LKV

3 | 22 32. Jahrgang, Seiten 97 - 144

Landes- und Kommunalverwaltung

Verwaltungsrechts-Zeitschrift
für die Länder Berlin | Brandenburg | Sachsen | Sachsen-Anhalt | Thüringen

Redaktionsanschrift: LKV – Landes- und Kommunalverwaltung, Hauptschriftleitung, Konrad-Zuse-Ring 12A, 14469 Potsdam
E-Mail: lkv@nomos.de, **Internet:** www.lkv.nomos.de

Grundrechtseingriffe bei einem hoheitlichen Einsatz von Drohnendetektions-Systemen

Professor Dr. Peter Hantel und Gabriele Heinze-Mayer, beide Wildau

Zur Prävention und Bekämpfung von Terrorismus fördert das Bundesministerium für Bildung und Forschung im Rahmen des Programms „Forschung für die zivile Sicherheit" zehn Verbundprojekte, darunter auch vier Projekte zur Abwehr unbemannter Flugsysteme.[1]

A. Drohnendetektions-Projekte an der Technischen Hochschule Wildau

Die Technische Hochschule Wildau wurde bei einem Teil der Projekte[2] mit der logistischen Umsetzung von Drohnendetektions-Systemen und der juristischen Begleitforschung beauftragt. In diesem Rahmen wurden auch mögliche Beeinträchtigungen von Grundrechten beim Betrieb entsprechender Anlagen thematisiert, deren Ergebnisse in diesem Beitrag komprimiert dargestellt werden.

I. Technische Voraussetzungen für eine Detektion von Drohnen

Bei den von der TH Wildau begleiteten Projekten ORAS und ADIS handelt es sich um Entwicklung und Einsatz mobiler und statischer Geräte in Koffergröße mit Antenne und Laptop zwecks Erfassung der Daten von Flugobjekten. Verbunden sind diese Geräte mit Radarsensoren, die auf festen Objekten angebracht werden können und die ihrerseits bis zu einer Entfernung von 100 Metern senden und empfangen können und ihre Daten an das mobile Gerät übermitteln.

Mittels der Radarsensoren kann

a) die Drohne erfasst und ihre Konfiguration und der Flugplan analysiert werden,

b) eine Übernahme der Cockpit-Sicht (First-Pilot-View) der Drohne ermöglicht werden,

c) die Frequenz erfasst werden, auf der die Drohne gesteuert wird.

Damit waren die genannten Projekte, abgesehen von dem oben genannten First-Pilot-View, vorrangig rein passive Monitoring-Systeme. Die Systeme nehmen daher keinen gezielten Einfluss auf die Steuerung der Drohne und können auch nicht anzeigen, von wo gestartet wurde. Mithin ist auch der Standort des Drohnen-Steurers nicht zu ermitteln.

1 Vgl. zur Geschichte des unbemannten Fliegens: Giemulla/van Schyndel/Friedl, Gewerblicher und privater Einsatz von Drohnen, 2018, S. 1, 2; ferner Grosskopf, CR 2014, 759; Daum/Boesch, CR 2018, 62; Steiger, Sicherheit und Recht 2014, 165.

2 Es handelt sich bei den Projekten um das sog. ORAS-Projekt (Akronym für Sensorgestütztes Überwachungs- und Alarmierungssystem zur Detektion und Verfolgung unbemannter Flugsysteme) und das sog. ADIS-Projekt (Akronym für Automatisiertes Drohnen-Informationssystem).

Da es sich bei den von der TH Wildau begleiteten Projekten vorrangig um rein passive Monitoring-Systeme handelte, steht in der nachfolgenden Untersuchung die Vereinbarkeit rein passiver Detektionsmaßnahmen[3] und weniger aktiver Maßnahmen[4] mit den Grundrechten im Vordergrund. Gleichwohl erfolgen auch ergänzende Ausführungen, zur Vereinbarkeit von aktiven Abwehrmaßnahmen bis zum Abschuss und Zerstörung einer Drohne mit den Grundrechten.

II. Rechtliche Implikationen bei der technischen Detektion von Drohnen

Die Erfassung von Drohnen erfolgt in drei Stufen: Als Erstes gilt es, die Drohne zu entdecken, was angesichts der u.U. hohen Geschwindigkeit der Flugobjekte und des begrenzten Erkennungsradius' der Sensortechnik eine technische und logistische Herausforderung darstellt. Im zweiten Schritt gilt es zu erkennen, um welchen Typ Drohne es sich handelt und ob sie überhaupt eine Gefahr darstellt.[5] Sofern das Flugobjekt als gefährliche Drohne erkannt wurde, die beispielsweise illegale Filmaufnahmen macht oder gar für einen Anschlag benutzt werden soll, muss als dritte Stufe jede Gegenmaßnahme, unter Beachtung dessen was technisch möglich und juristisch zulässig ist, abgewogen werden.[6]

Eingriffe in Grundrechte können damit verbunden sein, wenn Personen optisch, akustisch oder in sonstiger Weise erfasst werden. Ferner könnten die dargestellten technischen Maßnahmen der Detektions-Systeme die elektromagnetischen Steuerungsmöglichkeiten der Drohne beeinflussen und damit ebenfalls von Grundrechtsrelevanz sein.[7] Gleiches gilt für die mögliche Ermittlung des Standorts des Steuerers sowie für die harten Abwehrmaßnahmen bis zum Abschuss einer Drohne.[8]

Schließlich ergibt sich eine spezielle Eingriffsproblematik im Zusammenhang mit sog. Geofencing-Maßnahmen.[9] Entsprechende Maßnahmen enthalten die Verpflichtung der Drohnenhersteller, ihre Drohnen mit einem Geofencing-System auszustatten. Für die Hersteller würde sich die Verpflichtung zur Vorprogrammierung der Drohnensoftwaresysteme ergeben.[10]

B. Die möglicherweise betroffenen Schutzbereiche der Grundrechte

Nachfolgend werden die jeweiligen Grundrechte dargestellt, deren Schutzbereiche durch die dargestellten technischen Maßnahmen der Detektions-Systeme berührt sein können. Der Schwerpunkt liegt dabei wie ausgeführt auf der reinen Erfassung einer Drohne und der Beeinflussung ihrer Steuerung.

