Hartmut Aden / Jan Fährmann

Wie lassen sich Informationseingriffe der Polizei wirksam gesetzlich begrenzen?

Ein Ausblick am Beispiel der GPS-Ortung gestohlener Gegenstände

Ortungstechnik wie das *Global Positioning System* (GPS) spielt in unserem Alltag eine wichtige Rolle. Entsprechende Sender sind heute in vielen Alltagsgegenständen enthalten. Der Beitrag untersucht am Beispiel des Fahrraddiebstahls, wie Ortungsdaten gestohlener Gegenstände zur Polizei gelangen und zur Fahndung genutzt werden können. Dabei zeigt sich, dass es bisher keine gesetzliche Regelung gibt, die speziell für diesen Anwendungsfall konzipiert ist. Die Autoren stellen dieses Beispiel in den Kontext der grundsätzlichen Diskussion, ob Gesetzgebung polizeiliche Informationseingriffe überhaupt wirksam steuern kann.

Die meisten Menschen haben heute ständig mobile Geräte bei sich, die mit Ortungsfunktionen ausgestattet sind, z.B. Smartphones. Seit Anfang der 2000er Jahre hat die Ortung mit Hilfe von Geolokalisierungstechnik erheblich an Bedeutung gewonnen. Am bekanntesten und auch in Europa am weitesten verbreitet ist das US-amerikanische *Global Positioning System* (GPS), das ursprünglich in den 1970er Jahren für militärische Zwecke entwickelt wurde und heute in vielfältigen Anwendungen genutzt wird, u.a. in Smartphones und anderen mobilen Kommunikationsgeräten. Daneben gibt es chinesische und russische Systeme – und zukünftig auch das europäische *Galileo Positioning System*. Diese Technologien werden unter dem Oberbegriff *Global Navigation Satellite System* (GNSS) zusammengefasst. Sie basieren auf Satelliten-Netzwerken, die in der Lage sind, durch Distanzmessung die Position und die Geschwindigkeit eines Senders – von kleinen Abweichungen abgesehen – genau zu berechnen. Dabei wirken jeweils mehrere Satelliten zusammen, was die Genauigkeit der Ortung verbessert. Die Nutzer_innen empfangen dazu mittels eines Empfangsgerätes Signale der GNSS-Satelliten, aus denen sich die jeweilige Position und Geschwindigkeit berechnen lassen. Die Ortsbestimmung erfolgt etwa durch Berechnung der Distanz anhand der Signallaufzeit zwischen Satelliten und Empfangsgerät.

Die Wirkungen sind aus bürgerrechtlicher Sicht ambivalent. Die GPS-Ortung bietet zahlreiche praktische Funktionen, so bei der Suche nach dem richtigen Weg, der nächsten Bahn- oder Busverbindung oder einem passenden Laden oder Restaurant. Sie eröffnet aber privaten Firmen, die mobile Dienstleistungen anbieten, sowie staatli-

chen Stellen auch neue Möglichkeiten intensiver Überwachung. Menschen, die ständig Mobilgeräte bei sich tragen, hinterlassen umfangreiche Datenspuren. Daraus lassen sich leicht Bewegungsprofile rekonstruieren. Mobile Geräte entwickeln sich so zu technischen Helfern von Massenüberwachung.

Das „Internet der Dinge" führt zunehmend dazu, dass auch zahlreiche Alltagsgegenstände mit GPS-Sendern ausgestattet sind. Dies hat auch den Effekt, dass sie bei Bedarf leichter gefunden werden können. Wird ein solcher Gegenstand gestohlen, so wird dies bei rechtmäßigen Eigentümer_innen in der Regel den Wunsch auslösen, diesen Gegenstand mit Hilfe der Ortungsfunktion zurückzuerlangen – mit oder ohne Hilfe der Polizei. Funktioniert dies? Unter welchen Voraussetzungen darf die Polizei Ortungsdaten gestohlener Gegenstände nutzen? Dieser Beitrag untersucht dies am Beispiel gestohlener Fahrräder und stellt diesen Anwendungsfall in den Kontext der grundsätzlicheren Diskussion, ob Gesetzgebung polizeiliche Informationseingriffe überhaupt wirksam steuern kann.

Fahrraddiebstahl – GPS-Ortung als neue Strategie gegen ein Massendelikt mit niedrigen Aufklärungsquoten?

Fahrräder sind meist schlecht gegen Diebstahl gesichert und werden daher häufig gestohlen. Auch werden die Erwartungen der Bestohlenen an die Polizei meistens enttäuscht. Denn bei Fahrraddiebstählen hinterlassen Täter_innen in der Regel kaum Spuren, so dass polizeiliche Ermittlungsansätze für die Aufklärung nur beschränkt vorhanden sind oder gänzlich fehlen. Hohe Fallzahlen stehen daher einer sehr niedrigen Aufklärungsquote gegenüber, vielfach im Bereich von 3 Prozent.

