Fredrik Roggan

Die Überwachung von IT-Systemen und das Wohnungsgrundrecht

Was Online-Durchsuchungen mit Wohnungsdurchsuchungen zu tun haben (können)

Wenn es um die Einführung digitaler Überwachungs- bzw. Ermittlungsbefugnisse geht, wird oft der Vergleich mit den Befugnissen in der analogen Welt gezogen – frei nach dem Motto: was an Überwachungsmöglichkeiten für die klassische Briefpost möglich war, muss auch für den Mailverkehr gelten. Gerade die Online-Durchsuchung von IT-Geräten zeigt jedoch, dass die digitalen Grundrechtseingriffe viel gravierender sein können, als dies in der „realen Welt" (zumindest der Bundesrepublik) jemals zulässig war. Fredrik Roggan verdeutlicht dies im folgenden Beitrag anhand des heimlichen Zugriffs auf den Wohnraum, der zur Umsetzung von Online-Durchsuchungen manchmal technisch notwendig scheint.

I. Einleitung

Wenn eine Sicherheitsbehörde sich den Zugriff auf ein Tagebuch verschaffen möchte, das sich in einer Wohnung befindet, so bedarf es zunächst des Betretens dieser Räumlichkeit, ihrer Durchsuchung und schließlich des physischen Zugriffs zwecks späterer Inaugenscheinnahme. Keinerlei Zweifel besteht daran, dass dieses Vorgehen mit einem Eingriff in das *Grundrecht auf Unverletzlichkeit der Wohnung* (Art. 13 Abs. 1 GG) verbunden ist.

Möchte dieselbe Sicherheitsbehörde einen in demselben Raum befindlichen Computer oder auch ein Smartphone im Rahmen einer Online-Durchsuchung heimlich überwachen, so ist nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) das Wohnungsgrundrecht nicht ohne weiteres (dazu aber im Folgenden) betroffen, weil der Zugriff auf die darauf gespeicherten Informationen unabhängig von seinem Standort erfolgen kann. Ein raumbezogenes Grundrecht wie Art. 13 Abs. 1 GG vermag die spezifische Gefährdung solcher Daten durch staatliche Ermittlungsmaßnahmen nicht abzuwehren. Diesen Umstand nahm das BVerfG zum Anlass, das *Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme* (kurz: IT-Grundrecht) aus der Taufe zu heben.[1]

Auf den allerersten Blick haben die Zugriffe auf das eingangs genannte Tagebuch sowie derjenige auf den Computer also keinerlei grundrechtliche Schnittmenge. Diese Perspektive ändert sich jedoch schnell, wenn das (heimliche) Auslesen des informationstechnischen Systems nur dadurch möglich wird, indem zur Vorbereitung dieser Maßnahme ein physischer Zugriff auf das Gerät erfolgen muss. Dieses Problem wird in der bereits angeführten Rechtsprechung des BVerfG auch bereits angesprochen: Wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren, ist das Wohnungsgrundrecht unzweifelhaft betroffen. Ein weiterer Anwendungsfall des Art. 13 Abs. 1 GG wäre die Infiltration eines informationstechnischen Systems, das sich in einer Wohnung befindet, um mit Hilfe dessen bestimmte Vorgänge innerhalb der Wohnung zu überwachen, etwa indem die an das System angeschlossenen Peripheriegeräte wie ein Mikrofon oder eine Kamera genutzt werden.[2] Im ersten Fall ist das Wohnungsgrundrecht lediglich in der Vorbereitung der Ermittlungsmaßnahme betroffen, im zweiten auch im Rahmen der Durchführung.

Ganz offensichtlich kann der physische Zugriff auf zu überwachende informationstechnische Systeme also mit Eingriffen in das Wohnungsgrundrecht verbunden sein. Oder mit anderen Worten: In allen Fällen, in denen es den ermittelnden Personen nicht gelingt, auf das informationstechnische System außerhalb einer dem Wohnungsgrundrecht unterfallenden Räumlichkeit zuzugreifen, muss dieser Zugriff eben innerhalb einer Wohnung (wozu auch Betriebs- und Geschäftsräume zählen) erfolgen. Deshalb können Maßnahmen der Online-Durchsuchung (und übrigens auch der nicht näher thematisierten Quellen-TKÜ) sehr wohl eine Schnittmenge von Wohnungs- und IT-Grundrecht besitzen. Für beide Eingriffe gilt es, verfassungskonforme gesetzliche Regelungen zu finden. Dies ist bislang auf der Ebene des Bundesrechts überhaupt noch nicht der Fall, auf Landesebene lediglich sehr vereinzelt.