1. Recht auf informationelle Selbstbestimmung

Als betroffenes Grundrecht kommt zunächst das Recht auf informationelle Selbstbestimmung nach Art. 2 I, Art. 1 I GG im Falle der Erfassung unbeteiligter Dritter in Betracht. Dieses Recht trägt Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich für den Einzelnen – insbesondere unter den Bedingungen moderner Datenverarbeitung – aus informationsbezogenen Maßnahmen ergeben.[11] Es flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatfreiheit. Ein solcher Eingriff ist auch nicht dadurch ausgeschlossen, dass technische Einrichtungen möglicherweise automatisch reagieren und ggf. kommunizieren. Auch der Datenaustausch und die Datenweitergabe von technischen Einrichtungen können einen Eingriff darstellen, sofern es willensgesteuert zu entsprechenden Reaktionen und Maßnahmen kommt.[12]

Sofern eine Drohne ohne Rückschluss auf den Steuerer erfasst wird, dürfte ein Eingriff in das Recht auf informationelle Selbstbestimmung nicht vorliegen. Dies ist insbesondere dann der Fall, wenn die Drohne im Widerspruch zu den gesetzlichen Regelung[13] nicht gekennzeichnet und damit

3 Bei der Drohnenabwehr wird zwischen passiven und aktiven Maßnahmen, bei letzteren zwischen weichen oder harten Methoden unterschieden. Passive Maßnahmen beschränken sich zum Beispiel darauf, einen Alarm auszulösen. Aktive Maßnahmen sind eine Herausforderung für Mensch und Technik, denn jeder Eingriff ist heikel und muss rechtlich genau abgewogen werden. Zu den weichen Maßnahmen gehört das sogenannte „Jammen", bei dem Störsignale die Funkverbindung zur Drohne abreißen lassen, um sie so zur Landung zu zwingen. Das funktioniert nur, wenn sie für solch einen Fall zur Landung programmiert ist. Die Gefahr besteht, dass die Drohne unkontrolliert weiterfliegt und abstürzt. Beim „Spoofing" hingegen wird der Drohne ein falsches GPS-Signal vorgegaukelt, um sie so von ihrem Kurs abzubringen. Vgl.u.a. Marosi/Skobel, CR 2019, 65; Daum/Boesch, CR 2018, 62; Solmecke/Nowak, MMR 2014, 431.

4 Als weitere harte Abwehr wird das physische Abfangen oder Abschießen der Drohne bezeichnet. Ein derartiger Eingriff wird nur als Ultima Ratio eingesetzt, da unbeteiligte Personen gefährdet werden könnten. Die Methodenauswahl ist groß: Abschießen mittels Laser, Wasserwerfer oder mit der Schusswaffe, Kamikazedrohnen oder Einsatz eines Fangnetzes stören. Vgl. hierzu Solmecke/Nowak, MMR 2014, 431; ferner Josipovic, NVwZ 2019, 438; Kettiger, Jusletter.ch, 11. 4. 2016.

5 Vielleicht ist das Objekt, das so bedrohlich surrend über dem Starterfeld des City-Marathons schwebt, ja nur die Kameradrohne des lokalen TV-Senders.

6 Um welches Modell handelt es sich? Wie schnell ist die Drohne? Welche Nutzlast trägt sie? Auf welcher Funkfrequenz wird sie gesteuert? All diese Analysen und Informationen müssen nahezu in Echtzeit zur Verfügung stehen, denn im Ernstfall bleiben oftmals nur wenige Sekunden, um die richtige Entscheidung zu treffen und eine geeignete Gegenmaßnahme zur Abwehr einzuleiten.

7 Zu nennen wäre die Störung von Funksignalen oder die Übernahme der Steuerung. Das Aussenden von Radar- oder Funksignalen mit dem Ziel der Ablenkung der Drohne wird als sog. Jammen bezeichnet; vgl. Daum/Boesch, CR 2018, 62; Marosi/Skobel, CR 2019, 65.

8 Zu Rechtsfragen bei der Ermittlung des Standortes des Steuerers vgl. Daum/Boesch, CR 2018, 62; ferner Marosi/Skobel, CR 2019, 65.

9 Vgl. Daum/Boesch, CR 2018, 62 (63) sowie 130; Vgl. zu Drohnenverbotszonen auch grundlegend die sog. U Space Verordnung (EU) 2019/945 sowie die Durchführungsverordnung 2021/664.

10 Durch Geofencing-Maßnahmen könnten Luftbereiche gewissermaßen durch virtuelle Zäune umschlossen werden, so dass Drohnen nicht in der Lage wären über die abgegrenzten Bereiche, z.B. von Atomkraftwerken, Gefängnissen oder sonstigen sensiblen Räumen einzufliegen. Die entsprechende Verpflichtung gegenüber Herstellern würde einen Grundrechtseingriff in die unternehmerische Freiheit darstellen, der einer ausreichenden Rechtsgrundlage bedarf. Die technische Ausweisung von Flugverbotszonen mit entsprechender funktechnischer Unterstützung durch Hoheitsträger dürfte für sich gesehen aber noch keinen Eingriff darstellen.

11 Vgl. BVerfGE 65, 42; 115, 341; Marosi/Skobel, DVBl 2019, 678.

12 Vgl. BVerfG vom 6. 7. 2016 – 2 BvR 1454/13, Rn. 38, Fundstelle?.

kein sofortiger Rückschluss auf den Steuerer möglich ist. Gleiches gilt auch für Maßnahmen zur Ermittlung der Funkfrequenz, auf der die Drohne ferngesteuert wird. Bei der bloßen Identifizierung einer Drohne handelt es sich im Grunde um die Erfassung von Sachdaten und nicht um personenbezogenen Daten.[14]

Desweiterem fehlt es nach der Rechtsprechung des BVerfG[15] auch an der Eingriffsqualität, sofern Daten ungezielt und allein technisch bedingt zunächst mit erfasst, aber unmittelbar nach der Erfassung technisch wieder anonym, spurlos und ohne Erkenntnis für die Behörde ausgesondert werden. Dies ist dann der Fall, wenn eine Drohne nur kurz erfasst und vom System als ungefährlich identifiziert und die Daten wieder gelöscht werden.

Erst wenn mittels Fotos oder sonstiger Maßnahmen der Steuerer oder unbeteiligte Personen identifiziert werden können, ist das Recht auf informationelle Selbstbestimmung betroffen, so dass es auf die verfassungsrechtliche Rechtfertigung ankommt. Insbesondere wenn es sich nicht lediglich um Echtzeitaufnahmen, sondern um gespeicherte Aufnahmen handelt, die die Person erkennen lässt, läge ein Eingriff vor.[16]

2. Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

Dieses vom BVerfG aus Art. 2 I, Art. 1 I GG[17] entwickelte Grundrecht soll Schutz vor Eingriffen mit technischen Mitteln in oder von Betroffenen genutzten informationstechnischen Systemen gewähren. Da der Zugriff auf das System (z. B. durch sog. Staats-Trojaner) einen Einblick in wesentliche Teile der Lebensgestaltung der Person ermöglicht, ist ein entsprechender Eingriff nur zum Schutz überragend wichtiger Gemeinschaftsgüter (vor allem schwerer Straftaten) zulässig.[18]

Das bloße Erfassen einer Drohne würde noch keinen Eingriff in dieses Grundrecht darstellen. Es fehlt an der erforderlichen staatlichen Manipulation von informationstechnischen Systemen. Sofern aber durch den Betrieb des Detektions-Systems in die Verbindung zwischen Bodenstation und Drohne eingegriffen wird,[19] könnte der Schutzbereich des vorgenannten Grundrechts tangiert sein. Ziel dieser Maßnahmen wäre es, die Sensoren der Drohne ohne Kenntnis des Steuerers so zu manipulieren, dass sie nicht mehr von der Bodenstation gesteuert werden kann oder sie nicht in bestimmte Flugverbotszonen nach den §§ 21 a bis h LuftVO einfliegt, vergleichbar den Geofencing-Maßnahmen.