Mittlerweile wird auch in Fahrrädern zunehmend GPS-Technik verbaut, die anzeigt, wo sich das Fahrrad befindet. Diese Lösung wird vornehmlich von Betreiber_innen von Fahrradflotten eingesetzt, die Fahrräder einsammeln müssen, wenn sie von Nutzer_innen an ungünstigen Orten abgestellt wurden. Auch immer mehr Privatpersonen nutzen GPS-Technik in Fahrrädern, beispielsweise zum Navigieren, aber auch zum Diebstahlschutz. Wird ein solches Fahrrad unrechtmäßig benutzt oder gestohlen, so könnten die Ortungsdaten hilfreich sein, um das Fahrrad zurückzuerlangen. Allerdings gibt es aktuell noch keine Möglichkeit, die GPS Daten gestohlener Gegenstände in die Fahndungs- und Kommunikationssysteme der Polizei zu übernehmen.

In dem interdisziplinären Forschungsprojekt *FindMyBike*[1] wurde daher von der Beuth Hochschule für Technik Berlin und dem Forschungsinstitut für Öffentliche und Private Sicherheit (FÖPS Berlin) der Hochschule für Wirtschaft eine Lösung in Form einer rechtskonformen standardisierten Schnittstelle entwickelt, die GPS-Daten gestohlener Fahrräder an die Polizei überträgt, um deren Auffinden durch die Polizei mit Hilfe von GPS-Ortung zu erleichtern. Bei der Konzeption der Schnittstelle zeigte sich allerdings, dass die Erhebung von Ortungsdaten gestohlener Fahrräder durch die Polizei nach der derzeitigen Gesetzeslage rechtlich problematisch ist.

Rechtliche Möglichkeiten zur Erhebung von GPS Daten gestohlener Gegenstände

Ist ein Fahrrad gestohlen worden, so eröffnet dies den Anfangsverdacht einer Straftat. Die Polizei muss daher regelmäßig die Eingriffsbefugnisse aus der Strafprozessordnung (StPO) nutzen. Die Ermächtigung zur Erhebung von GPS-Daten gestohlener Gegenstände könnte sich auf den ersten Blick aus § 100h Abs. 1 Nr. 2 StPO ergeben. Bei der Norm handelt es sich um eine Generalklausel für den Einsatz von technischen Geräten, für die keine speziellere Eingriffsgrundlage in der StPO besteht.[2]

Die zur Datenerhebung nötige Tracking-Technologie ist ein sonstiges technisches Mittel im Sinne des § 100h Abs. 1 Nr. 2 StPO.[3] Zudem erfordert die Norm eine Observation, die nur dann vorliegt, wenn es darum geht, die Bewegungen des gestohlenen Gegenstandes zu beobachten, um beispielsweise Hinweise auf kriminelle Strukturen zu erhalten. Diese Voraussetzung wäre bei einer bloßen Ortung mit dem Ziel, den Gegenstand aufzufinden, nicht erfüllt.[4] Die Eingriffsbefugnis nach § 100h StPO darf im Übrigen nur bei Straftaten von erheblicher Bedeutung eingesetzt werden. Die Gesetzgebung verwendet diese Beschränkung bei vielen polizeilichen Eingriffsbefugnissen, um sicherzustellen, dass die Polizei bei Bagatelldelikten auf Mittel verzichtet, die mit weitreichenden Grundrechtseingriffen verbunden wären. Von erheblichen Straftaten ist auszugehen, wenn sie mindestens dem Bereich der mittleren Kriminalität zuzurechnen sind und den Rechtsfrieden empfindlich stören. Dazu müssen die Delikte einen gewissen Schweregrad aufweisen,[5] wofür ein einfacher Diebstahl in der Regel nicht ausreicht,[6] es sei denn, die gestohlene Sache weist einen erheblichen Wert auf, etwa ein LKW mit wertvoller Ladung.[7] Straftaten können allerdings auch dann als schwerwiegend einzustufen sein, wenn durch eine Vielzahl von Delikten oder eine arbeitsteilige Herangehensweise insgesamt ein sehr hoher Schaden verursacht wird.[8] Erhebliche Bedeutung haben daher meist Diebstahlserien bzw. organisierte oder bandenmäßige Begehungsformen.[9] Dies ist vielfach aber bei einem einzelnen Diebstahl (noch) nicht erkennbar, wenn die Geschädigten bei der Polizei Anzeige erstatten. Vielmehr kann sich ein Verdacht auf Zusammenhänge mit weiteren Straftaten erst später aus der Beobachtung des gestohlenen Gegenstandes oder weiteren Ermittlungen ergeben. Im Regelfall wird § 100h StPO die Polizei daher nicht zur Datenerhebung bei Fahrraddiebstählen ermächtigen, da bei einem Fahrraddiebstahl vielfach weitere Ermittlungsansätze fehlen.

