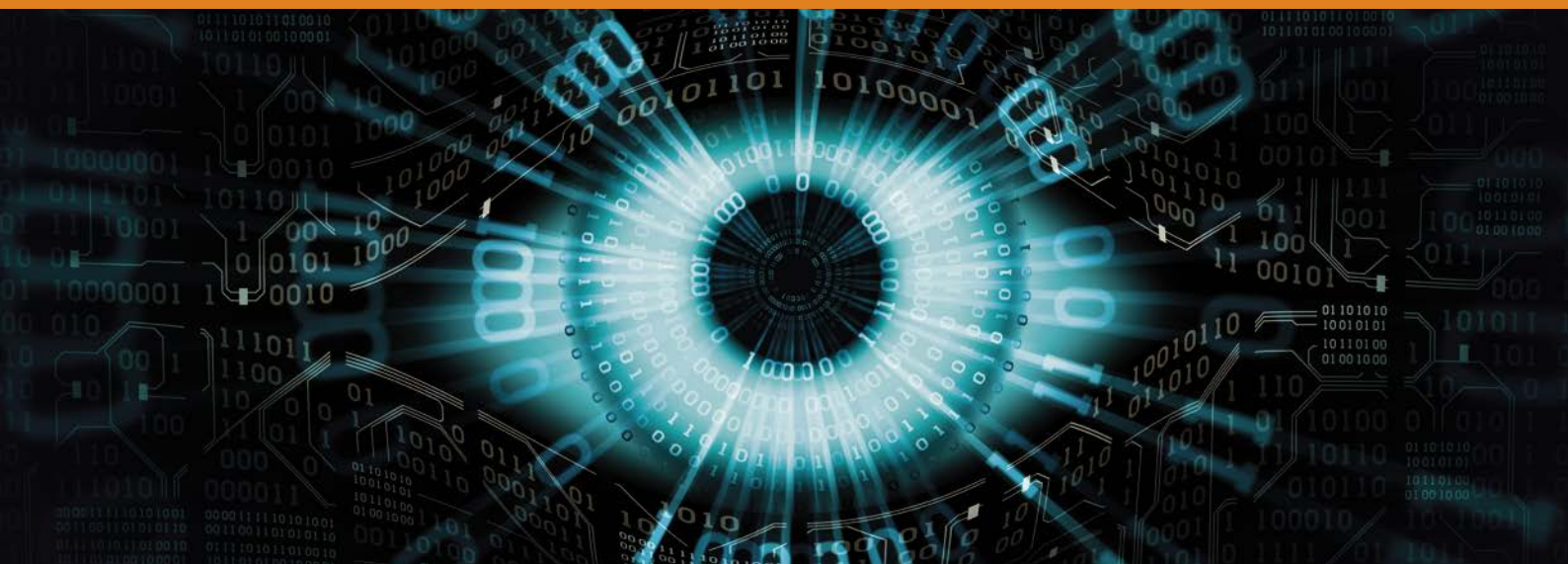


SKP INFO

2 | 2021

DAS MAGAZIN DER SCHWEIZERISCHEN KRIMINALPRÄVENTION

Thema
Überwachung



Liebe Leserin, lieber Leser



SKP

Wer das Wort «Überwachung» hört, denkt wahrscheinlich zuerst einmal an «Big Brother»: an einen Feind der Privatsphäre, an ein potentes Unterdrückungsinstrument der Mächtigen. Oder auch an die gleichnamige Fernsehshow, in der die Privatsphäre zur Belustigung des Publikums von den Teilnehmenden freiwillig aufgegeben wird. Das sind schon mal zwei wichtige Aspekte, die auch in dieser Ausgabe des SKP INFO näher

beleuchtet werden: Erik Schönenberger (Geschäftsführer der Digitalen Gesellschaft) warnt in einem Interview vor dem staatlichen Einsatz von Überwachungstechnik ohne die entsprechenden recht(sstaat)lichen Grundlagen; und der politisch aktive Schriftsteller Jürg Halter weist in einem anderen Interview auf das merkwürdige Missverhältnis hin, dass viele Menschen einerseits ständig und freiwillig private Daten preisgeben, z. B. in den Social-Media-Kanälen, und andererseits in der COVID-Krise nicht mithelfen, eine Kontaktverfolgung zu ermöglichen, weil sie einen Missbrauch ihrer Daten befürchten. Für eine verstärkte und differenzierte Rechtsprechung bei der Frage, wer wen wann filmen darf, plädiert in seinem Beitrag der Anwalt Martin Steiger – in einer Zeit, in der gefühlt jeder jeden immer filmt.

Überwachung als Instrument zur Kriminalitätsbekämpfung wird in Form des «Cyber Patrolling» immer wichtiger (dazu die NEDIK-Analystin Tamara Schmid), und wie das «Electronic Monitoring» (umgangssprachlich «Fussfessel») in Zukunft auch gegen häusliche Gewalt und Stalking eingesetzt werden könnte, erläutern Alain Hofer (Stv. GS-KKJPD) und Janine Repetti-Dittes (Verein Electronic Monitoring). Ausserdem berichtet Nadja Capus (Professorin an der Uni Neuenburg) über die technischen und rechtlichen Schwierigkeiten, denen sich Sprachmittler/innen bei der Echtzeit-Überwachung von Verbrecher-Kommunikation ausgesetzt sehen; sie erforscht dieses hochinteressante Nischenthema mit dem Ziel, Standards für die Praxis entwickeln zu können. Und schliesslich werfen wir noch einen juristischen Blick darauf, worauf überall Drohnen mittlerweile einen Blick werfen können, sollen, dürfen: Dazu die Autorinnen Sandra Bodmer und Amanda Boekholt in ihrem Artikel.