II. Zur Bedeutung des physischen Zugriffs

Für eine Online-Durchsuchung informationstechnischer Systeme wird eine spezielle Überwachungssoftware („Trojaner“) benötigt. Über deren technische Details und Funktionsweise ist kaum etwas bekannt, es handelt sich um ein gut geschütztes Geheimnis. Das gilt nicht nur für die Überwachungssoftware als solche, sondern auch für die Frage, auf welche Weise ein auszuspähendes IT-System infiltriert werden kann. Diese Geheimhaltung ist folgerichtig, weil beispielsweise das Bekanntwerden der Funktionsweise bzw. technisch-spezifischen Eigenschaften des Trojaners seinen Einsatz gefährden oder sogar verhindern könnte.[3] Beispielsweise ließen sich IT-Systeme wirksam schützen, indem die Überwachungssoftware von den zu infiltrierenden Systemen anhand spezifischer Merkmale erkannt würde. Wer ein solches technisches Mittel einsetzen will, muss es vor der öffentlichen Aufmerksamkeit also bestmöglich schützen.

Unabhängig davon ist freilich bekannt, dass Überwachungsmaßnahmen in der Vergangenheit stets dadurch vorbereitet wurden, dass auf die IT-Systeme hardwaremäßig zugegriffen wurde, die Ermittler das Gerät also zumindest kurzfristig „in den Hän-

den“ hielten. Dagegen scheint eine rein softwaremäßige Infiltration (etwa per Email-Anhang) nicht Erfolg versprechend zu sein. Dies dürfte vor allem auch daran liegen, dass der Kreis der möglichen Betroffenen regelmäßig für denkbare Überwachungsmaßnahmen sensibilisiert sein dürfte.[4]

In der Vergangenheit bedienten sich Ermittlungsbehörden kriminalistischer List, etwa indem das Aufspielen der Überwachungssoftware auf ein Handy während einer Grenzkontrolle ermöglicht wurde.[5] Freilich wird sich auch dieses Verfahren in den einschlägigen Kreisen zwischenzeitlich herumgesprochen haben, so dass beispielsweise ein – wenn auch nur kurzzeitig – aus den Augen verlorenes Smartphone als „verbrannt“ betrachtet werden dürfte. Damit stellt sich aus der Sicht von Ermittlungsbehörden die Frage, wie Online-Durchsuchungen überhaupt noch vorbereitet werden können. Spätestens dann geraten diejenigen Räumlichkeiten ins „Visier“, in denen sich die zu infiltrierenden technischen Geräte zeitweise unbeaufsichtigt befinden.

III. Zur Rechtfertigung von Eingriffen in das Wohnungsgrundrecht

Soll auf ein IT-System unbemerkt zugegriffen werden, das sich in einer von Art. 13 Abs. 1 GG geschützten Räumlichkeit befindet, so ist hierfür sowohl ein Betreten als auch ein Durchsuchen dieser Räume erforderlich. Hiermit verbunden ist regelmäßig eine intensive Inaugenscheinnahme der räumlichen Sphäre. Die mit der Vorbereitung einer Online-Durchsuchung betrauten Personen werden sich in diesem Zusammenhang einen ebenso umfassenden Überblick über die betroffene Wohnung verschaffen müssen, wie dies bei einer offen durchgeführten Durchsuchung der Fall ist. Um den Maßnahmezweck nicht zu gefährden, werden sie freilich darauf achten müssen, keine registrierbaren Veränderungen zu hinterlassen. Solche verdeckten bzw. heimlichen Wohnungsdurchsuchungen kommen zu jeder Tages- und Nachtzeit in Betracht und sind selbst bei anwesenden Bewohnern denkbar. Dass letzteres keineswegs abwegig ist, ergibt sich aus dem Umstand, dass manche IT-Systeme überhaupt nur „unbewacht“ sind, wenn ihre Besitzer*innen schlafen.

Es liegt auf der Hand, dass heimliche Wohnungsdurchsuchungen noch intensiver in das Wohnungsgrundrecht der Betroffenen eingreifen, als dies bei einer offenen Durchführung der Fall ist. Die dabei gewonnenen Einblicke können bereits für sich genommen tief in das Privat- oder sogar Intimleben der Betroffenen hineinreichen – selbst dann, wenn das Erlangen dieser Erkenntnisse nicht der primäre Zweck einer solchen Maßnahme wäre bzw. sein dürfte. Damit ist die Frage zu beantworten, ob das Grundgesetz heimliche Wohnungsdurchsuchungen überhaupt zulässt – unabhängig davon, zu welchem Zweck diese erfolgen.

