PinG
Privacy in Germany
Datenschutz und Compliance
www.PinGdigital.de

Hinweise für das Anfertigen von Beiträgen

Stand: Februar 2019

Beiträge/Zielgruppe

Die PinG legt einerseits den Fokus auf das Datenschutzrecht und beleuchtet andererseits unterschiedliche Facetten der Informationsverarbeitung. Die Zeitschrift richtet sich gleichermaßen an die verschiedenen Akteure der datenschutzrechtlichen Praxis und der Wissenschaft. Diesem Publikum sind in der Regel die Sachverhalte (wie bspw. Facebook oder WhatsApp) geläufig, und die rechtliche Aufbereitung der jeweiligen Thematik steht ohne große „Ausschweifungen" im Vordergrund. Die PinG kommt somit auf den Punkt und fördert den Diskurs auch abseits der herrschenden Lehre.

Die PinG ist in folgende Bereiche gegliedert:

- TEIL A: PRIVACY TOPICS
  Klassische Wissenschaftliche Aufsätze
- TEIL B: PRAXIS DATENSCHUTZ & COMPLIANCE
  Beiträge mit Themen aus der Praxis, möglichst mit Arbeitshilfen: Checklisten, Musterverträge/-klauseln u. ä.
- TEIL C: PRIVACY NEWS

Information der Schriftleitung

Bitte stimmen Sie sich mit der Schriftleitung vorab kurz über Ihre geplante Veröffentlichung, über die Zielgruppe und über den Zeitpunkt der Fertigstellung des Manuskripts ab, damit Ihr Beitrag rechtzeitig in den Redaktionsplan aufgenommen werden kann (Anschrift der Schriftleitung siehe Kasten).

Kontaktdaten Schriftleitung „PinG"

Dr. Sebastian Golla/Dr. Carlo Piltz
Schriftleitung PinG
Erich Schmidt Verlag GmbH & Co. KG
Genthiner Str. 30 G, 10785 Berlin
Telefax: 0 30/25 00 85-305
E-Mail: PinG@ESVmedien.de

Hinweise der Schriftleitung für Beiträge des Teils A:

PRIVACY TOPICS

1. Die Texte sollten angesichts der heutigen Lesegewohnheiten möglichst kurz und prägnant gefasst sein.
   Eine Gliederung des Beitrags mit Zwischenüberschriften erleichtert die Lesbarkeit.
2. Unter der Überschrift und einem eventuellen Untertitel folgt der Name des Autors/der Autoren mit ausgeschriebenem Vornamen und Titel. Beiträge erhalten eine Abbildung sowie eine **Kurzvita des Autors** (max. 200 Zeichen mit Leerzeichen). Bilder können als Datei (z. B. JPEG) eingereicht werden. Die Kurzvita enthält in Stichworten Angaben zur Person und ggf. Funktion.
3. Es folgt ein kurzer Vorspann (**Abstract**), der das Kernanliegen des Beitrags hervorhebt. Das Abstract sollte 400 bis 650 Zeichen mit Leerzeichen umfassen.
4. Beenden Sie bitte Ihren Beitrag mit einer kurzen Zusammenfassung der zentralen Ergebnisse.
5. Der Text sollte mit einer gängigen Textverarbeitung (vorzugsweise Word) im Fließtext mit Absatzmarken geschrieben werden. Die Zwischenüberschriften sollten als solche bereits kenntlich gemacht werden.
6. Bitte teilen Sie zudem die wesentlichen Keywords mit, welche u. a. später für das Jahresstichwortverzeichnis verwendet werden (in der Regel 3 bis 5 Keywords). **Bitte markern Sie hierfür die Keywords im Text gelb unterlegt an.**
7. Verwenden Sie bitte folgende Gliederungsstruktur:
   I. [Hauptüberschrift]
   1. [Gliederungsebene 2]
   a) [Gliederungsebene 3]
   aa) [Gliederungsebene 4]
8. Die Zitierweise folgt den in juristisch orientierten Zeitschriften üblichen Regeln:
   – Fußnoten sind hinter das Satzzeichen zu platzieren.
   – Autorennamen sind stets kursiv zu schreiben.

Beispiel: *Mustermann*, PinG 2016, 22, 24.
Mustermann, in: Simitis, BDSG, 8. Aufl. 2014, § 1 Rn. 1.
Mustermann, Datenschutzrecht, 2016, Rn. 116 oder
Mustermann, Datenschutzrecht, 2016, S. 123.