Wir sehen sofort, dass Überwachung so viele Gesichter hat, dass wir in diesem SKP INFO nur ein ganz paar ausgewählte davon zeigen können. Dass eine gelungene Überwachung neben Straftaten z. B. auch Verkehrsunfälle und Umweltkatastrophen verhindern kann, für den Luftraum unabdingbar ist und vor allem in der Medizin täglich Leben rettet, sollte nicht vergessen werden! Wichtig ist, dass sie immer auf einer stabilen Rechtsgrundlage stehen muss und dass demokratisch überprüfbar bleibt und auch tatsächlich überprüft wird, wie die erhobenen Daten verwendet werden.

Ich wünsche Ihnen eine anregende Lektüre!

Fabian Ilg

Geschäftsleiter Schweizerische Kriminalprävention

IMPRESSUM

Herausgeberin und Bezugsquelle

Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
Postfach
3001 Bern

info@skppsc.ch
Tel. 031 511 00 09

Das **SKP INFO 2 | 2021** ist als PDF-Datei zu finden unter:
www.skppsc.ch/skppinfo. Es erscheint auch
in französischer und italienischer Sprache.

Verantwortlich Chantal Billaud,
Stv. Geschäftsleiterin SKP

Redaktion, Interviews Volker Wienecke, Bern

Übersetzungen **F** ADC, Vevey
I Annie Schirrmeister, Massagno

Layout Weber & Partner, Bern

Druck Länggass Druck AG, Bern

Auflage D: 1350 Ex. | F: 300 Ex. | I: 250 Ex.

Erscheinungsdatum Ausgabe 2 | 2021, Juli 2021

© Schweizerische Kriminalprävention, Bern

«Ist die Schweiz ein Überwachungsstaat, Herr Schönenberger?»

Ein Gespräch mit dem IT-Security-Spezialisten Erik Schönenberger über die derzeitige Praxis (und die Frage nach deren Rechtmässigkeit) bei verschiedenen Überwachungsinstrumenten wie Vorratsdatenspeicherung, Kabelaufklärung und Gesichtserkennung in der Schweiz. Herr Schönenberger ist Geschäftsleiter der Digitalen Gesellschaft, die er auch mitinitiiert hat.

Ist die Schweiz ein Überwachungsstaat, Herr Schönenberger?

Ja, das könnte man schon so sagen. Denn in der Schweiz werden nach und nach Massenüberwachungsprogramme eingeführt und ausgebaut, wie die Vorratsdatenspeicherung oder die Kabelaufklärung.

Wie funktioniert die Vorratsdatenspeicherung?

Die Vorratsdatenspeicherung umfasst die Daten, die belegen, wer wann wen angerufen und wie lange das Gespräch gedauert hat, wer sich wann ins Internet eingeloggt hat und für welche Dauer, wer wann wem ein E-Mail oder SMS geschickt hat. Wird ein Mobiltelefon verwendet, werden auch die Standortinformationen des Telefons gespeichert. Alle diese Informationen müssen für sechs Monate abgelegt und auf Verlangen an Strafverfolgungsbehörden oder den Geheimdienst herausgegeben werden.

Die Provider müssen also das Kommunikationsverhalten ihrer Kundinnen und Kunden für sechs Monate festhalten. Ursprünglich wurde damit die Kommunikation zwischen Menschen aufgezeichnet, welche detaillierte Beziehungsnetze offenbarte. Mittlerweile wird bereits ein Datensatz für jede



Erik Schönenberger, IT-Security-Spezialist und Geschäftsleiter der Digitalen Gesellschaft

Kommunikation angelegt, die ein Smartphone macht. Also auch dann, wenn eine App im Hintergrund prüft, ob eine neue Nachricht eingetroffen ist.

Der Zugriff auf die Daten ist bereits beim Vorliegen eines Verdachts zu jedem Verbrechen oder Vergehen möglich. Zusätzlich werden die Vorratsdaten auch

für sogenannte Antennensuchläufe verwendet, also einer Rasterfahndung bei Tatverdacht gegen «Unbekannt». Dabei soll herausgefunden werden, wer zu einem definierten Zeitpunkt an einem bestimmten Ort war und eine Straftat begangen haben könnte. Damit sind u. U. Personen angehalten, ihre Unschuld zu beweisen, wenn ihr Handy zum untersuchten Zeitpunkt in eine der untersuchten Funkzellen eingebucht war. Es ist ein Fall bekannt, bei dem die Mobilfunkanbieterin über 150 000 Verbindungsdaten geliefert hat.