Nach der gegenwärtigen Rechtslage wäre eine solche Maßnahme zur Aufklärung besonders schwerer Straftaten nach § 100 a I Nr. 3 S. 2, § 100 b StPO oder nach Landespolizeirecht zur Abwehr einer dringenden Gefahr für Leib, Leben und Freiheit einer Person (§§ 33 a,b, BbgPolG) zulässig[20]

3. Fernmeldegeheimnis nach Art. 10 I GG

Sofern die Funksignale zur Steuerung der Drohne gestört oder verändert werden, könnte sodann ein Eingriff in das Fernmeldegeheimnis nach Art. 10 I GG vorliegen. Geschützt ist die Vertraulichkeit der individuellen Kommunikation zwischen Personen, die sich wegen der räumlichen Distanz eines Übermittlungsmediums bedienen müssen. Erforderlich ist also die Weitergabe kommunikationsbezogener Daten.[21]

Die durch Fernsteuerung ausgesandten Funksignale vom Steuerer zur Drohne können allerdings nicht als kommunikationsbezogener Vorgang bewertet werden. Das Fernmeldegeheimnis nach Art. 10 I GG soll vorrangig die Vertraulichkeit des Kommunikationsvorgangs schützen, die bei der Steuerung einer Drohne nicht betroffen ist. Bei einer solchen Steuerung geht es nicht um die Weitergabe vertraulicher Daten, sondern um die Steuerung bzw. Lenkung einer Maschine mittels Funksignalen. Art. 10 I GG schützt nicht die Steuerung bzw. Lenkung einer Maschine durch Funksignale.

Insoweit würde weder die Ermittlung der Funkfrequenz, auf der die Drohne gesteuert wird, noch die Unterbrechung der Funkverbindung oder die Übernahme der Steuerung durch Hoheitsträger einen Eingriff in Art. 10 I GG darstellen.

Erst recht kann nicht von einem Eingriff ausgegangen werden, wenn festgestellt wird, dass die Drohne autonom fliegt und auch autonom von einer Drohnendetektionsanlage erfasst wird. Der bloße Datenaustausch zwischen selbständig agierenden technischen Geräten oder Anlagen stellt – wie oben schon ausgeführt – keinen Eingriff in das Fernmeldegeheimnis dar.[22] Daher stellt die Erfassung einer autonom fliegenden Drohne und die damit einhergehende technische Ermittlung einer fehlenden Funkfrequenz keinen Eingriff in das vorgenannte Grundrecht dar.

4. Meinungs- und Informationsfreiheit nach Art. 5 I GG

Gleiches gilt für einen möglichen Eingriff in das Grundrecht der Meinungs- und Informationsfreiheit nach Art. 5 I GG. Durch das mögliche Aussenden elektromagnetischer Wellen wird nicht der Austausch von Meinungen und Informationen, sondern lediglich die technische Steuerung und Len-

13 Vgl. hier,§ 19 III LuftVZO,§ 21 h LuftVO.

14 Vgl. zur Unterscheidung Sachdaten und personenbezogene Daten Krügel, ZD 2017,459; Forgo/Krügel, MMR 2010,17, Josefin Neumann Bachelorarbeit TH Wildau 2020, S. 63-68.

15 Vgl. BVerfG vom 18. 12. 2018 – 1 BvR 142/15, NJW 2019, 827; 1 BvR 2795/09, 1 BvR 3187/10, NJW 2019, 842.

16 Entsprechende Maßnahmen könnten gegenüber unbeteiligten Personen nur unter Beachtung der Grundsätze über die Inanspruchnahme von Nichtstörern verfügt werden; Vgl. Götz, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl. (2008), S. 76 ff; Schenke, Polizei- und Ordnungsrecht, 6. Aufl. (2009), Rn. 310 ff; Knemeyer, Polizei- und Ordnungsrecht, 11. Aufl. (2007), Rn. 347 ff.

17 Vgl. BVerfGE 120, 274 (308, 309).

18 Vgl. BVerfGE 120, 274 (308, 309).

19 Vgl. Hänsenberger, Diss. Universität St. Gallen, 2018, S. 25, 26.

20 Vgl. zur sog. Quellen-TKÜ und zum Eingriff in informationstechnische Systeme: BVerfGE 106, 37; 115, 186; 124, 43; ferner Köhler, in: Meyer-Goßner/Schmitt, StPO, 62. Aufl. (2019), § 100 a, Rn. 14 a – 14 m.

21 Vgl. BVerfG vom 22. 8. 2006 – 2 BvR 1345/03, NJW 2007, 351 sowie vom 6. 7. 2016 – 2 BvR 1454/13, NJW 2016, 3508.

22 Vgl. zum fehlenden Eingriff in die Telekommunikation nach § 100 a StPO beim bloßen Datenaustausch zwischen digitalen Endgeräten: Meyer-Goßner/Schmitt (o.Fußn. 20), § 100 a, Rn. 14 f.

kung einer Drohne beeinträchtigt. Die ungehinderte Steuerung oder Lenkung von Maschinen mittels elektromagnetischer Wellen fällt aber nicht in den Schutzbereich von Art. 5 I GG.

5. Versammlungsfreiheit nach Art. 8 I GG

Schließlich kann der Einsatz von stationären oder mobilen Drohnendetektionssystemen im Zusammenhang mit Versammlungen Art. 8 I GG tangieren. Danach wird allen Deutschen das Recht garantiert, sich friedlich und ohne Waffen zu versammeln. Der Einsatz eines Detektionssystems im Zusammenhang mit Versammlungen unter freiem Himmel könnte als faktischer Eingriff[23] in Art. 8 I GG gewertet werden. Die Möglichkeit der Erfassung von Personen anhand von Aufnahmen kann mit einer einschüchternden oder abschreckenden Wirkung auf Teilnehmer einer Demonstration verbunden sein, die die Entschließungsfreiheit an Versammlungen teilzunehmen, beeinträchtigt.[24] Personen werden seltener an einer Versammlung teilnehmen, wenn sie befürchten müssen, optisch erfasst zu werden.

Allerdings ist der Einsatz von Drohnenabwehrsystemen nicht vergleichbar mit Filmaufnahmen von Demonstrationsteilnehmern nach §§ 12 a, 19 a VersG, bei denen gezielt gewalttätige Demonstranten identifiziert werden sollen Das eigentliche Ziel der Drohnendetektion ist die Erfassung von Drohnen und nicht von Personen. Selbst wenn man der bloßen Möglichkeit einer zufälligen Erfassung unbeteiligter Dritter eine Eingriffsqualität zurechnen will, wäre die abschreckende Wirkung doch eher unbedeutend, so dass auch nicht von einem faktischen Eingriff in Art. 8 I GG ausgegangen werden kann.

