Dateneingriffe zur vorbeugenden Kriminalitätsbekämpfung

Teil 1

Von Gerrit Domenghino LL.M., Münster[1]

1 Agieren statt reagieren

„Wenn Terroristen ihre Anschläge per WhatsApp planen, können wir uns kein Polizeigesetz aus dem Wählscheiben-Zeitalter leisten."[2] Mit dieser etwas plakativ wirkenden Aussage hat der NRW-Innenminister Herbert Reul die derzeitige Lage mit wenigen Worten drastisch beschrieben. Während die (organisierte) Kriminalität das Internet und den Missbrauch von Daten längst für ihre perfiden Machenschaften entdeckt und nutzbar gemacht hat, ist die (vorbeugende) Kriminalitätsbekämpfung an die gesetzlichen Vorgaben gebunden. Zwar können sich durch die Entwicklung immer leistungsfähigerer Technik rein faktisch die polizeilichen Eingriffsmöglichkeiten erweitern, ohne dass es einer Veränderung der gesetzlichen Befugnisse dem Wortlaut nach bedarf,[3] doch kann dieses auch kritisch gesehen werden. Denn durch einen rasant – wenn nicht sogar exponentiell – entwickelnden technischen Fortschritt steigt nicht nur die Möglichkeit der Datenerhebung, sondern auch die Gefahr eines Grundrechtseingriffs, vor allem in Hinblick auf das Recht auf informationelle Selbstbestimmung (RIS).

In die Aussage des Innenministers kann auch eine Forderung nach einer steten Anpassung der Polizeigesetze und der darin konkret normierten Eingriffsbefugnisse, sowie eine zeitgemäße Interpretation der verschriftlichten und bis dato zugesprochenen Befugnisse in Hinblick auf die veränderte Lage, hineininterpretiert werden. Selbstverständlich nutzen die Polizeien heute schon in weiten Teilen moderne Technologien wie dienstliche Smartphones, Drohnen oder spezielle Software. Vor allem im Rahmen der Datengewinnung und -verarbeitung werden ihnen jedoch aufgrund rechtlicher Vorschriften oder Bedenken teilweise Hindernisse in den Weg gestellt, die es zu nehmen gilt, und die in manchen Fällen die Polizei auch ins Wanken bringen kann. Im Allgemeinen wird im Beitrag der Fokus auf Maßnahmen der primären und sekundären Kriminalprävention liegen, bei der einerseits die Ursachen der Entstehung von Kriminalität so beeinflusst werden sollen, dass sie von vornherein unterbunden wird, und andererseits Maßnahmen zur Abschreckung potentieller Täter vorsieht, da aufgrund dieser ein erhöhtes Entdeckungsrisiko existiert.[4]

In diesem Teil des zweiteiligen Beitrags wird nach einem historischen Abriss zum Dateneingriff der Blick auf die Online-Streife gelegt, die als einfache Form zur Sichtung von Daten im Rahmen der präventiven Kriminalitätsbekämpfung genutzt werden kann.

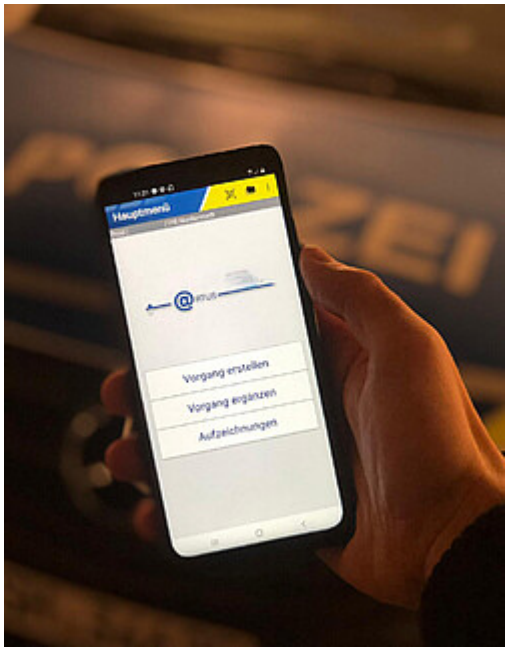
2 Daten sind Gold

„Daten sind das Gold des 21. Jahrhunderts"[5] ist ein geflügelter Ausspruch, der metaphorisch den Wert von Daten in der heutigen Zeit verdeutlichen soll. Unternehmen buhlen öffentlich um die Daten der Menschen, und diese geben sie mehr oder