Dabei besteht nach wie vor keine genügende Rechtsgrundlage für den Antennensuchlauf. Die Überwachung einer Person darf nur angeordnet werden, wenn ein konkreter Tatverdacht gegen sie besteht. Oft wird die Vorratsdatenspeicherung damit begründet, dass die Untersuchungsbehörden bei Straftaten im Internet «gleichlange Spiesse» wie die Straftäter benötigen. Bei dieser Überwachungsmassnahme geht es jedoch gerade nicht um Straftaten im Internet. Vielmehr werden zusätzliche Ermittlungswerkzeuge geschaffen, indem unsere Smartphones als Ortungswanzen missbraucht werden.

Und wie funktioniert die Vorratsdatenspeicherung im Internet?

Mit der Vorratsdatenspeicherung gilt auch eine Identifikationspflicht. Zudem müssen zugewiesene IP-Adressen sechs Monate gespeichert werden. Diese sind für die Kommunikation im Internet notwendig und einem bestimmten Anschluss, also beispielsweise einem ADSL-Modem oder TV-Kabel, zugewiesen. Da die IP-Adressen knapp sind, werden in Public WLAN und Mobilfunknetzen diese meist geteilt. Die Technologie nennt sich Network Address Translation (NAT). Die Provider müssen diese Übersetzungstabellen ebenfalls sechs Monate aufbewahren. Und nun explodieren auch hier die Datensätze: Wir sprechen nun von einer Milliarde NAT-Übersetzungsvorgängen pro Mobilfunknetz und Tag!



123RF/Kheng Ho Toh

«Die Beschwerde gegen die Vorratsdatenspeicherung ist – mit guter Aussicht auf Erfolg – in Strassburg hängig.»

Was ursprünglich als Identifikation gedacht war, führt nun zur Überwachung unserer Internetnutzung, da der Dienst Überwachung Post- und Fernmeldeverkehr (ÜPF) verlangt, nicht nur den Übersetzungsvorgang an sich, sondern zusätzlich auch noch die Zieladressen zu speichern. Mit diesen Daten können nun alle besuchten Webserver und verwendeten Internetdienste einer Person nachvollzogen bzw. alle Benutzer eines Dienstes oder Servers festgestellt werden.

Aber werden diese Daten nicht zur Verbrechensaufklärung benötigt?

Leider gibt es nur wenige Studien, welche die Notwendigkeit der Vorratsdatenspeicherung zur Verbrechensbekämpfung untersuchen. Das Max-Planck-Institut kommt in einem Gutachten im Auftrag des deutschen Bundesamtes für Justiz zu dem Schluss, dass die in der Schweiz praktizierte Vorratsdatenspeicherung zu keiner systematisch höheren Aufklärung geführt hat. Eine Einschränkung von Grundrechten ist jedoch unrechtmässig, wenn die Nützlichkeit der Massnahme nicht nachgewiesen ist oder werden kann!

Wie wir sehen, betrifft die Vorratsdatenspeicherung ausnahmslos alle Menschen. Sie stellt einen schwerwiegenden und unverhältnismässigen Eingriff in den verfassungsmässig garantierten Schutz der Privatsphäre dar und gefährdet auch das Anwalts-, Arzt- und Redaktionsgeheimnis. Bis jetzt haben alle Verfassungsgerichte in Europa sowie der Europäische Gerichtshof, welche Gesetze zur Vorratsdatenspeicherung beurteilen mussten, diese ausnahmslos aufgehoben.

Für die Schweiz hat die Digitale Gesellschaft ein strategisches Gerichtsverfahren am Europäischen Gerichtshof für Menschenrechte angestrengt. Die Beschwerde gegen die Vorratsdatenspeicherung ist – mit guter Aussicht auf Erfolg – in Strassburg hängig.

Verlassen wir den Bereich der Strafverfolgung. Wie sieht es bei der nachrichtendienstlichen Überwachung aus?

Mit der Umsetzung des neuen Nachrichtendienstgesetzes und der Einführung der Kabelaufklärung wurde auch hier eine neue Massenüberwachung geschaffen. Die Kabelaufklärung hat ihren Ursprung bei der Funkaufklärung, welche

ursprünglich eine rein militärische Überwachung von ausländischen Vorgängen war. Diese militärische Funkaufklärung wurde dann im Geheimen zur Satellitenüberwachung ausgebaut. Dabei ging es auch noch tendenziell um ausländische, aber bereits zivile Kommunikation.

Da heute immer mehr Kommunikation per Glasfaser übertragen wird, kommt nun mit der Kabelaufklärung der dritte Ausbau hinzu. Im Unterschied zu ausländischen Satelliten können ausländische Kabel jedoch nicht überwacht werden. Daher werden grenzüberschreitende Glasfaserleitungen angezapft. Bei jeder grenzüberschreitenden Kommunikation ist aber auch jemand aus dem Inland beteiligt, da es kaum Leitungen gibt, welche die Schweiz einfach nur durchqueren.

In der Praxis sieht das so aus: Die Kommunikation, die über grenzüberschreitende Leitungen führt, wird vom Zentrum für elektronische Operationen (ZEO) der Armee nach definierten Suchstichworten gerastert. Laut Gesetz ist die Verwendung der erfassten Signale zulässig, wenn sich entweder Sender und/oder Empfänger im Ausland befinden. Gemeint sind damit IP-Adressen.