Mangels speziellerer Norm kommt in den meisten Diebstahlsfällen folglich nur die Ermittlungsgeneralklausel aus den §§ 161 Abs. 1 und 163 Abs. 1 StPO in Betracht. Diese Normen rechtfertigen nur Ermittlungsmaßnahmen mit geringer Eingriffsintensität.[10] Mithin ist zu prüfen, wie schwer der Grundrechtseingriff durch die GPS-Ortung wiegt. Außerdem darf ein Rückgriff auf die Generalklauseln nicht dazu führen, dass die strengeren Anforderungen (wie z.B. die des § 100h StPO) in vergleichbaren Fällen umgangen werden. Eine Speicherung und Auswertung von Daten kann daher aufgrund ihrer Eingriffsintensität grundsätzlich nicht auf die Generalklausel gestützt werden. Allenfalls die bloße Ortung zum direkten, kurzfristigen Auffinden des Gegenstandes könnte nach der hier vertretenen Rechtsauffassung von der Generalklausel gestattet werden. Die Eingriffsintensität ist gering, da nur sehr wenige Rückschlüsse auf Perso-

nen möglich sind, die mit einem gestohlenen Fahrrad im öffentlichen Raum unterwegs sind. Im Moment der Anzeige ist meist noch nicht einmal klar, wer das Fahrrad im Besitz hat, da dieses leicht weitergegeben werden kann.

Polizeiliche Generalklauseln sind allerdings nicht dafür gedacht, Eingriffe durch neue Technologien dauerhaft zu rechtfertigen. Zwar ist es nicht zwingend, dass jede Nutzung kriminaltechnischer Neuerungen sofort ausdrücklich normiert wird. Aus dem verfassungsrechtlichen Bestimmtheitsgebot folgt für die Gesetzgebung aber, dass technische Eingriffsinstrumente möglichst genau bezeichnet werden müssen. Dadurch wird sicherstellt, dass die Adressat_innen der jeweiligen Norm erkennen können, wann es zu entsprechenden Eingriffen kommt. Nur so kann außerdem gesichert werden, dass die Polizei neue technische Möglichkeiten rechtmäßig einsetzt, insbesondere unter strenger Beachtung der Verhältnismäßigkeit. Daher muss die Gesetzgebung neue technische Entwicklungen aufmerksam beobachten und deren Nutzung bei Fehlentwicklungen im Interesse des Grundrechtsschutzes durch neue Ermächtigungsgrundlagen korrigieren.[11] Die polizeilichen Generalklauseln sind folglich dahingehend zu verstehen, dass sie der Polizei ermöglichen, auf unvorhergesehene Situationen auch mit näher regelungsbedürftigen, aber nicht eingriffsintensiven Maßnahmen vorläufig zu reagieren. Keinesfalls können neue Eingriffsmaßnahmen dauerhaft über die Generalklauseln zugelassen werden.[12] Absehbar wird in Zukunft die Ortung gestohlener Gegenstände noch wesentlich praxisrelevanter werden als heute, da in immer mehr Gegenständen entsprechende Sender enthalten sein werden. Die Gesetzgebung sollte somit in der Strafprozessordnung für diese Fälle eine spezielle Regelung ergänzen, die es der Polizei ermöglicht, Ortungsdaten von gestohlenen Gegenständen im Interesse der Geschädigten und einer effektiven Strafverfolgung unter Wahrung der Verhältnismäßigkeit und unter Vermeidung von Massendatenerhebungen zu nutzen.

Polizeiliche Eingriffsbefugnisse und schneller technischer Wandel

Hinreichend bestimmte Ermächtigungsgrundlagen fehlen nicht nur bei der polizeilichen Ortung gestohlener Gegenstände, sondern bei der Nutzung vieler technischer Neuentwicklungen, z.B. beim polizeilichen Röntgeneinsatz, der Drohnendetektion oder bei der polizeilichen Nutzung von *Social Media*-Plattformen wie *Twitter* oder *Facebook*. Dies gilt nicht nur für die StPO sondern auch für das ebenfalls eingriffsintensive Polizeirecht. Dabei ist zu berücksichtigen, dass technische Zwänge und die Intensität staatlicher Überwachung einen ganz erheblichen Einfluss auf die Verwirklichungsbedingungen der Grundrechte haben.

Defizitäre Entwicklungstendenzen in der Sicherheitsgesetzgebung

Die Polizeigesetze und die StPO ermöglichten der Polizei in den zurückliegenden Jahrzehnten immer mehr Grundrechtseingriffe durch technische Maßnahmen. Da mittlerweile nahezu alle Lebensbereiche von Technik durchsetzt sind, können aus entspre-

chenden Eingriffen sehr viele und genaue Rückschlüsse auf die Lebensführung der Bürger_innen gezogen werden.[13] Die Polizei kann so immer weiter in den privaten Bereich der Bürger_innen vordringen, sogar in Richtung des absolut geschützten Kernbereichs.[14] Dadurch können elementare Grundsätze des Rechts auf informationelle Selbstbestimmung in Frage gestellt werden. Die technische Entwicklung begründet mithin zahlreiche Risiken für den Grundrechtsgebrauch.[15]

Auch ist eine Tendenz zur massenhaften Datenerhebung auf Vorrat zu erkennen. Dies kann etwa durch „intelligente Videoüberwachung" oder einen Musterabgleich wie nach § 4 Abs. 1 Fluggastdatengesetz (FlugDaG) geschehen.[16] Die Vorratsdatenhaltung stellt einen weiteren Schritt in Richtung eines Datenabgleichs von Menschenmassen im öffentlichen Raum dar, mit dem Einzelpersonen Kategorien zugeordnet werden können. Damit geht die Polizei nicht einem Verdacht oder bestimmten Anhaltspunkten für eine Gefahr nach, sondern versucht Anhaltspunkte dafür erst zu generieren.[17] Dementsprechend müssen die betroffenen Menschen auch keinerlei Anlass für die Datenerhebung gesetzt haben. Solche Maßnahmen sind aufgrund ihrer hohen Eingriffsstreubreite verfassungsrechtlich extrem problematisch.[18]