6. Eingriffe in Leib, Leben und Gesundheit nach Art. 2 II 1 GG und Eigentum nach Art. 14 GG

Eine Verletzung des Rechtes auf Leib, Leben und Gesundheit nach Art. 2 II 1 GG sowie des Eigentumsrechts nach Art. 14 I GG dürfte nicht gegeben sein, da das Erfassen von Drohnen grundsätzlich nicht einen Eingriff in die Gesundheit oder in die Eigentumssubstanz des Fluggerätes darstellt.[25]

Allerdings wäre dieses Grundrecht bei harten Abwehrmaßnahmen wie etwa der Einsatz von Netzwerfern oder der Abschuss einer Drohne mittels Laser, Schusswaffen oder Greifvögel betroffen, wenn Personen hierdurch zu Schaden kommen können. Eine solche Maßnahme würde daher zur Rechtfertigung eine erhebliche Gefahr erfordern, die schon wegen der möglichen Auswirkungen auf Unbeteiligte nur in Ausnahmefällen zulässig wäre.[26]

Bei solchen harten Drohnenabwehrmaßnahmen könnte im Falle der Zerstörung einer Drohne auch ein der Eingriff auf das Recht aus Art. 14 I GG vorliegen. Allerdings genießen nach der ständigen Rechtsprechung des BVerfG Tatwerkzeuge oder Gegenstände, die aus Straftaten hervorgebracht werden, nicht den Schutz von Art. 14 I GG. Da eine gefährliche Drohne in der Regel ein Tatwerkzeug wäre, läge ein Eingriff in den Schutzbereich von Art. 14 I GG gar nicht vor. Auch der Verlust von Eigentum als Nebenfolge einer strafrechtlichen Verurteilung, wie etwa die Einziehung der instrumenta und producta sceleris, fallen nicht unter den Eigentums- bzw. Enteignungstatbestand von Art. 14 GG.[27]

7. Allgemeine Handlungsfreiheit nach Art. 2 I GG

Sofern die vorgenannten Grundrechte nicht einschlägig sind, wäre immer noch ein Eingriff in das Recht der allgemeinen Handlungsfreiheit nach Art. 2 I GG möglich.[28] Das Grundrecht der allgemeinen Handlungsfreiheit schützt menschliche Verhaltensweisen und Freiheitsbereiche umfassend, wobei eine Einschränkung aufgrund der verfassungsmäßigen Ordnung, also der geschriebenen Rechtsordnung unter Verhältnismäßigkeitsgründen zulässig ist.[29]

Soweit beim Erfassen von Drohnen – etwa durch ihre Kennzeichnung und Rückverfolgungsmöglichkeit auf den Steuerer – in Art. 2 I GG eingegriffen wird, sind lediglich einfache öffentliche Interessen erforderlich, um eine solche Detektion zu rechtfertigen. In Anbetracht der geringen Eingriffsintensität reicht allein ein plausibler Gefahrenverdacht, um entsprechende Detektionsmaßnahmen zu rechtfertigen.

Sofern etwa in die Steuerung eines Hobbypiloten eingegriffen wird, wäre ebenfalls die allgemeine Handlungsfreiheit nach Art. 2 I GG tangiert. Wenn der Steuerer aber gegen geschriebenes Recht verstößt, sind Eingriffe aufgrund der einschlägigen gesetzlichen Regelungen unter Wahrung des Verhältnismäßigkeitsprinzips zulässig.

Bei autonom fliegenden Drohnen dürfte ein Eingriff nach Art. 2 I GG tatbestandlich gar nicht vorliegen. Der Steuerer hat durch das Auslösen des Timers bzw. das Starten der Drohne seinen Einfluss auf das Fluggerät abgegeben. Etwaige Abwehrmaßnahmen können daher nicht mehr in seine Grundrechte eingreifen.

Entsprechendes gilt für das Sonderproblem, wenn sich Steuerer gegen Flugverbotszonen rechtlich zur Wehr setzen. Sofern ihnen verwehrt wird, in bestimmte Flugverbotszonen mit der Drohne einzufliegen,[30] kann ein Eingriff in die allgemeine Handlungsfreiheit nach Art. 2 I GG angenommen werden. Gleichwohl ist die Einführung einer Flugverbotszone aufgrund der vorhandenen gesetzlichen Regelungen eine zulässige Maßnahme zur Gefahrenabwehr, so dass auch

23 Vgl. zu faktischen Grundrechtseingriffen BVerfGE 105, 279 (303); BVerwG, NJW 2018, 716 (720).

24 Vgl. BVerwG, NJW 2018, 716, 720.

25 Sollten Detektionsanlagen als Nebeneffekt auch Röntgenstrahlungen aufweisen, wäre ein Eingriff in Art. 2 II 1 GG denkbar, sofern die Abschirmmaßnahmen unzureichend sind. Aufgrund der technischen Konfiguration der in den oben genannten Projekten begleiteten Systeme konnte war aber ein solcher Eingriff nicht erkennbar.

26 Vgl. hier BVerfGE 115,118 zur Vereinbarkeit von § 14 III LuftSG mit Art. 2 II 1 GG.

27 BVerfGE 22,387 (422); wie oben ausgeführt betrafen die von der TH-Wildau betreuten Projekte keine harten Abwehrmaßnahmen, sodass in dieser Abhandlung nicht vertiefter auf mögliche Grundrechtsverletzungen eingegangen werden soll; Vgl. hierzu insbesondere Daum/Boesch, CR 218,134; Marosi/Skobel, CR 219, 76; Marosi/Skobel, DVBL 219, 682.

28 Vgl. BVerfGE 6, 37; 21, 234; 63, 60; 67, 171; 70, 23; 77, 118.

29 Vgl. BVerfGE 6, 37; 21, 234; 63, 60; 67, 171; 70, 23; 77, 118.

30 Vgl. hierzu grundlegend die sog. U-Space Verordnung (EU) 2019/945 sowie die Durchführungsverordnung 2021/664.

tatsächlich keine Verletzung des Grundrechts nach Art. 2 I GG vorliegt.

C. Gesetzliche Ermächtigungsgrundlagen für den Einsatz hoheitlicher Drohnendetektionssysteme

Sofern Detektionsmaßnahmen einen Eingriff in Grundrechte darstellen ist eine formell und materiell wirksame gesetzliche Ermächtigungsgrundlage zur Rechtfertigung erforderlich. Da es sich bei der Detektion von Drohnen vorrangig um eine Gefahrenabwehrmaßnahme handelt, ergeben sich die wichtigsten Eingriffsnormen aus den allgemeinen Regelungen der Landespolizeigesetze zur Gefahrenabwehr. Die Gesetzgebungskompetenz zur Gefahrenabwehr steht – abgesehen von Spezialermächtigungen zur Gefahrenabwehr und sog. Annex-Kompetenzen[31] – grundsätzlich den Bundesländern zu.[32]

I. Ermächtigungen zur Gefahrenabwehr durch Einsatz technischer Mittel nach Landespolizeirecht[33]

Entscheidendes Tatbestandsmerkmal für alle polizeilichen Eingriffsmaßnahmen ist das Vorliegen einer Gefahr für die öffentliche Sicherheit und Ordnung.[34] Die Drohne kann aufgrund von Flugbahn, Flughöhe, technischer Ausstattung usw. eine Gefahr für die öffentliche Sicherheit darstellen. Die Gefahren für Leib, Leben, Gesundheit und Eigentum sind bei illegal über Menschenmassen oder Wohn- und Industriegebieten fliegenden Drohnen offenkundig, Ebenso wenn die sonstigen gesetzlichen Vorgaben für den Flugbetrieb von Drohnen nach den § 21 a – h LuftVO nicht beachtet werden.