Bitte geben Sie zu Entscheidungen immer Datum (achtstellig), Aktenzeichen und Fundstelle an. Werden mehrere Entscheidungen desselben Gerichts zitiert, werden diese durch ein Semikolon getrennt. Auch wenn es sich um Entscheidungen desselben Gerichts handelt, muss das Gericht nach dem Semikolon nochmals genannt werden.

Beispiel: KG Berlin, Urt. v. 07.03.2012 – 26 U 65/11, PinG 2012, 132, 133; KG Berlin, Beschl. v. 23.08.2011 – 4 W 43/11, ITRB 2012, 54, 55.

Ein Verweis auf die hierzu erste Fußnote – wie z. B. durch a. a. O. (Fn. 2), a. a. O., (o. Fn. 2) oder ebenda – ist nicht zulässig.

Vorschriften werden wie folgt zitiert:

§ 1 Abs. 2 Nr. 1 BDSG
§ 1 Abs. 5 Halbs. 2 TMG
Art. 9 Abs. 2 lit. f) DSGVO
ErwG. 5 S. 2 RL 95/46/EG

Bitte verwenden Sie die gebräuchlichen Abkürzungen. Für Datumsangaben verwenden Sie bitte z. B. 07.01.2016; für Betragsangaben verwenden Sie bitte die folgende Form: 25.000 Euro.

→

Drucksachen des Bundestages werden wie folgt zitiert: **BT-Drs. 13/7385, S. 21**.

Fußnoten enden stets mit einem Punkt.

9. Die Schriftleitung behält sich grundsätzlich Änderungen vor.
10. Das Manuskript schicken Sie bitte per E-Mail an die Schriftleitung unter: PinG@ESVmedien.de

Hinweise der Schriftleitung für Beiträge des Teils B:

PRAXIS DATENSCHUTZ & COMPLIANCE

1. Die Praxisbeiträge sollten ebenfalls möglichst kurz und prägnant gefasst sein.

   Eine Gliederung des Beitrags mit Zwischenüberschriften kann die Lesbarkeit erleichtern.
2. Unter der Überschrift und einem eventuellen Untertitel folgt der Name des Autors/der Autoren mit ausgeschriebenem Vornamen und Titel. Beiträge erhalten eine Abbildung sowie eine **Kurzvita des Autors** (max. 200 Zeichen mit Leerzeichen). Bilder können als Datei (z. B. JPEG) eingereicht werden. Die Kurzvita enthält in Stichworten Angaben zur Person und ggf. Funktion.
3. Es folgt ein kurzer Vorspann (**Abstract**), der das Kernanliegen des Beitrags hervorhebt. Das Abstract sollte 400 bis 650 Zeichen mit Leerzeichen umfassen.
4. Der Text sollte mit einer gängigen Textverarbeitung (vorzugsweise Word) im Fließtext mit Absatzmarken geschrieben werden. Die Zwischenüberschriften sollten als solche bereits kenntlich gemacht werden.
5. Bitte teilen Sie zudem die wesentlichen Keywords mit, welche u. a. später für das Jahresstichwortverzeichnis verwendet werden. **Bitte markern Sie hierfür die Keywords im Text gelb unterlegt an.**
6. Verwenden Sie bitte folgende Gliederungsstruktur:

   I. [Hauptüberschrift]
   1. [Gliederungsebene 2]
   a) [Gliederungsebene 3]
   aa) [Gliederungsebene 4]
7. Sofern Sie Zitierungen in den Praxisbericht einfügen möchten, verfahren Sie bitte wie in den Hinweisen zu Teil A unter Ziff. 8.
8. Die Schriftleitung behält sich grundsätzlich Änderungen vor.
9. Das Manuskript schicken Sie bitte per E-Mail an die Schriftleitung unter: PinG@ESVmedien.de

Äußere Form des Manuskripts

1. Text und Tabellen
Der Text sollte mit einer gängigen Textverarbeitung (vorzugsweise Word) im Fließtext mit Absatzmarken geschrieben werden. Die Zwischenüberschriften sollten als solche bereits kenntlich gemacht werden, ebenso wie die Positionierung etwaiger Abbildungen, Grafiken und Tabellen.