Zusätzlich sind die Regelungen der Polizeigesetze und der StPO für die Techniknutzung sowohl für die Polizei als auch für die Bürger_innen nicht immer ausreichend verständlich.[19] Die tatbestandlichen Voraussetzungen sind in vielen Fällen weich und unterliegen damit vielfach sich wandelnden Wertungen,[20] wodurch die Eingriffsweite und die Grenzen für polizeiliches Handeln oft nicht klar genug zu erkennen sind. So sind polizeiliche Befugnisse für die Verarbeitung personenbezogener Daten gesetzlich zumeist nur an die Erforderlichkeit für die Aufgabenerfüllung gebunden, vgl. etwa §§ 100j Abs. 1, 98c StPO oder § 28 Abs. 1 ASOG Berlin.

Unklare und weit gefasste Eingriffsbefugnisse eröffnen der Verwaltung jedoch einen zu weiten Eingriffsspielraum, der sich nur schwer durch die Rechtsprechung kontrollieren lässt, insbesondere weil bei der polizeilichen Techniknutzung viele Vorgänge verdeckt ablaufen.[21] Eine Intensivierung staatlicher Überwachungsmaßnahmen erhöht zudem das Risiko einer Unterdrückung der Opposition, der Verdächtigung und möglicherweise sogar Verurteilung Unschuldiger und führt letztlich dazu, dass alle Menschen als potenziell verdächtig betrachtet werden.[22] Dabei ist davon auszugehen, dass ein Freiheitsverlust durch staatliche Überwachung nicht durch einzelne Reformen des Sicherheitsrechts herbeigeführt wird. Vielmehr ist damit zu rechnen, dass gemäß dem Sprichwort „*liberty dies by inches*" Schritt für Schritt ein Abbau der Freiheiten geschieht, vielfach unbemerkt von den Betroffenen. *Roßnagel* hat bereits 1993 prophezeit, dass dieser Prozess eintreten wird und sich in einer Neuinterpretation der Verfassung durch die Gerichte und insbesondere durch das BVerfG widerspiegeln wird. Hätten wir uns erst an vermehrte Datenerhebung und -verarbeitung gewöhnt, würden wir ein anderes Verständnis von Freiheit entwickeln.[23] Mehr als ein Vierteljahrhundert später ist eine klare Tendenz zu erkennen, dass seine Prognose zutrifft. Betrachtet man beispielsweise die Proteste gegen die Volkszählung von 1983, bei der es um weitaus weniger personenbezogene Daten ging als heute tagtäglich freiwillig preisgegeben werden, wird deutlich, dass sich das Freiheitsverständnis drastisch verändert hat.[24] Bisher wurde zudem weder von der Gesetzgebung noch vom BVerfG eine befriedigende Antwort auf die Frage gefunden, wie eine aufgrund des technischen

Fortschrittes mögliche und teilweise bereits durchgeführte Massendatenverarbeitung wirksam im Sinne eines effektiven Grundrechtsschutzes beschränkt werden kann. Weitere Gradmesser, ob sich die Interpretation der Verfassung weiter verändert, werden u.a. die anstehenden Entscheidungen des BVerfG über das Fluggastdatengesetz und die Normierung der „drohenden Gefahr" im bayerischen Polizeiaufgabengesetz (PAG) sein. *Roßnagel* kommt aber in seiner Studie aus dem Jahr 1993 auch zu dem Schluss, dass diese Entwicklung keinesfalls determiniert ist und dass auch von Widerständen innerhalb der Gesellschaft auszugehen ist.[25] Unter welchen Umständen solche Widerstände auch zu rechtlichen Schutzmechanismen gegen eine Massenüberwachung beitragen können und wie diese aussehen könnten, wird im Folgenden betrachtet.

Ist Technik überhaupt noch gesetzlich regulierbar?

Recht und Technik haben einen großen Einfluss sowohl auf die individuelle Lebenswirklichkeit der Individuen als auch die sozialen Entwicklungsbedingungen der gesamten Gesellschaft. Sie beeinflussen sich in einem wechselseitigen Prozess. Manche technische Neuerungen ermöglichen Verhaltensweisen, die nach rechtlichen Regelungen verlangen. Zugleich können entsprechende Neuerungen Verwirklichungs- und Umgehungsmechanismen für bereits bestehende Rechtsnormen liefern.[26]

Die Einflüsse von Technik hängen von unterschiedlichen Faktoren ab, u.a. von den beteiligten Akteur_innen. Die rechtliche Regulierung neuer Technologien kann keinesfalls alle Aspekte ihrer Nutzung erfassen. Für das Datenschutzrecht stellt sich zunehmend die Frage, ob es sich gegen Paradigmen technischer Machbarkeit und gegen das große Interesse an der Datenverarbeitung in der Polizei behaupten kann.[27] Im privatwirtschaftlichen Bereich erzeugen der ökonomische Druck neuer Geschäftsmodelle und das Streben nach Wettbewerbsfähigkeit im globalen Vergleich ähnliche Herausforderungen.