weniger bewusst preis. So gibt es zum Beispiel in Deutschland über 31 Millionen PAYBACK Kunden, die bereitwillig für ein paar Cent als gläserner Kunde dem in München ansässigen Unternehmen und seinen Partnern eine detaillierte Analyse ihrer Kaufverhalten zugestehen. Auch aus polizeilicher Perspektive sind Daten eine wichtige Informationsquelle, die zur Prognose möglicher Straftaten herangezogen werden kann. Die Sicherheitsbehörden dürfen von einer so offenen Preisgabe persönlicher Daten, wie es im Falle der konsum- und sparorientieren Punktesammler, jedoch nur träumen. Denn gerade ihre *„Kunden“* möchten tunlichst vermeiden, dass zu viel über sie und ihre Machenschaften ans Licht gerät. Also halten sie sich lieber im Dunkeln und versuchen den Sicherheitsbehörden die Jagd auf ihren Daten und auf sich selbst so schwer wie möglich zu machen. Um dennoch an die gewünschten Daten zu gelangen, müssen sich die Sicherheitsbehörden im Rahmen ihrer gesetzlich zugesprochenen Möglichkeiten bewegen, um mithilfe von Daten präventiv zur Kriminalitätsbekämpfung tätig zu werden. Dabei muss der Staat stets die Waage zwischen seiner Schutzpflicht gegenüber den Bürgern und den Grundrechten derselbigen waren.

3 Dateneingriff – Ein Blick zurück

Die heutigen Befugnisse der Sicherheitsdienste in Deutschland sind unter anderem bedingt durch die langen Schatten einer düsteren Zeit. Sowohl die Bürger der ehemaligen Deutschen Demokratischen Republik als auch diejenigen unter uns, die die schrecklichen Zeiten des Nationalsozialismus miterleben mussten, haben noch am eigenen Leib erfahren, was es heißt, in einem Überwachungsstaat zu leben. Vergleichbar weitreichende Befugnisse der Polizei und ihre zentralistische Struktur während des Nationalsozialismus wollten die Besatzungsmächte nach dem Zusammenbruch des Dritten Reichs um jeden Preis verhindern. Neben der Entnazifizierung waren die Demokratisierung der Bevölkerung und die Dezentralisierung der Polizei vorrangige Ziele der Alliierten, was vor allem in den britischen und amerikanischen Besatzungszonen dazu führte, dass es zu einer Beschränkung der polizeilichen Befugnisse und einer *„Entpolizeilichung“* der Verwaltungsrechtsbereiche kam.[6] Auf dieser Grundlage ist die heute in einigen Bundesländern vorzufindende grundsätzliche Trennung zwischen Behörden der allgemeinen Ordnungsverwaltung, die originär für die Gefahrenabwehr zuständig sind, und der Polizei im engeren Sinne, die diese Aufgabe lediglich subsidiär durch den Polizeivollzugsdienst wahrzunehmen hat, zurückzuführen.[7] So gibt es u.a. in Bayern, Berlin, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz und Schleswig-Holstein noch heute grundsätzlich eine organisatorische Trennung der Behörden und ihrer Aufgabenbereiche. Diese organisatorische Trennung findet sich in einigen Ländern auch bei der gesetzlichen Regelung der Eingriffsbefugnisse wieder; wie in Bayern, Brandenburg, Nordrhein-Westfalen und Thüringen, wo es neben den gesetzlichen Vorschriften für die Ordnungsbehörden für die Polizei eigenständige Polizeigesetze (PolG) bzw. Polizeiaufgabengesetze (PAG) gibt. Diese klare Trennung findet sich in den meisten anderen Ländern nicht wieder, wo zwar die Behörden aus organisatorischer Sicht teils klar voneinander getrennt sind, sie für ihr Tätigwerden jedoch auf dasselbe Eingriffsgesetz zurückgreifen.