2. Grafiken, Abbildungen/Bilder
Grundsätzlich ist die Auflockerung des Textes durch Abbildungen, Grafiken und Tabellen sehr erwünscht.

a) Grafiken

Grafiken können Diagramme, Schaubilder o. Ä. sein. Bitte speichern Sie Grafiken, die nicht in Word erstellt worden sind, möglichst separat als editierbare Datei. Verwendbar sind Dateien aus Programmen der Office-Familie wie PowerPoint oder Excel, aber auch aus professionellen Grafik-Programmen wie Adobe Illustrator, Freehand oder Corel Draw (in diesem Fall die Grafiken bitte im EPS-Format oder alternativ im PDF-Format speichern).

Vermeiden Sie bitte, Grafiken farbig anzulegen. Eine spätere (automatische) Umwandlung nach Graustufen führt zu unkontrollierbaren Resultaten. Benutzen Sie stattdessen Grautöne und schwarze/weiße Füllmuster. Grafiken oder Grafikelemente, die bereits farbig vorliegen, sollten vor Weitergabe an den Verlag in Graustufen umgewandelt werden.

b) Abbildungen/Bilder

Abbildungen oder Grafiken sind immer auch als separate Bild-Dateien oder Scanvorlagen zu übermitteln. Auf Schatten, runde Ecken und auf eine dreidimensionale Darstellung bei Diagrammen ist bei der Erstellung zu verzichten. Beachten Sie bitte bei der Erstellung der Grafiken, dass die Endgröße der Großbuchstaben bei der Bildbeschriftung 2 mm nicht unterschreiten darf.

Bilder können als Originalvorlage (Foto, Dia etc.) oder als Datei eingereicht werden. Diese Fotos dürfen nicht mit einer Strukturfolie überzogen sein. Beim Fotografieren mit einer Digitalkamera ist „höchste Bildqualität" zu wählen bzw. eine Auflösung von ca. 300 dpi. JPEG- oder TIFF-Dateien sollten nicht komprimiert sein und mindestens Endformatgröße haben.

Korrekturen und Honorar

Vom Verlag erhalten Sie auf elektronischem Weg einen Korrekturabzug im PDF-Format. Bitte drucken Sie den Korrekturabzug aus und vermeiden Sie möglichst Korrekturen, die über die Beseitigung von Satzfehlern hinausgehen. Leiten Sie die korrigierte Fassung bitte als (mit der Kommentarfunktion korrigierte) PDF-Datei, als Scan oder als Ausdruck an den Verlag und die Schriftleitung per Mail oder Fax weiter.

In Absprache mit der Schriftleitung kann etwa vier Wochen nach Erscheinen ein Honorar gezahlt werden. Nicht vollständig bedruckte Seiten werden entsprechend als halbe bzw. viertel Seite honoriert. Für Rezensionen wird grundsätzlich kein Honorar gezahlt. Auf den Seiten enthaltene Anzeigen werden bei der Berechnung des Umfangs eines Beitrags nicht mitgerechnet. Bitte geben Sie auf dem Formular, das Sie vom Verlag erhalten, Ihre aktuelle Postadresse und Ihre Bankverbindung an (ferner USt-Option und Steuer-Nr. nicht vergessen). Sie erhalten etwa vier Wochen nach Erscheinen der Zeitschrift zwei Belegexemplare der Printausgabe.

Veröffentlichungsrechte

Zur Veröffentlichung angebotene Beiträge müssen frei sein von Rechten Dritter. Veröffentlicht werden nur Originalbeiträge. Sollten sie auch an anderer Stelle zur Veröffentlichung oder gewerblichen Nutzung angeboten worden sein, muss dies angegeben werden. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag das ausschließliche Verlagsrecht und das Recht zur Herstellung von Sonderdrucken für die Zeit bis zum Ablauf des Urheberrechts. Das Verlagsrecht umfasst auch die Rechte, den Beitrag in fremde Sprachen zu übersetzen, Übersetzungen zu vervielfältigen und zu verbreiten sowie die Befugnis, den Beitrag bzw. Übersetzungen davon in Datenbanken einzuspeichern und auf elektronischem Wege zu verbreiten (online und/oder offline), das Recht zur weiteren Vervielfältigung und Verbreitung zu gewerblichen Zwecken im Wege eines fotomechanischen oder eines anderen Verfahrens sowie das Recht zur Lizenzvergabe. Dem Autor verbleibt das Recht, nach Ablauf eines Jahres eine einfache Abdruckgenehmigung zu erteilen; sich ggf. hieraus ergebende Honorare stehen dem Autor zu. Bei angeforderten oder auch bei unaufgefordert eingereichten Manuskripten behält sich die Schriftleitung das Recht der Kürzung und Modifikation der Manuskripte ohne Rücksprache mit dem Autor vor.