Als Ermächtigungsgrundlage kommen neben der allgemeinen polizeirechtlichen Generalklausel[35] die spezielleren Regelungen zur Erhebung und Ermittlung von Daten in Betracht. Die allgemein als Datenerhebungsgeneralklausel[36] bezeichnete Ermächtigungsgrundlage zur Erhebung von Daten betrifft allerdings lediglich allgemeine Ermittlungsmaßnahmen, insbesondere die Befragung von Personen. Der Einsatz technischer Mittel ist in der Datenerhebungsgeneralklausel in aller Regel nicht vorgesehen, so dass diese Normen als Ermächtigungsgrundlage für die Detektion von Drohnen durch Drohnendetektionssysteme nur nachrangig in Betracht kommen können.

Einschlägiger für die Detektion von anfliegenden Drohnen sind dann die Spezialregelungen zur Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen, die ausdrücklich den Einsatz technischer Mittel vorsehen.[37] So kann die Polizei bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen personenbezogene Daten durch Ermittlungen oder durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen von Teilnehmern erheben, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten begangen werden. Dabei dürfen auch personenbezogene Daten über Dritte erhoben werden, soweit das unvermeidbar ist, um eine Datenerhebung durchführen zu können.[38]

Ferner ist nach den in den Landespolizeigesetzen enthaltenen Ermächtigungsgrundlagen auch die Datenerhebung an gefährdeten Objekten durch Anfertigung von Bildaufnahmen zulässig. So kann in diesen Fällen die Polizei zur Erfüllung ihrer Aufgaben an einem gefährdeten Objekt, insbesondere an einem Gebäude soweit zur Zweckerreichung zwingend erforderlich, personenbezogene Daten durch Anfertigung von Bildaufnahmen erheben und die Bilder zur Beobachtung übertragen und aufzeichnen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass an oder in einem Objekt dieser Art Straftaten drohen.[39]

Auch im Zusammenhang mit längerfristigen Observationen ist der Einsatz technischer Mittel zulässig, wobei es in diesem Fall insbesondere um die Beobachtung von Personen und nicht von Drohnen geht.[40] Gleichwohl dürfte als milderes Mittel auch das Recht zur Drohnendetektion aus diesen Normen hergeleitet werden. Eine Ermächtigung zum Einsatz von Drohnendetektionssystemen kann sich auch aus der speziellen Standardmaßnahme „Blockierung des Mobilfunkverkehrs“ ergeben.[41] Danach kann bei einer dringenden Gefahr für Leib oder Leben die Polizei im Nahbereich einer Sprengvorrichtung zur Entschärfung den Mobilfunkverkehr blockieren.[42]

---

31 Vgl. zu sog. Annex-Kompetenzen: BVerfGE 8, 143; 28, 310; 41, 355; 84, 247; Götz, Allgemeines Polizei- und Ordnungsrecht, 14. Aufl. (2008), § 1 Rn. 13.

32 Vgl. Knemeyer (o.Fußn. 16), § 11 Rn. 10 – 15; Götz (o.Fußn. 16), § 3; siehe auch Jarass/Pieroth, GG, 15. Aufl. (2018), Art. 73 Rn. 23 Schutzgut der öffentlichen Sicherheit ist die Unverletzlichkeit der objektiven Rechtsordnung, also aller geschriebener Gesetze, der subjektiven verfassungsrechtlich geschützten Rechte und Rechtsgüter sowie der Einrichtungen und Veranstaltungen des Staates.

33 Vgl.§ 25 BerlASOG; § 33 BbgPolG; § 21 BWPolG; Art. 33 BayPAG; § 33 BremPolG; § 10 Gesetz über die Datenverarbeitung der Polizei (Hamburg); § 15 HSOG; § 32 MVSOG; § 35 NPOG; §§ 15 a, 17 NWPolG; § 27 RPPOG; § 38 SächsPolG; § 17 SachsAnhSOG; § 185 SHLVwG; § 34 ThürPAG.

34 nnnText fehlt nnn.

35 Z.B. § 11 BayPAG; § 17 ASOG; § 13 BbgOBG; § 3 SächsPolG; § 11 NPOG; § 6 BWPolG; § 10 BremPolG.

36 Vgl. § 18 ASOG, §§ 29, 30 BbgPolG, § 19 BWPolG, Art. 30 BayPAG, § 27 BremPolG, § 2 Gesetz über die Datenverarbeitung der Polizei (Hamburg), § 13 HSOG, § 26 MWSOG, § 30 NPOG, § 9 NWPolG, § 26 RPPOG, § 25 SPolG, § 36 SächsPolG, § 15 SachsAnhSOG, § 178 SHLVerwG, § 31 ThürPAG.

37 Vgl.§ 24 ASOG, § 31 BbgPolG, § 21 BWPolG, Art. 32 PAG Bay, § 29 BremPolG, § 8 Gesetz über die Datenverarbeitung der Polizei (Hamburg), § 14 HSOG, § 32 NPOG, § 15 NWPolG, § 27 SPolG, § 37 SächsPolG, § 16 SachsAnhSOG, § 184 SHLVerwG, § 33 ThürPAG.

38 So u.a. § 24 I 3 ASOG.

39 Vgl.§ 24 a ASOG, Art. 32 PAG Bay, § 29 BremPolG, § 8 Gesetz über die Datenverarbeitung der Polizei (Hamburg). § 14 HSOG, § 37 SächsPolG, § 16 SOG LSA, § 33 ThürPAG.

40 Vgl.§ 25 ASOG; § 33 BbgPolG. Die Ermächtigung zum Einsatz von Drohnendetektionssystemen aufgrund allgemeinen Polizei- und Ordnungsrechts betrifft gleichermaßen den Einsatz von stationären und mobilen Drohnendetektionssystemen. Nach den Landespolizeigesetzen wird beim Tatbestandsmerkmal technisches Mittel kein Unterschied zwischen dem Einsatz stationärer und mobiler Abwehrsysteme gemacht.

41 Vgl.§ 29 b ASOG, § 33 b III Ziffer 3 BbgPolG, § 23 a VII BWPolG, Art. 34 a IV PAG Bay, § 10 b II Gesetz über die Datenverarbeitung der Polizei Hamburg, § 15 a IV HSOG, § 34 a III MVSOG, § 33 b II NPOG, § 20 b NWPolG (keine Ermächtigung zur Blockierung des Funkverkehrs), § 31 d I, 2 RPPOG, § 33 II SachsAnhSOG, § 34 d I ThürPAG.