Sind technische Anwendungen erst einmal fest in gesellschaftlichen Abläufen etabliert, ist eine nachträgliche Korrektur oft nur mit großem Aufwand möglich. Wird beispielsweise eine bestimmte technische Anwendung verboten, die bereits Einzug in behördliche Strukturen erhalten hat, so ist mit erheblichen Widerständen gegen die Veränderung zu rechnen. Dies ist auch und insbesondere im Sicherheitsbereich zu beobachten, wo polizeiliche Eingriffsbefugnisse nur selten zurückgenommen oder nachträglich grundrechtsschonend korrigiert werden.

Die Technikentwicklung wird meist zu einem Zeitpunkt in Gang gesetzt, an dem entweder noch wenig über die Risiken und Chancen der Technik nachgedacht wird oder diese noch nicht vollumfänglich ersichtlich sind. Denn die Etablierung einer Technik ist ein sozialer Prozess, der durch unterschiedliche Faktoren beeinflusst wird.[28] Der effektivste (meist frühe) Zeitpunkt zur Technikregulierung wird daher vielfach verpasst. Allerdings erwächst aus dem Umstand, dass es sich bei der rechtlichen Technikgestaltung um einen sozialen, nicht determinierten Prozess handelt, gleichwohl die Möglichkeit der Korrektur im Sinne einer grundrechtsschonenderen

Ausgestaltung der technischen Eingriffsbefugnisse. Dazu sind die rechtlichen Anknüpfungspunkte für eine gesetzgeberische Korrektur festzulegen.

Gesetzgeberische Möglichkeiten zur grundrechtsschonenden Gestaltung polizeilicher Informationstechnik

Auch wenn das Recht die Technikgestaltung nicht vollständig vorgeben kann, so ist es doch möglich, zentrale Entscheidungen und Wertmaßstäbe für das Handeln der Akteur_innen festzulegen.[29] An dieser Stelle werden exemplarisch einige Vorschläge für den Umgang mit der technischen Entwicklung im eingriffsintensiven Sicherheitsbereich erörtert. Die technische Entwicklung begründet nämlich nicht nur Risiken für den Grundrechtsgebrauch, sondern stellt gleichzeitig auch die Mittel zur Verfügung, entsprechende technisch bedingte Risiken zu minimieren bzw. sogar zu neutralisieren.[30]

Als Reaktion auf die technische Entwicklung sind etwa die Grundsätze der Datenminimierung, d. h. die Beschränkung der Datenverarbeitung auf das zwingend erforderliche Minimum an Daten, und die Ausgestaltung informationstechnischer Systeme nach dem Grundsatz *Privacy by Design* entstanden. Diese stellen zentrale Wertmaßstäbe für die Ausgestaltung der Technik dar und sind potentiell wirksame gesetzgeberische Instrumente zur Regulierung der technischen Entwicklung.[31]

Die Datenminimierung ist ein zentraler Grundsatz des Datenschutzrechts, der jetzt EU-weit einheitlich in Art. 5 Abs. 1c DSGVO normiert ist. Auch in § 71 Abs. 1 Satz 1 BDSG, eine der für Polizei und Strafjustiz maßgeblichen Regelungen, wird der Grundsatz der Datensparsamkeit genannt. Laut Gesetzesbegründung soll diese Regelung sicherstellen, dass die Datenminimierung wirksam umzusetzen ist.[32] Ferner folgt aus § 483 Abs. 1 StPO, dass nur Daten gespeichert werden dürfen, die für das Strafverfahren erforderlich sind. Die gesetzgeberischen Vorgaben im polizeilichen Sektor werden gleichwohl der Bedeutung des Grundsatzes noch nicht gerecht. Anders als in der DSGVO wird der Grundsatz nicht explizit genannt, sondern muss durch Auslegung hergeleitet werden.

Aufgabe des Datenschutzrechts ist es nicht nur, negative Technikfolgen zu mindern, sondern es muss sicherstellen, dass bereits im Vorfeld der Technikentwicklung Einfluss auf die datenschutzfreundliche Ausgestaltung der Anwendungen und Systemstrukturen genommen wird, um Eingriffe in das allgemeine Persönlichkeitsrecht so milde wie möglich zu gestalten oder auszuschließen – *Privacy by Design*, geregelt in Art. 25 DSGVO und § 71 Abs. 2 BDSG.[33] Da viele Prozesse automatisiert ablaufen, ist eine entsprechende Ausgestaltung zunehmend für einen effektiven Datenschutz essentiell. Der Grundsatz *Privacy by Design* spiegelt sich aber noch nicht konkret in den Polizeigesetzen oder in der StPO wider. Da Gesetzgebung und Praxis eine immer umfassendere Datenerhebung und -verarbeitung anstreben und ermöglichen, sollte dieser Grundsatz in allen eingriffsintensiven Gesetzen zur gesetzgeberischen Leitlinie werden.