B 1: Das Smartphone als zeitgemäßes Einsatzmittel der Landespolizei Schleswig-Holstein

Über die Jahre entwickelte sich das Polizeirecht in den einzelnen Bundesländern sowohl aus organisatorischer als auch in materiellrechtlicher Sicht sehr unterschiedlich. Um diesem Flickenteppich Einhalt zu gewähren und eine einheitlich geregelte Verhinderung und Verfolgung von Straftaten zu fördern, gab es schon früh Überlegungen für eine Vereinheitlichung oder zumindest Anpassung der Polizeigesetze der Länder. Dieses Ziel wurde durch die Herausforderungen forciert, die sich durch die Notwendigkeit des Einsatzes von Bundespolizei und Polizeien aus anderen Ländern bei Großveranstaltungen ergaben: die Einsatzkräfte sahen sich mit immer stärker auseinanderdriftenden Rechtsvorgaben am jeweiligen Einsatzort konfrontiert und sollten dennoch rechtssicher handeln. Im Jahre 1972 beschlossen die Innenminister der Länder erstmalig einen Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder (MEPolG), durch den eine einheitliche Fassung geschaffen werden sollte, die sowohl in Fragen des Rechts der Zwangsmittel als auch bei der Anwendung unmittelbaren Zwangs eine gleiche Gesetzesgrundlage schaffen sollte.[8] In diesem ersten MEPolG waren jedoch noch keine Regelungen in Bezug auf die Erhebung und Verarbeitung von personenbezogenen Daten enthalten, da damals die Informationsbeschaffung und -verarbeitung in der Mehrheit der Bevölkerung nicht als Grundrechtseingriff verstanden wurde.[9] Die Einstellung in Bezug auf die Erhebung und Verarbeitung von personenbezogenen Daten sollte sich einige Jahre später jedoch grundlegend ändern. Mit dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) im Jahre 1983 hatte sich Rechtsauffassung durchgesetzt, dass unter *„den Bedingungen der modernen Datenverarbeitung […] der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art 2 Abs 1 in Verbindung mit GG Art 1 Abs 1 umfasst“*[10] wird.

B 2: Smartphones bei der Landespolizei Rheinland-Pfalz.

Diese Entscheidung und das darin erstmalig vom BVerfG umschriebene Grundrecht auf informationelle Selbstbestimmung stärkte bei den Bürgern das Bewusstsein bezüglich ihres Rechts, über die Preisgabe und Verwendung der eigenen personenbezogenen Daten grundsätzlich selbst zu entscheiden.[11] In der Hinsicht war der einige Jahre später entstandene Vorentwurf zur Änderung des MEPolG im Jahre 1985 eine Weiterentwicklung, in dem Fragen bezüglich des Dateneingriffs Berücksichtigung fanden. Der Vorentwurf stieß jedoch auch auf Kritik, denn eine Beschränkung der Maßnahme gegen Störer war nicht explizit formuliert, so dass die Befürchtung geäußert wurde, dass jedermanns Daten erhoben werden könnten, sobald es im Sinne der polizeilichen Aufgabe der (abstrakten) Gefahrenabwehr als nötig erachtet würde, und dadurch letztlich eine Erweiterung und Vorverlagerung der polizeilichen Eingriffsmaßnahmen erfolgt.[12] In dem aktuell in Entstehung befindlichen MEPolG finden sich indes – wie in den Polizei(aufgaben)gesetzen – mannigfaltige Regelungen zum Dateneingriff, bei denen auch zukünftige Entwicklungen in der Informationstechnik bestmöglich Berücksichtigung gefunden haben. Denn letztlich muss es das Ziel sein, *„eine möglichst ländereinheitliche polizeiliche Datenerhebung und Datenverarbeitung im Präventiven Bereich auf klarer gesetzlicher Grundlage zu erhalten.“*[13] Ansonsten besteht die Gefahr, dass Kriminelle ihren Tätigkeitsort innerhalb der Bundesrepublik dorthin verlegen, wo Ihre Machenschaften keinen oder den vergleichsweisen geringsten strafrechtlichen Folgen unterworfen sind.

B 3: Smartphone statt Merkbuch: Der Hamburger Polizeipräsident Ralf Martin Meyer übergibt 1.400 Diensthandys.