«Gesichtserkennung kommt mehr und mehr an Flughäfen und Bahnhöfen zum Einsatz.»

Bei grenzüberschreitenden Leitungen wird es praktisch immer der Fall sein, dass sich eine IP-Adresse im Inland und eine im Ausland befindet. Das heisst, wir alle werden permanent überwacht, und unsere Kommunikation wird gerastert. Diese Überwachung, die eigentlich auf Vorgänge im Ausland zielt, wird nun selbstverständlich auch bei Bedrohungen im Inland verwendet.

Wie ist die Situation bei der zielgerichteten Überwachung, beispielsweise beim Einsatz von Staatstrojanern?

Digitale Gesellschaft

Die Digitale Gesellschaft ist ein gemeinnütziger und breit abgestützter Verein für Bürger- und Konsumentenschutz im digitalen Zeitalter. Die zivilgesellschaftliche Organisation setzt sich seit 2011 für eine nachhaltige, demokratische und freie Öffentlichkeit ein. Ihr Ziel ist die Verteidigung der Grundrechte in einer digital vernetzten Welt.

www.digitale-gesellschaft.ch

Der Einsatz von Staatstrojanern (Govware) ist im Bereich der Strafverfolgung und für den Geheimdienst zulässig. Während die Strafverfolgungsbehörden auf Kommunikationsdaten zugreifen dürfen, ist es dem Geheimdienst sogar erlaubt, eine Onlinedurchsuchung durchzuführen sowie Kamera und Mikrofon zu verwenden. Dies stellt einen – zumindest potentiellen – Eingriff in die digitale Intimsphäre der Betroffenen dar, da wir unglaublich viele höchst persönliche Informationen auf unseren Smartphones, Notebooks und PCs speichern. Diese erlauben Rückschlüsse z.B. auf unsere Gesundheit, unsere politischen Ansichten und unsere sexuellen Präferenzen. Auf diesen Geräten sind aber oft auch Geschäftsgeheimnisse oder die Korrespondenz mit der Anwältin oder dem Anwalt abgelegt. Ein Eingriff ist also durchaus vergleichbar mit dem heimlichen Eindringen in die Wohnung und dem Anbringen von Wanzen.

Wenn eine solche Massnahme zulässig sein soll, dann nur als Ultima Ratio, bei einer konkreten und unmittelbaren Gefährdung von Leib, Leben, Freiheit oder der nationalen Sicherheit.

Der begrenzende Deliktscatalog umfasst jedoch fast 100 Straftatbestände, inkl. einfachem Diebstahl!

Wo sehen Sie das Hauptproblem beim Einsatz von Govware?

Neben dem schwerwiegenden Eingriff in die digitale Intimsphäre stellt sich tatsächlich das Problem der Infektion. Diese beruhen eigentlich immer auf der Ausnutzung einer Sicherheitslücke. Die benötigten Sicherheitslücken werden üblicherweise direkt oder indirekt auf dem Schwarzmarkt besorgt, der damit faktisch mit staatlichen Geldern gestützt wird. Dies führt erschwerend auch dazu, dass die Sicherheitslücke nicht geschlossen wird, und wir alle verwundbar bleiben.

Ein Beispiel?

Die Schadsoftware WannaCry hat sich 2017 über eine Sicherheitslücke verbreitet, welche bereits mehrere Jahre von der NSA verwendet und geheimgehalten worden war, bevor sie dann von Kriminellen ausgenutzt wurde. Betroffenen und ausser Betrieb gesetzt waren mehrere hunderttausend Computer in 150 Ländern. Darunter waren Spitäler

in England und Schottland, aber auch Konzerne wie Nissan, Renault und die Deutsche Bahn. Das Interesse des Staates muss sein, für Sicherheit für sich und uns zu sorgen, indem Sicherheitslücken den Herstellern gemeldet und damit geschlossen werden. Sie dürfen nicht verheimlicht werden.

Was wäre Ihr Fazit? Wie sehen Sie die Zukunft der Überwachung in der Schweiz?

Überwachung orientiert sich stets am technisch Machbaren. Untersuchungen zur Nützlichkeit gibt es kaum. Zudem fehlt eine Überwachungsgesamtrechnung, die alle Massnahmen zusammen auf ihre Auswirkungen auf die Demokratie und Gesellschaft berücksichtigt.

Erschwerend fehlt der Schweiz ein Verfassungsgericht, das Gesetze auf ihre Verhältnismässigkeit prüfen kann. Das bedeutet, dass unsere Beschwerde gegen die Vorratsdatenspeicherung aus dem Jahr 2014 frühestens im kommenden Jahr in Strassburg behandelt wird. Unsere zweite Beschwerde gegen die Kabelauflärung aus dem Jahr 2017 wurde eben vom Bundesgericht an das Bundesverwaltungsgericht zur inhaltlichen Beurteilung zurückgewiesen.