Für weitere Fragen stehen wir Ihnen gern persönlich zur Verfügung.

Hier eine Leseprobe aus dem Bereich: **PRIVACY TOPICS:**

→

PRIVACY TOPICS

Prof. Dr. Frank Braun (Fachhochschule für öffentliche Verwaltung NRW)

Prof. Dr. Jan Dirk Roggenkamp (Hochschule für Wirtschaft und Recht Berlin)

0Zapftis v2.0

Repressive Staatstrojaner

Prof. Dr. Frank Braun und *Prof. Dr. Jan Dirk Roggenkamp*

Im Rahmen eines denkwürdigen Gesetzgebungsverfahrens[1] wurde kurz vor Ende der letzten Legislaturperiode die Strafprozessordnung „durch die Hintertür"[2] um Befugnisse zur Durchführung einer sog. Quellen-Telekommunikationsüberwachung (§ 100a Abs. 1 Sätze 2 und 3 StPO) sowie einer Online-Durchsuchung (§ 100b StPO) ergänzt. Gegen diese Regelungen sind inzwischen vier Verfassungsbeschwerden anhängig.[3] In dem nachfolgenden Beitrag werden die grundsätzlichen verfassungsrechtlichen Implikationen der Neuregelungen skizziert.

I. Ausgangslage

1. Online-Durchsuchung

§ 100b StPO gestattet eine sog. Online-Durchsuchung. Damit wird der heimliche Zugriff auf PCs, Smartphones, Tabletcomputer etc. (i.W. auch zusammenfassend „informationstechnische Systeme") bezeichnet, der auf eine längerfristige Überwachung[4] mit Hilfe einer Trojanersoftware abzielt.[5] Dabei haben die durchführenden Behörden mit Installation der Trojanersoftware vollumfänglichen Zugriff auf das informationstechnische System. Sie können sämtliche auf dem System vorhandenen Dateien lesen, verändern und herunterladen. Alle auf dem Gerät installierten Programme bzw. Apps können ausgeführt oder beendet werden; Software kann installiert und gelöscht werden. Vorhandene Kameras (Webcams, aber auch sonstige mit dem System verbundene Kameras wie optische Babyfone und Hausüberwachungssysteme) und Mikrofone können ein- und ausgeschaltet und über diese der Nutzer des Systems und dessen Umgebung beobachtet werden. Kurz: es besteht die Möglichkeit eines „Großen Spähangriffs".[6] Zudem kann jederzeit der aktuelle Bildschirminhalt überwacht und aufgezeichnet werden, so dass die Nutzung des informationstechnischen Systems de facto in Echtzeit mitverfolgt werden kann. Über Keylogging-Funktionen kann zudem jede Tastatureingabe registriert werden, auch wenn diese nicht in einer Datei auf dem informationstechnischen System gespeichert wird. So wird es z.B. ermöglicht Passworteingaben aufzuzeichnen, wenn diese auf dem Bildschirm nicht dargestellt werden.

2. Quellen-Telekommunikationsüberwachung

§ 100a Abs. 1 S. 2 StPO enthält eine Befugnis, eine sog. Quellen-Telekommunikationsüberwachung („Quellen-TKÜ") durchzuführen, die das Mitlesen und Mithören verschlüsselter laufender Kommunikation (z.B. über Messenger wie WhatsApp oder Signal) ermöglicht. Hierfür müssen sämtliche Kommunikationsinhalte vor der Verschlüsselung bzw. nach der Entschlüsselung ausgeleitet werden. Technisch wird dies durch einen Zugriff auf das informationstechnische System der Zielperson (der „Quelle" der Telekommunikation) bewerkstelligt.[7] Auch hier wird eine Trojanersoftware, die heimlich auf dem Zielsystem installiert werden muss, genutzt.

1 Vgl. die Darstellung bei *Roggan*, StV 2017, 821.
2 *Beukelmann*, NJW Spezial 2017, 440.
3 Die Verfasser sind Verfahrensbevollmächtigte einer dieser Verfassungsbeschwerden. Der vorliegende Text basiert auf den – weitergehenden – Ausführungen der Beschwerdeschrift.
4 Zur Dauer der Maßnahme vgl. unten II. 2. a) ee).
5 *Petri/Schwabenbauer*, in: Lisken/Denninger, Handbuch Polizeirecht, 6. Aufl. 2018, Teil G Rn. 617.
6 *Beukelmann*, NJW-Spezial 2017, 440.
7 Vgl. *Braun/Roggenkamp*, K&R 2011, 681.