42 Etwa wenn durch eine anfliegende Drohne die Gefahr besteht, dass Entschärfungsmaßnahmen behindert werden.

Zu berücksichtigen ist in diesem Zusammenhang, dass nach einigen Landespolizeigesetzen beim Einsatz technischer Mittel verdeckte Bild- und Tonaufzeichnungen grundsätzlich auszuschließen sind.[43] Allerdings sieht u.a. § 25 I Nr. 2 ASOG den verdeckten Einsatz technischer Mittel als zulässige Maßnahme vor, wenn Tatsachen die Annahme rechtfertigen, dass eine Straftat von erheblicher Bedeutung begangen werden soll.

Darüber hinaus existieren spezielle landesrechtliche Ermächtigungen zur Verhinderung des Mobilfunkverkehrs in Justizvollzugsanstalten.[44] So enthält u.a. § 4 SJVollzSichG ein Überflugverbot für Drohnen über Justizvollzugsanstalten. Nach § 2 MFunkVG Bln (Mobilfunkverhinderungsgestz) dürfen die Justizvollzugsanstalten technische Geräte und Systeme betreiben, die unerlaubte Mobilfunkkommunikation auf dem Anstaltsgelände verhindern (Mobilfunkblocker). Sie haben hierbei die von der Bundesnetzagentur festgelegten Rahmenbedingungen zu beachten. Frequenznutzungen außerhalb der Grundstücksgrenzen der Justizvollzugsanstalten dürfen nicht erheblich gestört werden. Insoweit lässt sich aufgrund dieser Ermächtigungsgrundlagen der Einsatz von stationären und mobilen Drohnendetektionssysteme im Bereich von Justizvollzugsanstalten rechtfertigen.

Sofern der Einsatz von Drohnendetektionssystemen auch mit einem Eingriff in die Substanz der Drohne verbunden ist, kommen ergänzend zu den vorgenannten Regelungen des allgemeinen Polizei- und Ordnungsrechts die Verwaltungsvollstreckungsgesetze des Bundes und der Länder zur Anwendung.[45]Unter Hinweis auf die jeweiligen Regelungen des unmittelbaren Zwangs[46] ist eine körperliche Einwirkung auf Drohnen zulässig, sofern die Behörde sich dabei im Rahmen ihrer Befugnisse bewegt, also ein entsprechender hypothetischer Grundverwaltungsakt rechtmäßig wäre.[47]

II. Ermächtigungen zur Gefahrenabwehr aufgrund von Annex-Kompetenzen des Bundes

Für den Bund können sich aus speziellen Kompetenztiteln nach Art. 73,74 GG im Rahmen der ausschließlichen und konkurrierenden Gesetzgebung sog. Annex-Kompetenzen ergeben, die auch das Recht zur Regelung von Gefahrenabwehrtatbeständen beinhalten. So wurde als Annex zum Kompetenztitel Straßenverkehr nach Art. 74 I Nr. 22 GG die Berechtigung zur Regelung von Gefahrenabwehrmaßnahmen durch den Bundesgesetzgeber anerkannt, die von außen auf den Straßenverkehr einwirken.[48]

Verfassungsrechtlich gehören Regelungen des Luftverkehrs zur ausschließlichen Gesetzgebungskompetenz des Bundes nach Art. 73 I Nr. 6 GG. Regelungen zur Gefahrenabwehr im Zusammenhang mit dem Luftverkehr gehören als Annex-Kompetenz zur ausschließlichen Gesetzgebungszuständigkeit des Bundes. Daher kann sich eine Spezialermächtigung zum Einsatz von Drohnendetektionssystemen auch aus § 29 I LuftVG ergeben, sofern es um die Abwehr betriebsbedingter Gefahren für die Sicherheit des Luftverkehrs geht. Nach § 29 I LuftVG ist die Abwehr von betriebsbedingten Gefahren für die Sicherheit des Luftverkehrs sowie für die öffentliche Sicherheit oder Ordnung durch die Luftfahrt (Luftaufsicht) Aufgabe der Luftfahrtbehörden und der Flugsicherungsorganisation.

Da die vorgenannte Norm nur zur Abwehr von betriebsbedingten Gefahren für die Sicherheit des Luftverkehrs ermächtigt, kann ergänzend § 3 LuftSiG herangezogen werden. Danach trifft die Luftsicherheitsbehörde die notwendigen Maßnahmen, um eine bestehende Gefahr für die Sicherheit des zivilen Luftverkehrs abzuwehren. Nach § 3 II LuftSiG können besondere Sicherheitsmaßnahmen angeordnet werden. Insoweit ließe sich auch der Einsatz von Drohnendetektionssystemen an Flughäfen mit § 3 II LuftSiG rechtfertigen. Auch lässt sich der Einsatz von Drohnendetektionssystemen zum Schutz von Kernkraftwerken aufgrund der Pflichten des Betreibers zur weiteren Vorsorge gegen Risiken auf die §§ 7, 7 d AtomG stützen.

Im Zusammenhang mit öffentlichen Versammlungen kommt als Ermächtigungsgrundlage für Eingriffe § 15 II VersG in Betracht. Nach dieser Vorschrift können zur Abwehr einer Gefahr für die öffentliche Sicherheit und Ordnung im Rahmen von Versammlungen auch alle Maßnahmen ergriffen werden, die weniger intensiv sind als die Versammlungsauflösung. Da mit dem Einsatz von Drohnendetektionssystemen ggf. auch Bild- und Tonaufnahmen verbunden sind, kommen die speziellen Ermächtigungsgrundlagen nach den §§ 12 a, 19 a VersG in Betracht.[49]

Dabei stellt sich die Frage, ob die Detektion von Drohnen als Bild- und Tonaufnahmen von Teilnehmern im Sinne der §§ 12 a, 19 a VersG angesehen werden können. Da aber schon die Aufnahme von Personen möglich ist, dürfte die Erfassung von Drohnen, die unrechtmäßig über Menschenansammlungen fliegen, als milderes Mittel von der genannten Ermächtigungsgrundlage mit erfasst werden.[50]

---

43 Vgl.§ 24 I 3 ASOG; kein grundsätzliches Verbot in den anderen Landespolizeigesetzen.

44 Vgl.§ 2 BerlMFunkVG, § 118 II Nr. 3 BbgJVollzG, § 22 II Nr. 2 BWJVollzGB, § 115 II Nr. 3 LJVollzG Rheinland-Pfalz, § 4 SJVollzSichG Saarland (Überflugverbot), § 5 SJVollzSichG Saarland, § 2 II Nr. 3 SächsJVollzSichG, § 117 II Nr. 3 SachsAnhJVollzGB, § 118 SachsAnhJVollzGB (Überflugverbot).

45 Vgl. Marosi/Skobel, CR 2019, 69; auch für die Ermittlung des Standortes des Drohnen-Steuerers kommen die allgemeinen polizeirechtlichen Ermächtigungsgrundlagen zur Anwendung, wie z.B. §§ 17, 24, 24 a ASOG; §§ 10, 30, 31 BbGPolG; §§ 3, 37 SächsPolG, § 16 SachsAnhSOG; § 33 ThürPAG.