Der Rechtsweg ist unglaublich langwierig, während sich die Technik und die Überwachungsmassnahmen rasant weiterentwickeln. Dies sehen wir beispielsweise bei der Gesichtserkennung. Gesichtserkennung kommt mehr und mehr an Flughäfen und Bahnhöfen zum Einsatz. Es gibt bereits riesige Gesichtsdatabanken, wie die ClearView AI. Die Kombination von vernetzten Überwachungskameras mit Machine Learning könnte tatsächlich zu einem dystopischen Überwachungsstaat führen.

Wir fordern daher – übrigens gemeinsam mit 60 anderen Grundrechtsorganisationen aus ganz Europa – ein Verbot von biometrischer Massenüberwachung im öffentlichen Raum!

Herr Schönenberger, vielen Dank für das informative Gespräch.

Die Überwachung mit Drohnen unter besonderer Berücksichtigung der Privatsphäre

Seit dem Beginn der sogenannten digitalen Revolution ab der zweiten Hälfte des letzten Jahrhunderts folgt in rasantem Tempo eine technische Innovation auf die andere. Die Erfindung der Drohne ist dafür ein gutes Beispiel. Mit seinen vielen Erscheinungsformen ist dieses unbemannte Luftfahrzeug vielseitig einsetzbar, z. B. in der Landwirtschaft, bei Inspektionen von Infrastrukturanlagen, aber auch von der Polizei zur Überwachung von Grossanlässen und von privaten Hobby-Piloten. Das bringt Vorteile, aber auch Probleme mit sich.

Die sogenannte «Industrie 4.0» mit dem Ziel der umfassenden Digitalisierung der industriellen Produktion bringt ständig neue Technologien auf den Markt, die durch eine «Hyper-Automation» und «Hyper-Konnektivität» charakterisiert sind, also die zunehmende Automatisierung von Prozessen und Objekten, welche mit ihrer Umgebung verbunden werden. Die Nutzung von Drohnen ist dafür ein gutes Beispiel. Dabei hat sich aber eine Problematik ergeben, die immer mehr auch von den Bürgerinnen und Bürgern wahrgenommen wird: Es geht um den Schutz ihrer Privatsphäre. Ein eindrückliches Beispiel für diese Problematik war in der derzeitigen COVID-19-Situation in Frankreich zu beobachten, wo die Polizei Drohnen zur Kontrolle der verhängten Massnahmen einsetzte. Im vorliegenden Artikel soll die rechtliche Seite des Spannungsfeldes Privatsphäre vs. Drohneneinsatz beleuchtet werden.

Ursprung der Drohne

Die Drohne – das Wort geht tatsächlich auf das «dröhnende» Geräusch fliegen-der Insekten zurück – wurde ursprüng-

lich im militärischen Umfeld entwickelt, erst später wurde die Technologie auch im zivilen Bereich genutzt. Obschon Drohnen inzwischen vielerorts anzutreffen sind, existiert für den Begriff «Drohne» nach wie vor keine Legaldefinition. Drohnen gehören zu den unbemannten Luftfahrzeugen. Das sind Luftfahrzeuge, die ohne einer/s sich an

Autorinnen

Amanda Boekholt

ist Kommunikations-spezialistin und verantwortlich für das Stakeholder-Management in der Sektion Innovation und Digitalisierung des Bundesamtes für Zivilluftfahrt (BAZL).



zvg

Sandra Bodmer

ist Juristin und arbeitet in der Stabsstelle Innovation und Digitalisierung des Bundesamtes für Zivilluftfahrt (BAZL). Sie leitet die Implementierung der EU-Drohnenregulierung in der Schweiz.



zvg



Adobe Stock/Julia Sokolovska

«Man weiss ja nicht, wer der Pilot ist und was er bezweckt, während er mit seiner Drohne gerade über dem Gartensitzplatz kreist.»

Bord befindlichen Pilotin/Piloten gesteuert werden oder autonom fliegen. Sie werden auch UAV/UAS oder RPAS genannt: UAV für *unmanned aircraft vehicle*; UAS für *unmanned aircraft system* und RPAS für *remotely piloted aircraft system*, wobei sich der Begriff RPAS auf die ferngesteuerten unbemannten Luftfahrzeuge beschränkt.

Privatsphäre

Drohnen werden wegen des technologischen Fortschritts immer kleiner und sind auch im Einzelhandel für Privatpersonen zu immer günstigeren Preisen frei erhältlich. Dies und ihre vielfältigen Einsatzmöglichkeiten haben der Drohnenindustrie weltweit einen enormen Schub verliehen. Im Jahr 2018 gab es in der Schweiz rund 80 Firmen, welche in der Herstellung von Drohnen aktiv waren, mit rund 2500 Beschäftigten. Doch wie immer beim Aufkommen

einer neuen Technologie gibt es nicht nur begeisterte Stimmen. Gerade der Einsatz im privaten Bereich schürt Unsicherheiten und Ängste und führt vielfach zu einer ablehnenden Haltung gegen Drohnen überhaupt. Das Bundesamt für Zivilluftfahrt (BAZL) erreichen immer wieder Anfragen von besorgten Bürgerinnen und Bürgern, die sich durch Drohnen in ihrem Umfeld beobachtet bzw. belästigt fühlen. Man weiss ja nicht, wer der Pilot ist und was er bezweckt, während er mit seiner Drohne gerade über dem Gartensitzplatz kreist. Nimmt die Drohne Bilder auf? Wenn ja, was geschieht mit diesen? Ist das überhaupt erlaubt?