3. Kleine Online-Durchsuchung

In § 100a Abs. 1 S. 3 StPO wird ergänzend ein heimlicher Zugriff auf „gespeicherte Inhalte und Umstände der Kommunikation" zugelassen, „wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können". Es handelt sich hierbei nicht um eine (Quellen-)Telekommunikationsüberwachung im eigentlichen Sinne, da diese nur die „laufende" Kommunikation erfassen darf. Dagegen gestattet § 100a Abs. 1 S. 3 StPO explizit auch einen Zugriff auf „ruhende" Kommunikation (auf einem informationstechnischen System gespeicherte Inhalte und Umstände der Kommunikation) und stellt insoweit einen Fall der Online-Durchsuchung dar. Sie wird auf Grund ihrer inhaltlichen Beschränkung auf Telekommunikationsinhalte und -umstände auch als „kleine Online-Durchsuchung" bezeichnet.[8]

4. Vorgehensweise

Unabhängig davon, ob eine Online-Durchsuchung, eine „kleine Online-Durchsuchung" oder eine Quellen-TKÜ durchgeführt werden soll, muss eine Softwarelösung[9] eingesetzt werden. Hierzu ist es erforderlich, auf dem informationstechnischen System der Zielperson (in der Regel einem Smartphone) eine „Trojanersoftware" heimlich zu installieren (sog. Infiltration), um dann aus der Ferne auf das informationstechnische System zugreifen zu können (sog. Remote Access).[10]

Die Infiltration erfolgt in der Regel durch Ausnutzen eines Programmierfehlers, einer sog. Sicherheitslücke in einer Software auf dem von der Zielperson genutzten System. Hierbei kann es sich um das Betriebssystem oder eine Anwendungssoftware handeln. Der Zielperson wird z. B. ein unverdächtig erscheinendes Textdokument zugesandt (oder auf einem Datenträger übergeben);[11] sobald dieses geöffnet wird, wird die Trojanersoftware bei bestehender Internetverbindung unbemerkt auf das Zielsystem geladen und installiert.[12]

Vor der Installation müssen eine solche Sicherheitslücke entweder eigenständig ermittelt oder entsprechende Informationen über diese Schwachstellen von Dritten „beschafft" werden. Der Ankauf von Informationen über offene Sicherheitslücken erfolgt regelmäßig auf entsprechenden „Schwarzmärkten". Hauptnachfrager sind nach Erkenntnissen der Gesellschaft für Informatik e. V. Cyberkriminelle, die diese für die Installation sog. Ransomware[13] ausnutzen wollen.[14]

Sobald die Hersteller die betreffenden Sicherheitsdefizite in ihren Softwareprodukten/Betriebssystemen beseitigen,[15] ist ein Zugriff ausgeschlossen. Dementsprechend ist es erforderlich, eine zu Überwachungszwecken genutzte Sicherheitslücke, den Anbietern der Software *nicht* mitzuteilen. Damit ein effektiver Zugriff auf ein möglichst breites Portfolio von Betriebssystemen (z. B. Windows, Linux, iOS, Android, MacOS) und Anwendungssoftware (z. B. Microsoft Office, Adobe PDF) möglich ist, müssen möglichst viele Sicherheitslücken vorgehalten und genutzt werden. Der Bedarf kann de facto nur durch einen Ankauf von Informationen zu (unbekannten) Sicherheitslücken und Möglichkeiten zur Ausnutzung auf dem „freien Markt" gedeckt werden.[16]

Wird eine Sicherheitslücke nicht geschlossen, kann sie nicht nur von den Strafverfolgungsbehörden, sondern auch von Cyberkriminellen genutzt werden. Das war z. B. im Jahr 2017 der Fall, als eine von der amerikanischen National Security Agency (NSA) „vorgehaltene" Sicherheitslücke zur Verbreitung des Schadprogramms „WannaCry" genutzt wurde. Dieses Schadprogramm infizierte im Mai 2017 innerhalb weniger Tage weltweit Millionen von informationstechnischen Systemen und legte sie lahm. Betroffen waren neben zahllosen privaten Nutzern z. B. die Deutsche Bahn AG, der japanische Autohersteller Nissan, der französische Autohersteller Renault sowie Banken, Geldautomaten und Schulen.[17] Auch lebenswichtige Einrichtungen wie Krankenhäuser waren beeinträchtigt.[18] Die Folgen des Angriffs dauern bis heute an.[19]

II. Verfassungsrechtliche Implikationen

1. Unvereinbarkeit mit der Menschenwürdegarantie

Sowohl die Online-Durchsuchung als auch die Quellen-TKÜ stellen unter Berücksichtigung der heutigen Nutzungsgepflogenheiten (mobiler) informationstechnischer Systeme nach hier vertretener Auffassung eine nicht zu rechtfertigende selbständige[20] Verletzung der durch Art. 1 Abs. 1 GG absolut geschützten Menschenwürde dar. Die heimlichen Überwachungsmaßnahmen implizieren einen Zugriff auf Informationen, die der unantastbaren Intimsphäre des Nutzers zuzurechnen sind.