46 Vgl.§ 8 BerlVwVfG i.V.m. § 12 VwVG; § 34 BbgVwVG; § 26 BWLVwVG; Art. 34 BayVwZVG; § 16 BremVwVG; § 15 HmbVwVG; § 90 MVSOG; § 10 NVwVG; § 62 NWVwVG; § 65 RPLVwVG; § 22 SVwVG; § 25 SächsVwVG; § 239 SHLVwG; § 51 ThürVwZVG.

47 Vgl. Knemeyer (o.Fußn. 16), Rn. 449; Schenke (o.Fußn. 16), Rn. 538 – 542; Götz (o.Fußn. 16), § 13 V.; Marosi/Skobel, CR 2019, 69.

48 Vgl. u.a. BVerfGE 8, 143; 28, 310; 41, 355; 84, 247; Götz (o.Fußn. 16), § 1 Rn. 13.

49 Nach Art. 125 a I Nr. 1 GG gelten die Vorschriften von § 19 a i.V.m. § 12 a VersG in den jeweiligen Bundesländern fort, die keine eigenständigen Regelungen erlassen haben.

50 Vgl. zu Eingriffen nach VersG unterhalb der Verbotsschwelle BVerwG, NJW 2018, 717 sowie BVerwG, NVwZ 2007, 1439.

III. Ermächtigungen zur Strafverfolgung durch Einsatz technischer Mittel

Sofern durch einen unbefugten Gebrauch von Drohnen bereits Straftatbestände erfüllt sind, kommen als Ermächtigungsgrundlagen neben den genannten Landespolizeigesetzen auch bundesgesetzliche Ermächtigungsgrundlagen – insbesondere nach der StPO – in Betracht. Die in Art. 74 I Nr. 1 GG enthaltene Kompetenznorm für das Strafrecht einschließlich des gerichtlichen Verfahrens umfasst auch Kompetenzen für entsprechende bundesrechtliche Eingriffsbefugnisse.[51] Neben der allgemeinen Ermächtigungsgrundlage nach § 163 StPO kommen spezielle Normen zum Einsatz technischer Mittel nach den §§ 100 h, e StPO in Betracht.

Danach dürfen ohne Wissen des Betroffenen zur Erforschung des Sachverhalts Bildaufnahmen hergestellt werden oder sonstige technische Mittel verwendet werden.[52] Eine Maßnahme nach § 100 h I 1 Nr. 2 StPO ist nur zulässig, wenn Gegenstand der Untersuchung eine Straftat von erheblicher Bedeutung ist.[53]

Des Weiteren kommt als Ermächtigungsgrundlage der § 100 i StPO in Betracht, der technische Ermittlungsmaßnahmen bei Mobilfunkgeräten erfasst. Bei der vorgenannten Norm geht es um die Erfassung von Positions- und Standortmeldungen von Mobiltelefonen.[54] Sofern die Steuerung einer Drohne unter Mithilfe eines Mobiltelefons erfolgt, wären entsprechende Maßnahmen auch aufgrund dieser Norm zulässig. Verfahrensrechtlich wäre bei diesen Maßnahmen der Richtervorbehalt nach § 100 e StPO zu beachten.

D. Verhältnismäßigkeitsaspekte im Zusammenhang mit möglichen Grundrechtseingriffen

Der Grundsatz der Verhältnismäßigkeit verlangt, dass der Staat mit dem Grundrechtseingriff einen legitimen Zweck mit geeigneten, erforderlichen und angemessenen Mitteln verfolgt.[55] Dabei darf die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen.[56]

a) Geringe Persönlichkeitsrelevanz der Drohnendetektion

Wie ausgeführt, kommt dem bloßen optischen, akustischen oder elektromagnetischen Erfassen einer Drohne gar keine Persönlichkeitsrelevanz zu, so dass es hier bereits an einem Eingriff fehlt. Allein im Falle von optischen oder akustischen Aufnahmen von Personen kann von einem Eingriff ausgegangen werden, wobei allerdings die Persönlichkeitsrelevanz im Falle einer flüchtigen Erfassung (Aufnahme in Echtzeit) eher gering sein dürfte.[57]

Darüber hinaus ist im Rahmen der Gewichtung eines möglichen Eingriffs bedeutsam, ob der Betroffene einen zurechenbaren Anlass der Informationserhebung gegeben hat. Insoweit können entsprechende Maßnahmen gegenüber Personen, die einen Eingriff veranlasst haben, leichter verfügt werden. Im Vergleich zu einer solchen anlassbezogenen Maßnahme besteht eine höhere Eingriffsintensität, wenn Personen erfasst werden, die durch ihr Verhalten die Maßnahme nicht veranlasst haben.[58]

b) Heimlichkeit einer Drohnendetektion

Die Eingriffsintensität bei der Drohnendetektion könnte allerdings durch die Heimlichkeit der Maßnahme erhöht sein. Die Heimlichkeit eines Eingriffs in Grundrechte führt zu einer Erhöhung des Gewichts der Freiheitsbeeinträchtigung.[59] Dieser Aspekt spielt allerdings nur dann eine Rolle, wenn Detektionssysteme nicht erkennbar sind, was insbesondere beim Einsatz von mobilen Geräten der Fall sein dürfte. Bei stationären Detektionssystemen kann dagegen nicht ohne weiteres von einem heimlichen Einsatz ausgegangen werden.

Allerdings dürfte der Aspekt der Heimlichkeit insbesondere bei autonom fliegenden Drohnen[60] ohne Bedeutung sein. Wie ausgeführt erschöpft sich bei autonom fliegenden Drohnen die menschliche Zurechnung auf die Programmierung vor dem Start, so dass bereits kein Eingriff vorliegen dürfte. Sobald die Drohne in der Luft ist, endet die menschliche Kontrolle.[61]

c) Verlust von Beweismitteln bei bloßer Echtzeiterfassung oder Verpixelung

Eine aus Verhältnismäßigkeitsgründen möglicherweise erforderliche Verpixelung oder Löschung von Fotos oder akustischer Aufnahmen von Personen kann allerdings dazu führen, dass bestimmte Beweise bei der Aufklärung des Sachverhalts verloren gehen. Wenn etwa das Gesicht des Steuerers oder sonstiger beteiligter Personen verpixelt und damit nicht mehr erkennbar ist, dürfte eine Strafverfolgung nur unter erschwerten Voraussetzungen erfolgreich sein. Gleiches gilt auch bei der bloßen optischen oder akustischen Echtzeiterfassung von Personen, wenn die Aufnahmen nicht – zum Zwecke des Strafverfahrens – gespeichert werden dürfen.