Schutzwürdiges Interesse (Art. 667 ZGB)

Überfliegt eine Drohne private Grundstücke, ist zu beachten, dass sich die Rechte des Grundeigentümers nicht

nur auf den Boden, sondern auch auf den Raum über dem Grundstück erstrecken. Die Interessen des jeweiligen Eigentümers sind im Einzelfall zu ermitteln. Obschon sich das Bundesgericht noch nicht zur maximalen Überflughöhe von Grundstücken geäussert hat, gibt es Stimmen in der Lehre, die bei einem Überflug einer Drohne in sehr geringer Höhe (10–40 Meter) bereits das schutzwürdige Interesse an der Ausübung des Grundeigentums tangiert sehen. Inwiefern Drohnen die Privatsphäre verletzen können, zeigt der folgende Überblick über die Aspekte der Privatsphäre.

Schutz der Persönlichkeit

Die Schweizerische Bundesverfassung (BV) regelt den Persönlichkeits- und Datenschutz in mehreren Bestimmungen. In Art. 10 Abs. 2 BV ist das Recht auf persönliche Freiheit, insbesondere

die körperliche und geistige Unversehrtheit sowie das Recht auf Bewegungsfreiheit enthalten. Daneben regelt Art. 13 BV ganz generell, dass jede Person Anspruch auf Schutz der Privatsphäre, insbesondere auch Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten hat.

Das Schweizerische Zivilgesetzbuch (ZGB) konkretisiert Art. 10 und Art. 13 der Bundesverfassung in Art. 28 ff ZGB. Art. 28 ZGB schützt die Persönlichkeit als Ganzes, ohne die einzelnen Persönlichkeitsgüter aufzuzählen. Damit eine Persönlichkeitsverletzung vorliegt, muss die Beeinträchtigung nach einem objektiven Massstab einer gewissen Intensität entsprechen. Die Verletzung des Persönlichkeitsrechts ist widerrechtlich, wenn sie gemäss Art. 28 Abs. 2 ZGB nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist. So kann die Aufnahme von Bildern ohne die Zustimmung der betroffenen Person – und sofern die Aufnahme nicht im öffentlichen Interesse geschieht – bereits eine Verletzung von Art. 28 ZGB darstellen. Eine Persönlichkeitsverletzung ist sicherlich gegeben, wenn eine Person durch die Überwachung auch für Dritte erkennbar ist, indem man beispielsweise auf einer Aufnahme deren Gesicht zeigt.

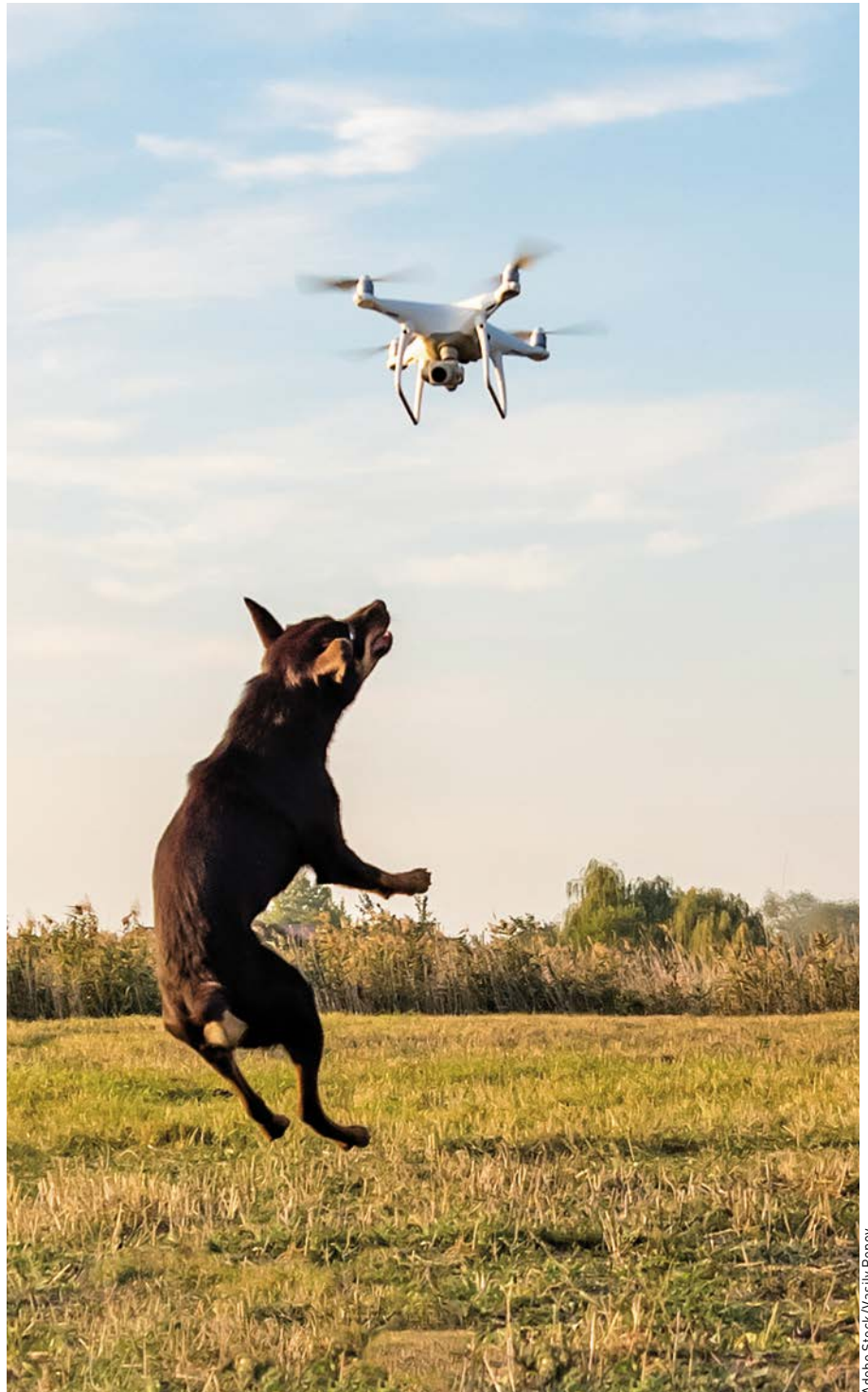
Das Kantonsgericht Luzern hat sich in seinem Entscheid vom 18. April 2018 eingehend mit der Thematik des Persönlichkeitsschutzes bei Drohnenaufnahmen auseinandergesetzt: Die Luftaufnahmen von Liegenschaften am Seeufer von Horw zum Zweck der Baukontrolle/Bauaufsicht wurden wegen der fehlenden gesetzlichen Grundlage als nicht zulässig erachtet. Selbst wenn die Arbeiten angekündigt wurden, entstünde über einen Zeitraum von einem Monat ein Gefühl des Überwachtseins. Dies führe laut Gericht zu einer schwerwiegenden Einschränkung des Rechts auf informationelle Selbstbestimmung und stelle einen Eingriff in das Recht auf Schutz der Privatsphäre nach Art. 13 BV dar, weshalb die gemachten