Im Jahr 2008 hat das *BVerfG* anhand der damaligen Nutzungsgepflogenheiten festgestellt, dass informationstechnische Systeme (seinerzeit ganz überwiegend Personal Computer) *„typischerweise bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien, genutzt"* werden.[21] Es hat dennoch eine Durchführung einer (präventiven) Online-Durchsuchung in eng umgrenzten Fällen für zulässig erachtet.

8 *Sinn*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o. g. Gesetzentwurf (2017), S. 5; *Roggan*, StV 2017, 821, 824.

9 Eine gewisse Marktführerstellung hat hierbei offenbar die Software FinSpy des Anbieters FinFisher, vgl. *Holland*, FinSpy: Deutsche Überwachungssoftware gegen türkische Opposition eingesetzt, heise.de v. 15. 05. 2018 – abrufbar unter: https://www.heise.de/newsticker/meldung/FinSpy-Deutsche-Ueberwachungssoftware-gegen-tuerkische-Opposition-eingesetzt-4049677.html.

10 *Petri/Schwabenbauer*, in: Lisken/Denninger, Handbuch Polizeirecht, 6. Aufl. 2018, Teil G Rn. 616 m. w. N.

11 Vgl. *Roggan*, StV 2017, 821, 822 m. w. N.

12 Vgl. z. B. *Gierow*, FINSPY: Neuer Staatstrojaner-Exploit in RTF-Dokument gefunden, golem.de v. 13. 09. 2017 – abrufbar unter: https://www.golem.de/news/finspy-neuer-staatstrojaner-exploit-in-rtf-dokument-gefunden-1709-130025.html.

13 Das ist eine Software, die einen Computer infiziert und sperrt. Ein Zugriff ist erst wieder nach Zahlung eines „Lösegelds" (Ransom) möglich; dazu *Salomon*, MMR 2016, 575.

14 *Federrath*, Stellungnahme der GI zum Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen v. 06. und 08. 02. 2018, abrufbar unter: https://gi.de/fileadmin/GI/Hauptseite/Aktuelles/Meldungen/2018/GI-Stellungnahme_Neuausrichtung_HessVS_2018-02-08.pdf.

15 Das Schließen einer Sicherheitslücke erfolgt über einen sog. Patch, der über die (häufig automatisch ausgeführte) Aktualisierungsfunktion der Software auf dem System eingespielt wird.

16 *Pohlmann/Riedel*, DuD 2018, 37.

17 *Biermann*, WannaCry: Großer Schaden für 31.000 Dollar, Zeit Online v. 14. 05. 2017, abrufbar unter: https://www.zeit.de/digital/datenschutz/2017-05/wannacry-ransomware-cyberattacke-bitcoin-windows-microsoft.

18 Vgl. z. B. *Wittmann*, Erpresser-Software lähmt 40 Kliniken in Großbritannien, Berliner Morgenpost v. 12. 05. 2017, abrufbar unter: https://www.morgenpost.de/politik/article210553117/Krankenhaeuser-in-England-durch-Hacker-Angriff-lahmgelegt.html.

19 *Gierow*, MS17-010: Noch immer Millionen Wanna-Cry-Infektionen aktiv, golem.de v. 14. 05. 2018, abrufbar unter: https://www.golem.de/news/ms17-010-noch-immer-millionen-wanna-cry-infektionen-aktiv-1805-134360.html.

20 Vgl. *Di Fabio*, in: Maunz/Dürig, GG, 84. EL. 2018, Art. 2 Abs. 1, Rn. 158.

21 BVerfGE 120, 274, 322 f. Rn. 231; ähnlich, ohne erkennbar neue Bewertung der zwischenzeitlich geänderten Nutzungsgepflogenheiten BVerfGE 141, 220, 306 f. – Rn. 218.