51 Vgl. BVerfGE 30, 29; 36, 314 (319); ferner Jarass/Pieroth (o.Fußn. 31), Art. 74 Rn. 4 – 7.
52 Vgl. BVerfG, NJW 2010, 2717; Bull, NJW 2009, 3279; Köhler, in: Meyer-Goßner/Schmitt (o.Fußn. 20), § 100 h, Rn. 1, 1 a; BGH-ST 44, 13.
53 Vgl. zur Verwertung von Aufzeichnungen privat genutzter Dashcams im Straßenverkehr: OLG Stuttgart, NJW 2016, 2218; ferner OLG Celle, NStZ 2018, 295.
54 Vgl. BVerfG, NJW 2007, 351; Puschke, NJW 2018, 2811; Köhler, in: Meyer-Goßner/Schmitt (o.Fußn. 20), § 100 i, Rn. 1 – 4; über § 100 i StPO ließe sich gegebenenfalls auch der Standort des Steuerers ermitteln.
55 Vgl. BVerfGE 110, 335; 67, 173, 175; 90, 172.
56 Vgl. BVerfGE 110, 335; 67, 173, 175; 90, 172.
57 Vgl. zum Problem der Persönlichkeitsrelevanz: BVerfGE 100, 376; 113, 382; 115, 347; 118, 168.
58 Vgl. BVerfGE 113, 348; 115, 354.
59 Vgl. BVerfGE 107, 321; 115, 194; 115, 353.
60 Vgl. Hänsenberger, Diss. Universität St. Gallen, 2018, S. 97.
61 Vgl. Hänsenberger (o.Fußn. 60).

E. Zusammenfassung und Darstellung der technischen Maßnahmen beim Einsatz und Betrieb von Drohnenabwehr-Systemen und ihre rechtliche Einordnung

Zusammenfassend ist im Rahmen der Verhältnismäßigkeitserwägungen zu berücksichtigen, dass die mit einer – auch heimlichen – Drohnendetektion möglicherweise verbundenen Grundrechtseingriffe als nicht besonders schwerwiegend anzusehen sind.[62] Einfache öffentliche Interessen vor allem zur Gefahrenabwehr reichen zur Rechtfertigung aus.

Sodann ist zu unterscheiden, ob es sich um eine gesteuerte oder eine autonom fliegende Drohne handelt.[63] Bei autonom fliegenden Drohnen sind die rechtsstaatlichen Hürden für ein staatliches Handeln zum Zwecke der Gefahrenabwehr mangels Eingriff gegenüber dem Steuerer ohnehin eher gering,[64] da dieser jeden Einfluss auf die Drohne aufgegeben hat.

Die entscheidenden Fragestellungen ergeben sich vielmehr bei der Vornahme harter Abwehrmaßnahmen. Hier wäre vor allem Leib, Leben und Gesundheit unbeteiligter Menschen zu berücksichtigen, so dass entsprechende Maßnahmen nur in Ausnahmefällen zum Schutz ganz gewichtiger Rechtsgüter verfassungsrechtlich zulässig wären.[65]

Als Fazit lassen sich hoheitlichen Maßnahmen zur technischen Detektion von Drohnen rechtlich wie folgt einordnen:

a) Maßnahmen ohne Eingriffscharakter:

- Auslösung eines akustischen Alarms mittels Radarsensorik/Erfassung akustischer Signale ohne Aufnahme von Gesprächen
- Auslösung eines optischen Alarms mittels Radarsensorik/Erfassung optischer Signale ohne Aufnahme von Personen
- Detektion einer Drohne mittels Radar[66]/Auswertung der Radarsignatur der Drohne
- Erfassen und Verfolgen der Drohne durch sonstige elektromagnetische Sensoren/Ermittlung der Funkfrequenz
- Erfassung der Drohne ohne Personenbezug mittels Fotoaufnahmen
- Erfassung der Drohne ohne Personenbezug mittels akustischer Aufnahmen
- Speicherung des letzten Kontaktpunktes
- Speicherung des Flugverlaufs (sog. Trekking)
- Speicherung der Drohnenmerkmale
- Abgleich mit vorhandenen Drohnendatenbanken

b) Maßnahmen mit Eingriffscharakter

aa) Weiche Abwehrmaßnahmen, die aufgrund der in Kapitel C genannten präventiven und repressiven Ermächtigungsgrundlagen unter Beachtung der Verhältnismäßigkeit zulässig wären:

- Aufnahme von Fotos unbeteiligter Personen
- Aufnahme von Gesprächen unbeteiligter Personen
- Abgleich mit vorhandenen Drohnendaten bei der Ermittlung von Drohnenkennzeichen die einer Person zuzuordnen ist
- Detektion/Ermittlung des Standortes des Steuerers[67]
- Störung von Funksignalen/Eingriff bzw. Übernahme der Funksteuerung/Jammen[68]
- Aussenden eines falschen GPS-Signals, um Drohne vom Kurs abzubringen (sog. GPS-Spoofing)[69]
- Geofencing-Maßnahmen gegenüber den Herstellern von Drohnen und sonstigen Fluggeräten
- luftverkehrsrechtliche Ausweisung von Geofencing-Zonen

b) Harte Abwehrmaßnahmen,[70] die aufgrund der in Kapitel C genannten präventiven und repressiven Ermächtigungsgrundlagen unter Beachtung der Verhältnismäßigkeit und Art. 2 II 1 GG in Ausnahmefällen zulässig wären:

- Einsatz von Netzwerfern
- Abschuss/Absturz der Drohne mittels Laser[71]
- Abschuss/Absturz der Drohne mittels Schusswaffe
- Abschuss/Absturz der Drohne mittels Wasserwerfer
- Abfangen und Fixieren der Drohne durch Greifvögel[72]

62 Vgl. BVerwG vom 22. 10. 2014 – 6 C 7/13; BVerfG, NJW 2008, 1505 zum Gewicht einer Kennzeichenerfassung.
63 Vgl.hierzu Hänsenberger a. a. O., S. 97 ff.
64 Vgl.zum autonomen Fliegen: Hänsenberger a. a. O.
65 Vgl.zu dieser Interessenlage auch BVerfGE 115,118 zur Vereinbarkeit von § 14 III LuftSG mit Art. 2 II 1 GG; ferner Arzt/Fährmann/Schuster, DÖV 2020, 866.
66 Vgl. Arzt/Fährmann/Schuster, DÖV 2020, 866 (870) (sofern Daten im Rahmen der Telekommunikation anfallen liegt aber Eingriff in Art. 10 I GG vor); ferner: Marosi/Skobel, DVBl, 2019, 678 (683).
67 Vgl.Daum/Boesch a. a. O. 130; ferner zum Problem der Ermittlung des Standortes des Steuerers bzw. Drohnenpiloten: Hänsenberger, Diss. Universität St. Gallen, 2018, S. 37.
68 Vgl. Marosi/Skobel, CR 2019, 66; Marosi/Skobel, DVBl. 2019, 682 (683); Arzt/Fährmann/Schuster, DÖV 2020, 866; Daum/Boesch a. a. O. 63; Grosskopf, CR 2014, 764; ferner Hänsenberger, Diss. Universität St. Gallen, 2018, S. 161.
69 Vgl. Daum/Boesch a. a. O. 134; ferner Hänsenberger a. a. O.
70 Vgl. Marosi/Skobel CR 2019, 67; Daum/Boesch, CR 2018, 63; Dieckert, Sicherheitsberater 2015, 1 (14).
71 Vgl. Daum/Boesch CR 2018, 134.
72 Vgl. Daum/Boesch a. a. O.