Aufnahmen aufgrund der fehlenden gesetzlichen Grundlage zu löschen seien.

Datenschutz

Schliesslich sei noch das Datenschutzgesetz (DSG) erwähnt, das den Schutz

der Persönlichkeit derjenigen Personen beabsichtigt, über die Daten bearbeitet werden. Somit behandelt das DSG eines der zentralen Themen der Industrie 4.0. Damit das DSG zur Anwendung kommt, müssen Personen-



«Es wird aber auch die Meinung vertreten, dass ein schnelles Handeln durchaus akzeptabel sei und damit auch das Einfangen oder Abschiessen der Drohne im Einzelfall rechtfertigen könnte.»

daten im Sinne von Art. 3 lit. a DSGVO bearbeitet werden. Werden die Aufnahmen der Drohne aber ausschliesslich zum persönlichen Gebrauch benutzt, sind die datenschutzrechtlichen Bestimmungen nach Art. 2 Abs. 2 lit. a DSGVO nicht anwendbar. Diese Sichtweise wird jedoch nicht von der gesamten Lehre geteilt, denn selbst wenn die Daten ausschliesslich zu persönlichen Zwecken verwendet werden und das DSGVO de jure nicht anwendbar ist, verhindert dies nicht die mögliche Verletzung der Privatsphäre und das Gefühl, ausspioniert zu werden. Im Zusammenhang mit dem Datenschutz und der Verwendung von Drohnen hat der Eidgenössische Datenschutzbeauftragte (EDÖB) ein Merkblatt für die Videoüberwachung mit Drohnen zusammengestellt, das die verschiedenen Punkte auflistet, die beim Betrieb von Drohnen zu beachten sind.¹ Der EDÖB geht davon aus, dass Aufnahmen von Drohnen nur mit einem entsprechenden Rechtfertigungsgrund (entweder der Einwilligung der betroffenen Person, bei Vorliegen eines überwiegenden privaten oder öffentlichen Interesses oder durch Gesetz) erlaubt sind.

Massnahmen gegen solche Eingriffe in die Privatsphäre

Eigentümern und Besitzern stehen verschiedene rechtliche Möglichkeiten zur Verfügung, um eine Störung abzuwehren:

Eigentumsfreiheitsklage

(Art. 641 Abs. 2 ZGB)

Mit der Eigentumsfreiheitsklage kann der Eigentümer eines Grundstücks gegen den Störer auf Abwehr der ungerechtfertigten Einwirkung klagen. Eine solche ungerechtfertigte Einwirkung kann vorliegen, wenn durch den Überflug mit einer Drohne die durch das schutzwürdige Interesse des Grundeigentümers bestimmte vertikale Grenze oder die horizontalen Grenzen gegen den Willen des Berechtigten verletzt werden.

¹ EDÖB, Videoüberwachung mit Drohnen durch Private (www.edoeb.admin.ch) → Datenschutz → Technologien → Videoüberwachung → Drohen



«Die Fernidentifikation von Drohnen ist ein Mittel, mit dem ein Drohnenbetreiber während eines laufenden Betriebs anhand seiner Registrierungsnummer – ähnlich dem Autonummernschild – identifiziert werden kann.»