4 Online-Streife als präventive Maßnahmen zur Kriminalitätsbekämpfung

Die Aufgabe der Polizei ist es, Gefahren für die öffentliche Sicherheit und Ordnung abzuwehren und im Rahmen dieser Aufgabe Straftaten zu verhindern sowie präventiv zu bekämpfen.[14] Um diesem nachzukommen und bei der Bevölkerung das Sicherheitsgefühl zu steigern, ist die Polizeistreife – sei es zu Fuß, auf dem Fahrrad oder motorisiert – ein probates Mittel, da der Bürger durch die Präsenz eines uniformierten Beamten den Eindruck gewinnt, dass der Staat sein Gewaltmonopol wahrnimmt, als direkter Ansprechpartner zur Verfügung steht und zwielichtige Personen von möglichen Straftaten und Ordnungswidrigkeiten abgeschreckt werden. Neben der Gefahrenabwehr, die als präventive Maßnahme einen potentiellen Schadenseintritt verhindern möchte, hat die Polizei auch die repressive Aufgabe der Strafverfolgung, sprich im Nachgang zu einer begangenen Straftat oder Ordnungswidrigkeit den Verantwortlichen zu identifizieren. Dabei ist die Abgrenzung zwischen präventiven und repressiven Maßnahmen der Polizei nicht immer einfach und die Übergänge teilweise fließend, so dass eine Beurteilung am konkreten Einzelfall vorgenommen werden muss.[15] Relevant ist die Unterscheidung in Hinblick auf die Ermächtigungsgrundlage, denn handelt es sich um eine präventive Maßnahme, ist in der Regel eine Norm aus dem Polizei(aufgaben)gesetz einschlägig, hingegen dürfte die repressive Handlung im Normalfall auf die Strafprozessordnung gestützt sein. Es gibt jedoch Maßnahmen, bei denen von vornherein sowohl präventive als auch repressive Elemente denkbar sind und somit eine Mischform vorliegt. Zu einer solchen Doppelfunktionalität des polizeilichen Handels kann es kommen, wenn mit ein und derselben Maßnahme einerseits mögliche Gefahren beseitigt werden sollen, und andererseits die Verursacher verantwortlich gemacht und sanktioniert werden sollen.[16] Ein Beispiel für eine solche doppelfunktionale Maßnahme ist die sogenannte *„Online-Streife“.*

4.1 Online-Streife – Eine Begriffsbestimmung

Wenn ein Mitarbeiter der Polizei im Internet öffentlich zugängliche Bereiche sichtet, wird dieses als Online-Streife, Internetstreife oder hoheitliches Surfen bezeichnet. Dass das Internet kein rechtsfreier Raum ist,[17] dürfte inzwischen jedem bekannt sein. Anders aber als in der realen Welt, scheint die Hemmschwelle für Straftaten verschiedenster Couleur im Netz niedriger zu sein. Dies mag daran liegen, dass sich die Täter dort durch die (gefühlte) Anonymität in Sicherheit wägen und dadurch ein anderes Verhalten an den Tag legen, als sie es im wirklichen Leben tun würden. In einer Gesellschaft, die das Internet und mobile Kommunikation als Selbstverständlichkeit ansieht und diese Technik tagtäglich nutzt, sollte es ebenso selbstverständlich sein, dass auch der Staat im Rahmen der Gefahrenabwehr diese Bereiche regelmäßig frequentiert. Die Online-Streife ist als polizeiliche Maßnahme derweil nicht so neuartig, wie man vielleicht denken könnte. Seit längerem zählt sie zu den üblichen Maßnahmen der Polizei zu Präventionszwecken im Internet.[18] Bereits 1998 gab es im Landtag von Nordrhein-Westfalen Stimmen die forderten, dass Polizeibeamte im Internet auf Streife gehen sollten; primär um Kindesmissbrauch und

Kinderpornographie effektiver zu verfolgen und wirksamer zu bestrafen.[19] Die Polizei sollte technisch und personell so ausgestattet werden, dass sie dazu befähigt ist, zur Gefahrenabwehr anlassunabhängig im Internet zu surfen. Doch schon damals gab es Zweifler, die es als Illusion bezeichneten, dass die bundesrepublikanische Polizei oder gar eine Polizeidienstelle in der Lage wäre, das Internet effektiv zu überwachen.[20] Diese Bedenken dürften auch heute noch bestehen und beim Blick auf die rasante Entwicklung des Internets und der dort eingespielten Datenmenge noch größer geworden sein. Dass die Streife im Internet nicht so schnell zur Selbstverständlichkeit und zu einem Mittel der effektiven Gefahrenabwehr geworden ist, wie es wünschenswert gewesen wäre, kann man auch aus den politischen Zielen ableiten, die immer wieder formuliert wurden. So vereinbarten beispielsweise die Parteien der Bundesregierung in ihrem Koalitionsvertrag im Jahr 2009, dass gemeinsam mit den Ländern durch den Einsatz von Internetstreifen durch die Polizei eine verbesserte Strafverfolgung in Kommunikationsnetzen erreicht werden solle.[21] Vergleichbar mit der Streifenfahrt in der realen Welt, soll durch die Präsenz von Polizeibeamten im virtuellen Raum sowohl eine gewisse Abschreckung in Bezug auf potentielle Straftäter erzeugt, sowie bei einer Straftat oder Gefahrensituation schnell reagiert werden, als auch ein Sicherheitsgefühl beim Bürger gestärkt werden, dem der Beamte als Ansprechpartner zur Verfügung steht.[22]