Diese Nutzungsgepflogenheiten haben sich allerdings seit dem Jahr 2008 drastisch gewandelt. Informationstechnische Systeme sind nicht mehr in erster Linie Arbeitsgeräte und werden *„auch"*, also nur nachrangig, zum Speichern persönlicher Daten genutzt. Sie sind inzwischen unabkömmliche persönliche Begleiter, die mitunter *„auch"* für die berufliche Tätigkeit genutzt werden. Darauf vorgehaltene persönliche Daten sind regelmäßig nicht nur von *„gesteigerter"*, sondern von höchster Sensibilität;[22] werden nicht nur bewusst, sondern auch unbewusst automatisiert erfasst und gespeichert.

Die modernen Nutzungsgepflogenheiten lassen es als ausgeschlossen erscheinen, ein informationstechnisches System zu infiltrieren, ohne hierdurch gleichzeitig nicht nur in das gewissermaßen „ausgelagerte Gehirn",[23] sondern in die Tiefen der Persönlichkeit eines Nutzers einzudringen. Das gilt insbesondere für die im Fokus der Ermittlungsbehörden stehenden Smartphones und andere mobilen Endgeräte (die es 2008 in der heutigen Form noch gar nicht gab). Es findet ein Zugriff auf Informationen statt, an denen die Zielperson der Maßnahme (und ebenfalls betroffene andere Personen, die das informationstechnische System mitnutzen) nicht einmal engste Vertraute teilhaben lassen würde. Die Erstellung eines allumfassenden Persönlichkeitsbildes – einschließlich der dem Betroffenen selbst nicht bewussten persönlichkeitsprägenden Merkmale – wird möglich.

Die ausnahmsweise Gestattung der (offenen!) Verwertung eines Tagebuchs zur Aufklärung einer besonders schweren Straftat wird nach hier geteilter Auffassung als „äußerste Grenze staatlicher Ausforschung der Intimsphäre"[24] angesehen. Die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung überschreiten diese Grenze bei weitem. Sie gestatten nicht nur die offene Verwertung höchstvertraulicher Informationen, sie erlauben gewissermaßen die dauerhafte heimliche Überwachung des Verfassens der Tagebucheinträge und dessen, was der Betroffene nicht einmal seinem Tagebuch anvertrauen würde.[25] Insbesondere die Online-Durchsuchung eröffnet, wie *Prantl* zutreffend formuliert, „die Möglichkeit, Gedanken auszulesen".[26]

Online-Durchsuchung und Quellen-TKÜ machen den Kernbereich privater Lebensgestaltung also denknotwendigerweise zum Ziel staatlicher Ausforschung und sind damit auszuschließen.[27] Es handelt sich bei beiden Eingriffsbefugnissen nicht lediglich um „verletzungsgeneigte Maßnahmen", sondern um Maßnahmen, denen eine Verletzung des Kernbereichs immanent ist. Es ist technisch nicht möglich, eventuelle nicht kernbereichsrelevante Informationen im Rahmen eines Zugriffs auszufiltern. Im Gegensatz zur Wohnraumüberwachung – bei der bestimmte Räumlichkeiten von der Überwachung ausgenommen werden können – besteht bei einer Online-Durchsuchung nur die Alternative von „ganz oder gar nicht".[28]

Können kernbereichsrelevante Daten vor oder bei der Datenerhebung nicht ausgesondert werden, ist nach dem *BVerfG* „ein Zugriff auf das informationstechnische System jedoch auch dann zulässig, wenn hierbei eine Wahrscheinlichkeit besteht, dass am Rande auch höchstpersönliche Daten miterfasst werden."[29] Hieraus folgt im Umkehrschluss, dass ein Zugriff auf informationstechnische Systeme dann nicht zulässig ist, wenn die Wahrscheinlichkeit besteht, dass nicht nur am Rande, sondern überwiegend höchstpersönliche Daten erfasst werden.