Zudem stellt sich die Frage, ob Eingriffsnormen neutral, d. h. offen für weitere Technologien sein sollten, oder ob die Gesetzgebung gerade Informationseingriffe

technisch spezifisch regeln sollte. Über das Für und Wider der beiden Ansätze besteht keine Einigkeit.[34] Während einige Autor_innen eine möglichst spezifische und detaillierte Technikregulierung fordern, um den Herausforderungen einzelner Verarbeitungsformen und Verarbeitungsbereiche möglichst exakt begegnen zu können,[35] erscheint dies für andere als innovationsfeindliche Überregulierung.[36] Der Ansatz der deutschen Gesetzgeber bestand bisher überwiegend darin, eine allgemeine, für alle Bereiche der Verarbeitung personenbezogener Daten geltende „Grundregulierung" im BDSG und den Landesdatenschutzgesetzen vorzusehen, daneben aber für bestimmte Technologien und Verarbeitungsbereiche spezifische Regeln zu schaffen. Die spezifischen Regeln orientieren sich dann vielfach an den Besonderheiten einzelner Technologien und normieren konkrete Datenerhebungen in Anwendungsfällen.[37]

Rechtliche Regeln müssen nicht auf jede technische Änderung reagieren, weil sie sich auf Anforderungen an technische Funktionalitäten beziehen, die durch unterschiedliche technische Designs erfüllt werden können.[38] Bei der aktuellen Geschwindigkeit der technischen Entwicklung wäre dies auch nicht zielführend. Ein Eingreifen des Gesetzgebers ist allerdings dann erforderlich, wenn die technische Entwicklung zu einer wesentlich erhöhten oder veränderten Eingriffsintensität führt. Daher sollte bei den Eingriffsgrundlagen nach der Eingriffsintensität differenziert werden und nicht nach einzelnen technischen Anwendungen.[39] Eine inhaltliche Regelung zur Vorsorge gegen technische Risiken muss nicht in der Weise erfolgen, dass technische Details fachsprachlich beschrieben und Beschaffenheitsanforderungen präzise ausgeführt werden oder dass auf eine bestimmte technische Norm Bezug genommen wird. Inhaltliche Anforderungen an die Technik können durch gewünschte Funktionen oder zu erreichende Ziele effektiv umschrieben und begrenzt werden.[40] Je höher die Eingriffsintensität der Technik für die Grundrechte der Betroffen ist, desto präziser und restriktiver müssen die rechtlichen Vorgaben sein.[41]

Fazit

Aufgrund des staatlichen Schutzauftrages für die Grundrechte der Bürger_innen ist es eine staatliche Aufgabe, Vorgaben für die Gestaltung technischer Systeme zu machen, um einen effektiven Grundrechtsschutz sicherzustellen. Der technische Wandel darf nicht als selbstdeterminierter Prozess angesehen werden, an den durch rechtliche Gestaltung die gesellschaftlichen Verhältnisse anzupassen sind. Vielmehr ist gerade die eingriffsintensive Sicherheitsgesetzgebung demokratisch und mit Blick auf einen effektiven Grundrechtsschutz zu steuern.[42] Dieser Beitrag hat gezeigt, dass die technische Gestaltung zu einer Verbesserung der Verwirklichungsbedingungen von Grundrechten beitragen kann.[43] Es ist die Aufgabe der Gesetzgebung, dafür den notwendigen Rahmen vorzugeben.

Die schnelle Entwicklung der polizeilich genutzten Technologien stellt die Gesetzgebung vor Herausforderungen. Sie bietet auch Chancen, Sicherheit effektiver zu gewährleisten und die damit verbundenen Grundrechtseingriffe zugleich zu begrenzen. Die polizeiliche Nutzung von GPS-Daten gestohlener Fahrräder, deren Möglichkeiten und Grenzen im *FindMyBike*-Projekt erforscht wurden, zeigt, dass bereits seit länge-

rem entwickelte Technologien auch durch neue Nutzungsvarianten zu Anwendungsfällen für polizeiliche Informationseingriffe werden können. Es ist nunmehr Aufgabe des Gesetzgebers festzulegen, ob und wie die Daten zur Polizei gelangen und inwieweit die Polizei selbst Daten gestohlener Gegenstände erheben dürfen soll, wenn Ortungstechnologie in dem gestohlenen Gegenstand verbaut ist. Vor dem Hintergrund, dass eine kurzfristige Beobachtung dieser Gegenstände nicht mit schweren Eingriffen verbunden ist – solange keine umfassenden Persönlichkeitsprofile erstellt werden – bestehen gegen eine entsprechende Norm keine grundlegenden verfassungsrechtlichen Bedenken. Denn hier ist nicht nur das staatliche Interesse an einer wirksamen Strafverfolgung relevant, sondern auch das Interesse der Geschädigten, ihr Eigentum zurückzuerlangen.