4.2 Rechtliche Einordnung

Nun kann man sich die Frage stellen, ob durch die Internetstreife ein Grundrechtseingriff erfolgt, für den es einer entsprechenden Ermächtigungsbefugnis bedarf, die das Handeln der Polizei legitimiert. Am naheliegendsten ist ein Eingriff in das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG als auch eine Verletzung des allgemeinen Persönlichkeitsrechts und speziell das RIS gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Das BVerfG hat in einer Entscheidung im Jahr 2002 konstatiert, dass *„unter einem Grundrechtseingriff im Allgemeinen ein rechtsförmiger Vorgang verstanden [wird], der unmittelbar und gezielt (final) durch ein vom Staat verfügtes, erforderlichenfalls zwangsweise durchzusetzendes Ge- oder Verbot, also imperativ, zu einer Verkürzung grundrechtlicher Freiheiten führt.“*[23] Diese Auffassung wurde weiterentwickelt, wobei der Fokus auf die Bewertung der Wirkung staatlichen Handelns gelenkt wurde. So kann bereits ein Grundrechtseingriff vorliegen, wenn es dem Grundrechtsträger aufgrund von Staatshandeln nicht mehr möglich ist, seine Grundrechte in vollem Umfang zu verwirklichen, diese Beeinträchtigung dem Staat zuzuschreiben ist und sie eine bestimmte Erheblichkeit aufweist.[24] In Hinblick auf die Sichtung des Internets hat das BVerfG in seiner Entscheidung zur Online-Durchsuchung aus dem Jahre 2008 jedoch festgestellt, dass der Staat nicht in Grundrechte eingreift, wenn er im Internet öffentlich zugängliche Kommunikationsinhalte wahrnimmt oder sich dort an öffentlich zugänglichen Kommunikationsvorgängen beteiligt.[25] Somit lässt sich festhalten, dass durch eine reine Online-Streife noch kein Grundrechtseingriff vorliegt. Denn Nutzer des Internets und sozialer Netzwerke, die freiwillig ihre personenbezogenen Daten der Öffentlichkeit oder zumindest einem nicht weiter abgegrenzten Personenkreis zu Verfügung stellen, dürfen nicht darauf vertrauen, dass Behörden diese Inhalte nicht beobachten.[26] Aufgrund des nicht vorhandenen Grundrechtseingriffs und fehlender Spezialbefugnisse für eine schlichte Sichtung der im Internet verfügbaren Inhalte kann diese Maßnahme aufgrund der allgemeinen Aufgabenzuweisung in den Polizei(aufgaben)gesetzen erfolgen. Sollten im Rahmen der Sichtung Auffälligkeiten zu einer gezielten Suche im Netz führen, kann dieses auf Grundlage der Generalklausel erfolgen. Würden die im Zuge der allgemeinen Sichtung der öffentlich zugänglichen Bereiche des Internets gewonnen Informationen jedoch gezielt zusammengetragen, gespeichert und – gegebenenfalls durch die Kombination mit weiteren Daten – ausgewertet, dann besteht dadurch die (abstrakte) Gefahr der Erstellung eines Persönlichkeitsprofils der betroffenen Personen und somit einer spezifischen grundrechtlichen Gefährdungslage für das RIS.[27]