2. Maßnahmebezogene Verfassungsverstöße

Wollte man den grundlegenden Einwand eines Verstoßes gegen die Menschenwürde nicht teilen, sind die gesetzlichen Neuregelungen auch im Übrigen nicht mit der Verfassung vereinbar.

a) Online-Durchsuchung

aa) Unangemessenheit des Anlasstatenkatalogs in § 100b Abs. 2 StPO

Bei der verfassungsrechtlichen Bewertung der präventiven Online-Durchsuchung hat das *BVerfG* festgestellt, dass eine Rechtfertigung ausschließlich bei Vorliegen einer im Einzelfall drohenden Gefahr für ein „überragend wichtiges Rechtsgut" in Betracht gezogen werden könne (Leib, Leben und Freiheit der Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt).[30] Die mit einer repressiven Online-Durchsuchung verfolgten Anlasstaten müssten demnach von einem Gewicht sein, das mit den Anforderungen an die zu schützenden „überragend wichtigen Rechtsgüter" bei der präventiven Online-Durchsuchung korreliert. Voraussetzung für eine solche Vergleichbarkeit ist, unter Heranziehung der „Nagelprobe" von *Buermeyer*, dass „eine Online-Durchsuchung zur Verhinderung der entsprechenden Taten hätte vorgesehen werden dürfen".[31] Das ist bei der Regelung des § 100b Abs. 2 StPO nicht der Fall.[32] Der dort manifestierte Katalog von Anlasstaten knüpft erkennbar nicht ausschließlich an „überragend wichtige" Rechtsgüter an; enthalten sind eine Vielzahl von Straftatbeständen, zu deren Verhinderung eine präventive Online-Durchsuchung unzulässig wäre.

Exemplarisch sei hier die in § 100b Abs. 2 Nr. 1c StPO genannte „Geld- und Wertzeichenfälschung" genannt. Die §§ 146 ff. StGB dienen dem Schutz des Rechtsguts „Allgemeininteresse an der Sicherheit und Zuverlässigkeit des Geldverkehrs",[33] einem zweifellos nicht „überragend" wichtigem Rechtsgut. Auch der in § 100b Abs. 2 Nr. 1h StPO genannte Bandendiebstahl, die in § 100b Abs. 2 Nr. 1k StPO genannten Hehlereidelikte (Schutzgüter: Eigentum), die in § 100b Abs. 2 Nr. 1l StPO genannte Geldwäsche (Schutzgut: „die inländische Rechtspflege in ihrer Aufgabe, die Wirkung von Straftaten zu beseitigen")[34] oder die in § 100b Abs. 2 Nr. 1k genannten Straftatbestände der Bestechlichkeit bzw. Bestechung (Schutzgut: „Vertrauen in die Unkäuflichkeit von Trägern staat-

22 Beispielhaft sei auf die weit verbreitete Nutzung von Datingplattformen wie Tinder (vgl. https://de.statista.com/statistik/daten/studie/804638/umfrage/online-dating-nutzer-in-deutschland/) oder bei Gesundheitsfragen (https://de.statista.com/statistik/daten/studie/546285/umfrage/eingabe-von-krankheitssymptomen-in-suchmaschinen-nach-geschlecht-in-deutschland/) verwiesen.

23 So die Umschreibung von *Baum/Schantz*, ZRP 2008, 137, 138.

24 *Herdegen*, in: Maunz/Dürig, GG, 84. EL 2018, Art. 1 Abs. 1 Rn. 90.

25 Im Ergebnis ebenso *Roggan*, StV 2017, 821, 826 f., der die Maßnahme in ihrer Eingriffsintensität mit wiederholten heimlichen Hausdurchsuchungen vergleicht.

26 *Prantl*, Der Staatstrojaner ist ein Einbruch ins Grundgesetz, SZ v. 22. 06. 2017 – abrufbar unter: https://www.sueddeutsche.de/digital/ueberwachung-der-staatstrojaner-ist-ein-einbruch-ins-grundgesetz-1.3555917.

27 BVerfGE 121, 220, 278 – Rn. 125.

28 BVerfGE 121, 220, 306 – Rn. 218.

29 BVerfGE 121, 220, 307 – Rn. 220.

30 BVerfGE 120, 274, 326 ff. – Rn. 247.

31 Vgl. die Stellungnahme im „Gesetzgebungsverfahren" von *Buermeyer*, Stellungnahme zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, A-Drs. 18(6)334, S. 12; ebenso *Roggan*, StV 2017, 821, 827, zustimmend *Petri/Schwabenbauer*, in: Lisken/Denninger, Handbuch Polizeirecht, 6. Aufl. 2018, Teil G Rn. 635.

32 Vgl. auch *Singelnstein/Derin*, NJW 2017, 2646, 2647.

33 *Lackner/Kühl*, StGB, 29. Aufl. 2018, § 146 Rn. 1. Über § 151 StGB werden bestimmte Wertpapiere dem Geld gleichgestellt.

34 *Lackner/Kühl*, StGB, 29. Aufl. 2018, § 261 Rn. 1 unter Verweis auf BT-Drs. 12/989, S. 27.