Das *FindMyBike*-Projekt hat gezeigt, dass Recht und Technik bei der Verwirklichung von Grundsätzen der Datenminimierung und *Privacy by Design* eng kooperieren müssen und können. Greift die Gesetzgebung solche Synergien zwischen Technik und Recht auf, so kann das Repertoire polizeilicher Techniknutzung sinnvoll ergänzt werden, ohne dass weitreichend in Grundrechte eingegriffen wird. Grundrechtschonende technische Lösungen sind also eine sinnvolle Alternative zu dem derzeitigen Trend, das Repertoire polizeilicher Eingriffsbefugnisse im Bereich der Techniknutzung ins Uferlose zu erweitern. Dabei ist stets das Risiko mit zu bedenken, dass einmal vorhandene technische Möglichkeiten in der Behördenpraxis nicht nur im Rahmen des gesetzlich Zugelassenen genutzt werden könnten. Dieses Risiko kann durch technische Voreinstellungen minimiert werden, die eine Nutzung nur im Rahmen des gesetzlich Zulässigen ermöglichen.

PROF. DR. HARTMUT ADEN ist Jurist und Politikwissenschaftler. Er ist Professor für Öffentliches Recht, Europarecht, Politik- und Verwaltungswissenschaft an der Hochschule für Wirtschaft und Recht Berlin, dort stellv. Direktor des Forschungsinstituts für Öffentliche und Private Sicherheit (FÖPS) sowie behördlicher Datenschutzbeauftragter der Hochschule. Webseite: www.hwr-berlin.de/prof/hartmut-aden.

DR. JAN FÄHRMANN studierte an der WWU Münster Jura mit kriminologischem Schwerpunkt. Nach dem Studium schloss sich eine rechtswissenschaftlich-kriminologische Promotion an der FU Berlin sowie ein Referendariat am Kammergericht in Berlin an. Aktuell ist er wissenschaftlicher Mitarbeiter und Dozent am Forschungsinstitut für öffentliche und private Sicherheit an der Hochschule für Wirtschaft und Recht. Seine Forschungsschwerpunkte liegen im Strafvollzugs-, Polizei- (aus strafprozessualer und gefahrenabwehrrechtlicher Perspektive), Datenschutz- und Betäubungsmittelrecht. Aktuelle Veröffentlichungen zu den Themen Resozialisierung im geschlossenen Vollzug (2019), zur Vereinheitlichung des Polizeirechts (gemeinsam mit H. Aden, 2018) sowie zur Polizeirechtsentwicklung und Techniknutzung (gemeinsam mit H. Aden, in ZRP 6/2019).

Literatur

Aden, Hartmut (2017): Anlasslose Personenkontrolle als grund- und menschenrechtliches Problem; in: Zeitschrift für Menschenrechte, S. 55 ff.

Aden, Hartmut/Fährmann, Jan (2018): Polizeirecht vereinheitlichen? Kriterien für Muster-Polizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive, Berlin, URL: https://www.boell.de/sites/default/files/endf_e-paper_polizeirecht_vereinheitlichen.pdf?dimension1=division_demo, zuletzt abgerufen am: 23.8.2019.

Arzt, Clemens (2017): Das neue Gesetz zur Fluggastdatenspeicherung; in: Die Öffentliche Verwaltung (DÖV), S. 1023 ff.

Bieker, Felix/Bremert, Benjamin/Hagendorff, Thilo (2018): Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf; in: Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.): Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung, Wiesbaden, S. 138 ff.

Ehmann, Eugen/Selmayr, Martin (2018): Datenschutz-Grundverordnung, 2. Aufl., München.

Gercke, Björn/Julius, Karl-Peter/Temming, Dieter/Zöller, Mark (2012): Strafprozessordnung, 5. Aufl., Heidelberg.

Gercke, Björn (2006): Einsatz des „Global-Positioning-System" (GPS); in: Roggan, Fredrik/Kutscha, Martin (Hrsg.): Handbuch zum Recht der Inneren Sicherheit, Berlin, S. 403 ff..

Gercke, Björn (2007): Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit; in Computer und Recht (CR) 2007, S. 245 ff.

Hannich, Rolf (Hrsg.) 2019: Karlsruher Kommentar zur Strafprozessordnung. Mit GVG, EGGVG, EMRK, 8. Aufl., München.

Hornung, Gerrit 2005: Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden.

Hornung, Gerrit 2018: Sind neue Technologien datenschutzrechtlich regulierbar? Herausforderungen durch „Smart Everything"; in: Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.): Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung, Wiesbaden, S. 315 ff.

Krüger, Philipp 2016: Datensouveränität und Digitalisierung; in: Zeitschrift für Rechtspolitik (ZRP), S. 190 ff.

Kutscha, Martin 2018: Schutzpflicht des Staates für die informationelle Selbstbestimmung?; in: Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.): Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung, Wiesbaden, S. 123 ff.

Kühne, Hans, Heiner 2001: Beweisgewinnung durch satellitengestütztes funkgesteuertes Navigationssystem. Anmerkung zur BGH-Entscheidung vom 24.1.2001; in: Juristen-Zeitung (JZ), S. 1148.

Puschke, Jens/Singelnstein, Tobias 2005: Verfassungsrechtliche Vorgaben für heimliche Informationsbeschaffungsmaßnahmen; in: Neue Juristische Wochenschrift (NJW), S. 3534 ff.