4.3 Einsatz gegen Hasskriminalität

Der Einsatzbereich der Online-Streife zur präventiven Kriminalitätsbekämpfung ist sicherlich begrenzt, doch kann die Maßnahme durchaus dort einen Erfolg erreichen, wo ein mahnendes Wort oder allein die Präsenz von Polizei seine Wirkung zeigt. In den vergangenen Jahren ist es nach Ansicht der Bundesregierung im Internet und insbesondere in den sozialen Netzwerken zunehmend zu einer Verrohung der Kommunikation gekommen.[28] Diese Art der verbalen Entgleisung wird in seiner extremen Ausprägung auch als Hasskriminalität bezeichnet und allgemein als ein Teil der politisch motivierten Kriminalität verstanden.[29] Um dieser effektiv begegnen zu können wurde das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität verabschiedet, welches zum 1. Januar 2021 in Kraft treten sollte. In dessen Entwurf wurde das Problem der Hasskriminalität ausführlich beschrieben: Im Internet werden gegenüber Personen – häufig solche, die als Repräsentanten für das Gemeinwesen tätig sind – vermehrt diffamierende Äußerungen oder Morddrohungen ausgesprochen oder zu Gewalt gegenüber diesen aufgerufen.[30] Hier kann man die Chance sehen, dass im Bereich der Hasskriminalität die Online-Streife in sozialen Netzwerken frühzeitig eingreifen und Diskussionen durch gezielte Kommentare sowie das Zeigen von Präsenz einfangen kann, bevor die Nutzer und die Stimmung eskalieren. In Anbetracht der schon heute und in Zukunft noch wachsenden Menge von potentiell strafbaren Inhalten sind die Sicherheitsbehörden mit einer Herausforderung konfrontiert, die nicht nur die Polizeien der Länder, sondern auch die Staatsanwaltschaften und die Gerichte mehr als auslasten könnten, so der Präsident des Bundeskriminalamts Holger Münch.[31] Um diesen Datenmengen Herr zu werden, bedarf es sicherlich

leistungsfähiger Software, die mit Hilfe von lernenden Algorithmen und künstlicher Intelligenz die Sicherheitsbehörden bei ihrer Arbeit unterstützen. Manchmal genügt es aber auch schon Schlüsselfiguren zu identifizieren und *„einzufangen“*, um einen Erfolg zu verzeichnen. So hat eine durchgeführte Hasskommentaranalyse von insgesamt 14.000 Kommentaren u.a. ergeben, dass rund 50% der Hasskommentare von lediglich 5% der Accounts befeuert wurden. Hier könnte die Online-Streife im Sinne der aus anderen Bereichen bekannten Taktik der *„[100] Nadelstiche“* eine Möglichkeit darstellt, dem Phänomen der Hasskriminalität entgegen zu treten.

4.4 Sichtbarkeit der Online-Streife

Wenn die vorbeugende Bekämpfung von Straftaten durch die Maßnahme der Online-Streife unterstützt werden soll, dann bedarf es im Sinne der Verhütung im Internet aber auch einer sichtbaren Polizeipräsenz, die in den kriminellen Milieus eine Verunsicherung weckt. Erst wenn diese nicht mehr das Gefühl der absoluten Überlegenheit haben, kann der Effekt eintreten, dass potentielle Täter nicht zu Tätern werden. Im digitalen Raum ist diese Sichtbarkeit ungleich schwerer zu bewerkstelligen, da die Erkennbarkeit als Polizeibeamter nicht so offensichtlich ist. Bisher werden in Deutschland mit der Polizeipräsenz im Internet primär zwei Ziele verfolgt: zum einen wird im Internet - nicht für jedermann ersichtlich – von Mitarbeitern der Polizei *„gesurft“*, um potentielle Straftaten oder Ordnungswidrigkeiten ausfindig zu machen und zu ahnden, zum anderen werden mit Hilfe von Social-Media-Accounts der Polizei Informationen verbreitet. Zwar ist hier in Hinblick auf die Nutzung des Internets als Kommunikationsplattform eine positive Entwicklung zu verzeichnen, da die Anzahl der Accounts von rund 130 im Jahr 2016[32] auf 330 im Jahre 2018[33] gestiegen ist. Da dieses Medium in erster Linie aber für Kommunikationszwecke genutzt wird, dürfte ein Effekt im Sinne einer präventiven Gefahrenabwehr kaum gegeben sein. Ein weitaus besseren Wirkungsgrad kann das in Deutschland noch nicht sehr weit verbreitete Konzept des *„digital community policing“* entwickeln, bei dem sich einzelne Polizeibeamte mit dienstlichen Accounts im Internet und speziell sozialen Netzwerken registrieren und dort Präsenz zeigen. Dadurch können sie mit dem Bürger in Kontakt treten, sind Ansprechpartner, bieten Präventionstipps oder geben Verhaltensanweisungen in konkreten Gefahrensituationen.[34] In den Niederlanden waren 2018 bereits rund 3.400 Beamten als sogenannte *„wijkagenten“* im Netz unterwegs und 2.200 hatten einen Twitter-Account,[35] gegenwärtig hat beispielsweise Niedersachen – im Verhältnis ungefähr die Hälfte an Einwohnern und Polizisten – vergleichbare Accounts im niedrigen zweistelligen Bereich.[36]

