechtigten Interessen der betroffenen natürlichen Person gebührend berücksichtigen" müssen.*

Aus Erwägungsgrund 26 JI-DSRL schließe ich: Einerseits darf der Grundsatz der Verarbeitung nach Treu und Glauben nicht zu weit ausgelegt und dahingehend missinterpretiert werden, dass der in Art. 5 Abs. 1 Buchst. a) DSGVO gewährleistete Grundsatz der Transparenz de facto auch in den Anwendungsbereich der JI-DSRL importiert wird. Andererseits setzt die Verarbeitung nach Treu und Glauben für bestimmte Fallkonstellationen *ausnahmsweise die Information über bestimmte Modalitäten einer personenbezogenen Datenverarbeitung* voraus.

Auch wenn die Fallkonstellationen der Quellen-TKÜ und des Ankaufs von Steuerdaten-CDs sich erheblich unterscheiden, scheint mir ein ähnlicher Gedanke in einer Kammerentscheidung des 2. Senats des Bundesverfassungsgerichts enthalten zu sein, die sich mit den Bestimmtheitsanforderungen einer Durchsuchungsanordnung auf Grundlage mutmaßlich rechtswidrig angekaufter Steuerdaten-CDs befasst hat.

BVerfG, Beschl. v. 04.04.2017 – 2 BvR 2551/12, juris Rn. 21 ff.,

Das Bundesverfassungsgericht hielt dabei fest, dass ein Durchsuchungsbeschluss den Tatvorwurf und die konkreten Beweismittel so beschreiben muss, dass der äu-

./.

ßere Rahmen abgesteckt wird, innerhalb dessen die Zwangsmaßnahme durchzuführen ist. Der Richter müsse die aufzuklärende Straftat, wenn auch kurz, doch so genau umschreiben, wie es nach den Umständen des Einzelfalls möglich ist. Dies versetze dann den von der Durchsuchung Betroffenen zugleich in den Stand, die Durchsuchung seinerseits zu kontrollieren und etwaigen Ausuferungen im Rahmen seiner rechtlichen Möglichkeiten von vornherein entgegenzutreten.

Grundlegend hierzu BVerfG, Beschl. v. 26.05.1976 – 2 BvR 294/76, juris Rn. 31

Was den Grundsatz der Verarbeitung nach Treu und Glauben anbelangt, stellen schließlich Teile der Literatur für mich überzeugend darauf ab, dass die jeweilige Verarbeitung innerhalb dessen liegen muss, „womit der Betroffene bei der Erhebung redlicher Weise hat rechnen müssen. ... Neben das Gebot der Transparenz und der Kontrollmöglichkeit durch Verfahrensrecht tritt somit auch ein Gebot der Vorhersehbarkeit."

Wolff in Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 60.

Das beschriebene Spannungsverhältnis zwischen fehlendem Transparenzprinzip einerseits und Transparenzanforderungen des Prinzips der Verarbeitung nach Treu und Glauben lässt sich meines Erachtens – im Einklang mit der bisherigen Rechtsprechung des Bundesverfassungsgerichts zu verdeckten polizeilichen Maßnahmen – nur dadurch auflösen, dass der Gesetzgeber die zulässige Vorgehensweise der Polizei nicht nur in Bezug auf die tatsächliche Infiltration und anschließende Verwendung der personenbezogenen Daten, sondern auch in Bezug auf vorgelagerte Annexmaßnahmen (Beschaffung) oder nachgelagerte Informationspflichten abstrakt generell regelt. Nur der Gesetzgeber kann die Voraussetzungen und Grenzen der Beschaffung von Sicherheitslücken rechtssicher definieren und zugleich durch eine Regelung auf abstrakt-genereller Ebene dafür sorgen, dass eine konkrete verdeckte polizeiliche Maßnahme nicht (unmittelbar) gegenüber einer konkreten Zielperson offengelegt werden muss.

./.

Was die Verhältnismäßigkeit einer solchen gesetzlichen Ausgestaltung der Maßnahme anbelangt, richten sich die Bestimmtheitsanforderungen nach der Eingriffsintensität der Maßnahme. Dabei werden die Gesetzgeber zu berücksichtigen haben, dass die Polizei bei remote-Zugriffen zwar aus legitimen Grund handelt, die Maßnahme aber überaus schwer wiegt und von außen betrachtet in Teilen des Geschehensablaufs sogar kriminellen Handlungen nicht unähnlich sein kann („Ankauf" von Sicherheitslücken im grauen Markt, Infiltration des Zielsystems mithilfe von Täuschungshandlungen, heimliches Ausleiten von vertraulichen Kommunikationsinhalten).

Im Ergebnis mag die Notwendigkeit gesetzlich geregelter Schutzmaßnahmen für die IT-Sicherheit zwar nicht mit dem Grundsatz der Rechtmäßigkeit der Verarbeitung nach Art. 8 JI-DSRL zu begründen sein, dessen Absatz 2 den Mindestinhalt einer gesetzlichen Verarbeitungsbefugnis beschreibt. Der Grundsatz einer Verarbeitung nach Treu und Glauben nach Art. 4 Buchst. a) JI-DSRL indes legt die rechtsstaatliche Notwendigkeit einer solchen Regelung zumindest sehr nahe. Eine solche Regelung müsste nicht nur die Voraussetzungen der Infiltration des Zielsystems hinreichend klar beschreiben, sondern muss darüber hinaus auch

- die Grenzen einer Beschaffung, und

- die Zurückhaltung von Erkenntnissen über bislang allgemein unbekannt gebliebene Sicherheitslücken

hinreichend klar regeln, um eine den Grundsätzen nach Treu und Glauben genügende Datenverarbeitung darzustellen. Ausgehend von den bisherigen Überlegungen wäre dabei etwa daran zu denken, dass die Polizei ihre Erkenntnisse über schwerwiegende Sicherheitslücken nicht zurückhalten kann, wenn es konkrete Anhaltspunkte dafür gibt, dass sie in absehbarer Zeit von Dritten zu Angriffen insbesondere auf kritische Infrastrukturen verwendet werden.

./.

3. Zusammenfassung

Nach vorstehenden Überlegungen kann ich somit im Ergebnis die Kritik der Beschwerdeführer an den angegriffenen Vorschriften nachvollziehen, soweit sie sich auf die vom Senat aufgeworfene Fragen bezieht.

Mit freundlichen Grüßen

Prof. Dr. Thomas Petri
Landesbeauftragter für den Datenschutz