Nogala, Detlef 1998: Moderne Überwachungstechnologien. Zum Stand der Kunst: in: Bürgerrechte & Polizei/CILIP, Heft 60, S. 6 ff.

Roßnagel, Alexander 1993: Rechtswissenschaftliche Technikfolgenforschung. Umrisse einer Forschungsdisziplin, Baden-Baden.

Roßnagel, Alexander 2008: „Technikneutrale" Regulierung: Möglichkeiten und Grenzen; in: Roßnagel, Alexander/Eifert, Martin/Hoffmann-Riem, Wolfgang (Hrsg.): Innovationsfördernde Regulierung. Innovation und Recht II, Berlin, S. 323 ff.

Schaar, Peter 2017: Trügerische Sicherheit, Hamburg.

Schneider, Hartmut 2014: Münchener Kommentar zur Strafprozessordnung, München.

Singelnstein, Tobias/Stolle, Peer 2012: Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert, 3. Aufl., Wiesbaden.

Tomerius, Carolyn 2017: „Gefährliche Orte" im Polizeirecht – Straftatenverhütung als Freibrief für polizeiliche Kontrollen?; in: Deutsches Verwaltungsblatt (DVBl), S. 1399 ff.

Trute, Hans-Heinrich 2013: Zur Entwicklung des Polizeirechts 2009–2013; in: Die Verwaltung, S. 537 ff.

Vassilaki, Irini 2005: Beweiserhebung und -verwertung bei GPS-Einsatz. Anmerkung zur BVerfG-Entscheidung vom 12.4.2005; in: Computer und Recht (CR), S. 569 ff.

Anmerkungen:

1 Das Projekt wurde 2017 bis 2019 vom Institut für Angewandte Forschung Berlin (IFAF) gefördert und vom Forschungsinstitut für Öffentliche und Private Sicherheit (FÖPS Berlin) der Hochschule für Wirtschaft und Recht sowie der Beuth Hochschule für Technik in Zusammenarbeit mit dem in Berlin ansässigen Unternehmen Noa Technologies GmbH und dem Landeskriminalamt Berlin durchgeführt.

2 Vgl. Kühne 2001: 1148.

3 BVerfG NJW 2005, 1338 (1339 f.); BGH NJW 2001, 1658 (1659) m. w. N.; kritisch Gercke, in: Gercke/Julius/Temming/Zöller 2012, § 100h Rn. 5 m. w. N.; Kühne 2001: 1148.

4 Vgl. zum Begriff der Observation BGH NJW 1998, 1237 (1237).

5 Vgl. EGMR NJW 2011, 1333 (1335); BVerfG NStZ 2003, 441 (442); NJW 2005, 1338 (1339).

6 LG Hildesheim, Beschl. v. 12.3.2008 - 12 Qs 12/08; Günther, in: Schneider 2014, § 100g Rn. 25.

7 AG Friedberg NStZ 2006, 517 (518).

8 Vgl. BGH NStZ 2001, 386 (387).
9 Vassilaki 2005: 572.
10 Z.B. BGHSt. 51, 211 (218); Gercke 2007: 251.
11 BVerfG NJW 2005, 1338 (1340).
12 BVerfG, Beschl. v. 8.11.2012 – 1 BvR 22/12 -, Rn. 25.
13 Vgl. Krüger 2016: 190.
14 Z.B. BVerfGE 6, 32 (41).
15 Aden/Fährmann 2018: 18; Aden 2017: 58; Singelnstein/Stolle 2012: 32.
16 Vgl. dazu Arzt 2017: 1026 f.
17 Schaar 2017: 59 f.
18 Vgl. BVerfGE 141, (220); Tomerius 2017: 1400.
19 Dazu ausführlich Aden/Fährmann 2018: 25 ff.
20 Vgl. Puschke/Singelnstein 2005: 3538.
21 Trute 2013: 558.
22 Bieker/Bremert/Hagendorff 2018: 142; Aden/Fährmann 2018: 22.
23 Roßnagel 1993: 229 f. m. w. N.
24 Vgl. Nogala 1998: 6 f.
25 Roßnagel 1993: 230 f.
26 Hornung 2005: 87.
27 Hornung 2018: 321 f.
28 Roßnagel 1993: 16.
29 Hornung (2018): 322.
30 Singelnstein/Stolle 2012: 32.
31 Vgl. Kutscha 2018: 134.
32 BT-Drs 18/11325, 98.
33 Baumgartner, in: Ehmann/Selmayr 2018, Art. 25 Rn. 9 f.
34 Zur Übersicht über die Debatte Roßnagel 2008: 323 ff.; Hornung 2018: 329.
35 Vgl. z. B. Gercke 2006: 404 ff.
36 Vgl. Roßnagel 2008: 324 ff. m. w. N.
37 Hornung 2018: 329.
38 Hornung 2018: 330.
39 Bruns, in: Hannich 2019, § 100h Rn. 7.
40 Roßnagel 2008: 327.
41 Vgl. Roßnagel 1993: 269.
42 Vgl. Roßnagel 1993: 242.
43 Roßnagel 1993: 225.