5 (Zwischen)Fazit

Der Dateneingriff zur präventiven Kriminalitätsbekämpfung ist in der heutigen Zeit als polizeiliche Maßnahme nicht mehr wegzudenken. Sowohl für den Bürger als auch für den Polizeivollzugsbeamten muss der virtuelle Raum klar als ein Bereich anerkannt werden, in dem Gesetz und Ordnung genauso gelten, wie in der realen Welt. Die Online-Streife ist nur der erste Schritt in die digitale Welt, aber einer der konsequent und sichtbar begangen werden muss, um das darin innewohnende Potential auszuschöpfen. Die technische Entwicklung fordert hier jedoch ihren Tribut durch immer präziser zu formulierende Normen für Eingriffsmaßnahmen, um dem Bestimmtheitsgrundsatz gem. Art. 20 Abs. 3 GG zu entsprechen. Im zweiten Teil des Beitrags wird folglich ein Blick auf ausgewählte Spezialbefugnisse der Polizei für Standardmaßnahmen geworfen, um dabei speziell Entwicklungen der jüngsten Zeit zu betrachten. Den um in Deutschland und Europa einen Raum der Freiheit, der Sicherheit und des Rechts zu wahren, ist es auch in Hinblick auf die präventive Kriminalitätsbekämpfung Aufgabe der Sicherheitsbehörden vor die Lage zu kommen, denn auch hier gilt: *„Stillstand ist Rückschritt.“*[37]

Bildrechte: T. Gründemann/GdP (B 1); Pressestelle PP Rheinpfalz (B 2); Pressestelle PP Hamburg (B 3).

Anmerkungen

1. Gerrit Domenghino LL.M. ist Wissenschaftlicher Mitarbeiter im Fachgebiet III.4 (Öffentliches Recht mit Schwerpunkt Polizeirecht) an der Deutschen Hochschule der Polizei in Münster.
2. Vgl. Ministerium des Inneren des Landes Nordrhein-Westfalen, online verfügbar unter: www.im.nrw/themen/polizei/sicherheitspaket-i-ein-zeitgemaesses-update-fuer-unser-polizeigesetz.
3. Fährmann, Jan/Aden, Hartmut/Bosch, Alexander, Kriminologisches Journal, 52. Jg, 2020, S. 135.
4. Vgl. Möllers, Martin, Wörterbuch der Polizei, 3. Aufl., C.H.Beck, München, 2018, S. 1751 f.