In den Blickpunkt gerät damit die Grundrechtsschranke in Art. 13 Abs. 2 GG, wonach Durchsuchungen nur durch den Richter, bei Gefahr im Verzuge auch durch die in den Gesetzen vorgesehenen anderen Organe angeordnet und nur in der dort vorgeschriebenen Form durchgeführt werden dürfen. Aber kann eine Durchsuchung im Sinne dieser Verfassungsnorm auch eine *verdeckte* Durchsuchung sein?

Das BVerfG hatte sich mit dieser Frage bislang nicht zu befassen, sondern kontrollierte bis dato lediglich die Verfassungsmäßigkeit von offen durchgeführten Maßnah-

men. In der (Kommentar-)Literatur zu Art. 13 GG wird einhellig angenommen, dass im Grundgesetz für den Begriff der Durchsuchung die *ausnahmslose Offenheit* des staatlichen Eingriffs kennzeichnend ist. Dies ergibt sich aus den dortigen Ausführungen entweder explizit[6] oder lässt sich implizit aus exemplarischen Besprechungen einzelner Maßnahmen folgern.[7] Die Offenheit der in die Privatheit der Betroffenen tief eingreifenden Maßnahme soll jene in den Stand versetzen, die Durchsuchung zu kontrollieren und etwaigen Ausuferungen im Rahmen ihrer rechtlichen Möglichkeiten von vornherein entgegenzutreten.[8] Folgt man dieser Auffassung und damit gleichsam dem Verfasser, so sind heimliche Wohnungsdurchsuchungen selbst dann verfassungswidrig, wenn ein Gesetz diese Art der Durchführung explizit erlaubt.

Ohne das an dieser Stelle vertiefen zu können, sind damit sämtliche Regelungen in den Ländern, die verdeckte Wohnungsdurchsuchungen in der Vorbereitungsphase von Online-Durchsuchungen (und Quellen-Telekommunikationsüberwachungen!) gestatten, unvereinbar mit den im Grundgesetz zugelassenen Beschränkungen des Wohnungsgrundrechts. In Bayern etwa sind solche Maßnahmen sowohl im Zusammenhang mit der Durchführung einer Online-Durchsuchung (vgl. Art. 45 Abs. 3 S. 5 BayPAG) als auch einer Quellen-TKÜ (vgl. Art. 44 Abs. 1 Satz 5 BayPAG) vorgesehen.

Auf Bundesebene existieren entsprechende Regelungen weder im Strafverfahrens- noch im Polizeirecht. Der Bundesgesetzgeber hat sich bisher also dafür entschieden, heimliche Wohnungsdurchsuchungen nicht zuzulassen.

IV. (Ausgerechnet) Das Geheimdienstrecht als bundesrechtlicher „Vorreiter"?

Im Sommer 2019 kursierte ein Entwurf für ein Gesetz zur „Harmonisierung des Verfassungsschutzrechts" in der Öffentlichkeit.[9] In ihm war eine Regelung enthalten, wonach das Bundesamt für Verfassungsschutz eine Wohnung (auch) heimlich *betreten* werden darf, u.a. um eine Online-Durchsuchung (und wiederum auch eine Quellen-TKÜ) vorzubereiten (§ 9e Abs. 6 BVerfSchG-E). Dies trug dem Geheimdienst in der aufmerksam gewordenen Medienöffentlichkeit den vorläufigen Titel eines „*Bundesamt(s) für Einbruch*" ein.[10]

Tatsächlich beträte das Geheimdienstrecht mit einer solchen – nach dem oben Gesagten: verfassungswidrigen! – Befugnis Neuland. Was der Polizei weder im Rahmen von Strafverfolgung noch von Gefahrenabwehr gestattet ist, soll einer Behörde erlaubt werden, die nach dem Verständnis des BVerfG nicht einmal als Sicherheitsbehörde zu betrachten ist.[11]

Dem Verdikt der Verfassungswidrigkeit würde eine solche Befugnis auch nicht dadurch entgehen, dass es den Eingriff in das Wohnungsgrundrecht auf ein „Betreten" beschränkt. Hierunter wird im Allgemeinen das Eintreten in eine fremde Wohnung und das Verweilen darin (ohne die Einwilligung des Berechtigten) und die schon auf diese Weise mögliche Kenntnisnahme von Personen, Sachen und Zuständen verstanden.[12] Die Regelung ergibt erst dadurch einen vollständigen Sinn, wenn der Zutritt für die Geheimdienstmitarbeiter mit der gezielten Suche nach einem zu infiltrierenden IT-System verbunden ist, beispielsweise also Schubladen, Schränke etc. geöffnet und damit in näheren Augenschein genommen werden dürfen. Unabhängig davon wäre