5. Hartmann, Matthias, Vorstandschef des Marktforschungsunternehmens GfK, online verfügbar unter: www.welt.de/wirtschaft/article127418980/Daten-sind-das-Gold-des-21-Jahrhunderts.html.
6. Schmidt, Rolf, Polizei- und Ordnungsrecht, 19. Aufl., Verlag Dr. Rolf Schmidt GmbH, Grasberg, 2017, Rn. 13.
7. Ebd., Rn. 14.
8. Vgl. Walter, Bernd, Die Hoffnung stirbt zuletzt - das mühsame Ringen um ein neues Musterpolizeigesetz, Kriminalistik 4/2019, S. 243, 244.
9. Schmidt, Rolf, Polizei- und Ordnungsrecht, 19. Aufl., Verlag Dr. Rolf Schmidt GmbH, Grasberg, 2017, Rn. 43.
10. BVerfG, Urteil vom 15.12.1983, – 1 BvR 209/83 – , BVerfGE 65, 1 - 71.
11. Ebd.
12. Vgl. CILIP, Ausgabe 2-1985, NEUES POLIZEIRECHT – Redaktionelle Stellungnahme zum Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder: Fassung vom 8.2.1985, S. 34f., online verfügbar unter: archiv.cilip.de/Hefte/CILIP_021.pdf.
13. Bundesministerium für Justiz, Große Strafrechtskommission des Deutschen Richterbundes, Gutachten zu dem Thema: Das Verhältnis von Gericht, Staatsanwaltschaft und Polizei im Ermittlungsverfahren, strafprozessuale Regeln und faktische (Fehl-?)Entwicklungen, online verfügbar unter: www.bmjv.de/SharedDocs/Downloads/DE/Fachinformationen/Das_Verhaeltnis_von_Gericht_Staatsanwaltschaft_und_Polizei_im_Ermittlungsverfahren.pdf.
14. Vgl. dazu etwa § 1, 2 PolG BW, Art. 2, 3 PAG Bay, § 1 ASOG Bln, § 1 Bbg PolG, § 1 Brem PolG, § 3, § 3 Hmb SOG, § 1 PolG NRW.
15. Thiel, Markus, Polizei- und Ordnungsrecht, 4. Aufl., Nomos, Baden-Baden, 2020, § 4 Rn. 17.
16. Ebd., Rn. 20.
17. So etwa die Bundeskanzlerin Angela Merkel in Ihrem Podcast zum Safer Internet Day, online verfügbar unter: www.bundesregierung.de/breg-de/mediathek/kanzlerin-podcast/merkel-das-internet-ist-kein-rechtsfreier-raum--1007676.
18. Vgl. BT-Drucksache 17/6587.
19. Vgl. Landtag NRW, Landtag intern, Plenarbericht, 29. Jahrgang, Ausgabe 18 vom 24.11.1998, S. 9, online verfügbar unter: www.landtag.nrw.de/portal/WWW/Webmaster/GB_II/II.1/Oeffentlichkeitstsarbeit/Landtag_Intern/landtag_intern.jsp.
20. So etwa der ehemalige Landtagsabgeordnete Roland Appel von der Fraktion Die Grünen, Landtag NRW, Landtag intern, Plenarbericht, 29. Jahrgang, Ausgabe 18 vom 24.11.1998, S.9, online verfügbar unter: www.landtag.nrw.de/portal/WWW/Webmaster/GB_II/II.1/Oeffentlichkeitstsarbeit/Landtag_Intern/landtag_intern.jsp.
21. Vgl. Koalitionsvertrag zwischen CDU, CSU und FDP, 17. Legislaturperiode, S. 101, online verfügbar unter: www.kas.de/de/web/geschichte-der-cdu/koalitionsvertraege.
22. Biemann, Jens, „Streifenfahrt“ im Internet, Richard Boorberg Verlag, 2013, S. 22.
23. BVerfG, Urteil vom 26.6.2002, - 1 BvR 670/91 -, R. 68.
24. Oermann, Markus/Staben, Julian, Mittelbare Grundrechtseingriffe durch Abschreckung? Zur grundrechtlichen Bewertung polizeilicher „Online-Streifen“ und „Online-Ermittlungen“ in sozialen Netzwerken, in: Der Staat, Duncker & Humbolt, Berlin, 2013, S. 630, 637
25. BVerfG, Urteil vom 27.2.2008, - 1 BvR 370/07 -, - 1 BvR 595/07 -, 5. Leitsatz.
26. Ebd., Rn. 308.
27. Ebd., Rn. 309.
28. Vgl. BT-Drucksache 19/17741.
29. Vgl. Möllers, Martin, Wörterbuch der Polizei, 3. Aufl., C.H.Beck, München, 2018, S. 1694 f.
30. Vgl. BT-Drucksache 19/17741.
31. Vgl. Münch, Holger, Innere Sicherheit weiterdenken, Kriminalistik 1/2020, S. 3, 6.
32. Statista, Anzahl der Social-Media-Accounts der Polizei in Deutschland in den verschiedenen Social-Media-Kanälen nach Bundesländern im Jahr 2016, online verfügbar unter: de.statista.com/statistik/daten/studie/613454/umfrage/social-media-accounts-der-polizei-in-deutschland-nach-bundeslaendern/.

33. Bouhs, Daniel/ Reisin, Andrej, Polizei betreibt über 330 Social-Media-Profile, 2018, online verfügbar unter: www.ndr.de/fernsehen/sendungen/zapp/Polizei-betreibt-ueber-330-Social-Media-Profile,polizei5110.html.
34. Rüdiger, Thomas-Gabriel, Polizei im digitalen Raum, Bundeszentrale für politische Bildung, 2019, online verfügbar unter: www.bpb.de/apuz/291183/polizei-im-digitalen-raum.
35. Vgl. Vandeputte, Bram, In Nederland patrouilleert de wijkpolitie ook op het internet, 2018, online verfügbar unter: www.vrt.be/vrtnws/nl/2018/02/14/digitale-wijkagent.
36. Vgl. Polizei Niedersachen, Digitales Community Policing, online verfügbar unter: www.polizei-nds.de/wir_ueber_uns/polni_socialmedia/digital.community.policing/digital.community.policing-112171.html.
37. Ein Ausspruch geprägt von Rudolf Christian von Bennigsen-Foerder, deutscher Industriemanager und langjähriger Vorstandsvorsitzender der VEBA AG.