eine Beschränkung der Maßnahme auf das bloße Eintreten und Verweilen auch kaum zu kontrollieren. Es wurde deshalb zu Recht der Vorwurf erhoben, dass der Entwurf (auch deswegen, weil er zahlreiche Schachtelsätze enthält) den Regelungsgehalt absichtsvoll verschleiere.[13] Dies freilich entspräche einer Doktrin der Hausleitung des Bundesinnenministeriums, wonach man brisante Verschärfungen von Sicherheitsgesetzen am effektivsten auf den Weg bringe, indem man das Gemeinte nicht explizit anspreche: „*Dann fällt es nicht so auf*".[14] Indessen: In diesem Fall fiel der Plan auf.

Nachdem von Seiten eines Koalitionspartners Kritik an dem Gesetzesvorhaben geäußert wurde, wurde der Entwurf im Sommer 2019 nicht mehr in den Bundestag eingebracht.[15]

V. Ein kurzer rechtspolitischer Schluss

In der DDR war es nach §§ 20 Abs. 2 i.V.m. 14 des Volkspolizei-Gesetzes vom 11. Juni 1968[16] u.a. auch den Angehörigen des Ministeriums für Staatssicherheit unter bestimmten, präventiv-polizeilich geprägten Gründen das (allerdings: nur) *Betreten* von Grundstücken, Wohnungen und anderen Räumen auch *ohne Wissen* des Wohnungsinhabers gestattet. Unter einem Betreten wurde seinerzeit „*jedes Eintreten oder gewaltsame Zugangverschaffen (...) in Wohnungen*" verstanden.[17] Die Gesetzgeber in Bund und Ländern sollten sehr grundsätzlich wägen, wie viel Nähe zu einer solchen Rechtslage der bundesrepublikanische Rechtsstaat verträgt.

PROF. DR. FREDRIK ROGGAN ist Professor für Strafrecht an der Hochschule der Polizei des Landes Brandenburg und war viele Jahre lang im Bundesvorstand der Humanistischen Union aktiv.

Anmerkungen:

1 BVerfGE 120, 274 (302 ff.).
2 BVerfGE 120, 274 (310).
3 Vgl. dazu VG Wiesbaden, Urt. v. 4.9.2015 – 6 K 687/15.WI, Rn. 38 – juris.
4 Meyer-Goßner/Schmitt/*Köhler*, StPO, 62. Aufl. 2019, § 100a Rn. 14d.
5 Vgl. etwa *Braun/Roggenkamp*, K&R 2011, S. 681.
6 Bonner Kommentar zum GG/*Herdegen*, 71. Lfg. (Oktober 1993), Art. 13 Rn. 52; *Wolff*, in: Hömig/Wolff, GG, 12. Aufl. 2018, Art. 13 Rn. 9; *Gornig*, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 13 Rn. 64 („Betriebsinhaber [eines Geschäftsraums ist] zu informieren").
7 Vgl. dazu *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Hennecke, GG, 14. Aufl. 2018, Art. 13 Rn. 11; *Ja-*

rass, in: Jarass/Pieroth, GG, Art. 13 Rn. 14; *Kunig*, in: v. Münch/Kunig, GG, 6. Aufl. 2012, Art. 13 Rn. 26 f.

8 *Papier*, in: Maunz/Dürig, GG, Lfg. 71 (März 2014), Art. 13 Rn. 28.

9 *Meister/Biselli*, https://netzpolitik.org/2019/wir-veroeffentlichen-den-gesetzentwurf-seehofer-will-staatstrojaner-fuer-den-verfassungsschutz/.

10 *Steinke*, Süddeutsche Zeitung v. 16.8.2019, S. 6.

11 Vgl. BVerfGE 133, 277 (327).

12 Vgl. nur *Graulich*, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Kap. E Rn. 618.

13 *Steinke*, Süddeutsche Zeitung v. 16.8.2019, S. 4.

14 Zitiert nach *Steinke*, Süddeutsche Zeitung v. 16.8.2019, S. 4.

15 Vgl. dazu *v. Behring*, https://netzpolitik.org/2019/einbrechen-fuer-staatstrojaner-verfassungsschutz-soll-mehr-befugnisse-erhalten-als-bisher-gedacht/

16 GBl. I Nr. 11 S. 232.

17 *Surkau/Korlek/Petasch/Garbe*, Pflichten und Befugnisse des Volkspolizisten zur Gewährleistung der öffentlichen Ordnung und Sicherheit, 6. Aufl. 1989, S. 75.