Nachbarrecht (Art. 679 f. ZGB)

Die Klage aus Nachbarrecht stützt sich auf übermässige Einwirkungen, die von einem Nachbargrundstück ausgehen. Besitzt der Nachbar eine Drohne und benützt sein Grundstück regelmässig zum Starten und Landen seiner Drohne, kann dies eine Überschreitung der aus dem Grundeigentum zustehenden Nutzungsrechte darstellen.

Besitzesschutz

(Art. 926 und Art. 928 ZGB)

Ausserdem stehen dem Besitzer (beispielsweise dem Mieter eines Hauses) ähnlich dem Eigentümer gewisse Rechtsbehelfe zur Verfügung. Im Falle einer Besitzesstörung kann der Besitzer Abwehrmassnahmen ergreifen, indem er sich gegen die Störung mit Gewalt zur Wehr setzt, wobei die Massnahme verhältnismässig zur Störung sein muss. Der Abschuss der Drohne ist gemäss der herrschenden Lehre das letzte Mittel bei der Abwehr von Störungen (sog. Selbsthilferecht nach Art. 926 ZGB). Es wird aber auch die Meinung vertreten, dass gerade in Zeiten von der Veröffentlichung via Social Media ein schnelles Handeln durchaus akzeptabel sei und damit

auch das Einfangen oder Abschiessen der Drohne im Einzelfall rechtfertigen könnte. Dies gilt allerdings nur, solange der Angriff unmittelbar andauert. Versäumt der Besitzer das Notwehrrecht, kann er seine Ansprüche klageweise durchsetzen.

Strafrecht (Art. 179^{quarter} StGB)

Auch das Strafrecht kann vor Drohneinsätzen schützen. Die Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte dürfte dann gegeben sein, wenn Aufnahmen von einem Bereich gemacht werden, der gegen die Einsicht durch Aussenstehende in irgendeiner Art und Weise gesichert ist.

Zivil- sowie Strafverfahren sind aufgrund ihrer Langwierigkeit selten geeignet, um unmittelbare Einwirkungen durch Drohnen rechtzeitig abzuwehren. Sie eignen sich stattdessen viel eher zur Abwehr von regelmässig geplanten Drohneinsätzen und wenn die Person, von der die Störungen ausgehen («der Störer»), bekannt ist.

Technische Massnahmen

Allen Fällen der Verletzung des Persönlichkeits- und Datenschutzes ist gemeinsam, dass die Identität des Piloten

nur selten feststellbar ist. Dies erschwert die Rechtsdurchsetzung erheblich, weil man den Piloten oder die Pilotin nicht einfach ausfindig machen und auffordern kann, die Aufnahmen zu löschen. Glücklicherweise legen die fortschreitende Technik und die angepasste Regulierung den Grundstein, um auch dieses Problem zu beheben und die Strafverfolgung zu erleichtern.

Einerseits müssen sich die Betreiber von Drohnen mit Inkrafttreten der neuen EU-Drohnenregulierung, deren Umsetzung in der Schweiz sich verzögert, in ein nationales Register eintragen, sobald sie Drohnen mit einem Abfluggewicht von mehr als 250g fliegen oder sofern die Drohne mit einem Sensor ausgerüstet ist, der personen-

bezogene Daten erfassen kann. Andererseits wird mit Inkrafttreten der «U-Space Regulierung» die sogenannte Netzwerk-Fernidentifikation (*network remote identification*, kurz: «Net-RID») eingeführt. Die Fernidentifikation von Drohnen ist ein Mittel, mit dem ein Drohnenbetreiber während eines laufenden Betriebs anhand seiner Registrierungsnummer – ähnlich dem Autokennzeichenschild im Strassenverkehr – identifiziert werden kann. Dies dient primär der besseren Sichtbarkeit und Integration aller Luftraumteilnehmer. Die Schweiz ist gerade dabei, die Fernidentifizierung auf freiwilliger Basis im Rahmen der Partnerschaft «Swiss U-Space Implementation» (SUSI) einzuführen und zu testen.

Schlussbemerkung

Dank den verschiedenen Rechtsbehelfen, aber insbesondere auch mit Hilfe der neuen technischen Massnahmen, hoffen wir, das Bewusstsein der Fernpilotinnen und -piloten für die Einhaltung der Regeln stärken sowie Verletzungen der Privatsphäre aller Personen besser verhindern bzw. ahnden zu können. Auch die Akzeptanz der Bevölkerung gegenüber diesen neuen Fluggeräten sollte dadurch erhöht werden. Ziel wird es sein, dass weder Datenschutzbedenken noch die Angst vor der Verletzung der Privatsphäre die Nutzung und Schaffung neuer – und gesellschaftlich höchst vielversprechender – Technologien erschweren oder ganz verhindern werden.

Freie Fahrt für Cyber Patrolling gegen Kriminalität im Netz!

Im Kampf gegen die digitale Kriminalität wurde in der Schweiz das Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK) gegründet. Die Polizeikörpers, die Teil von NEDIK sind, betreiben unter anderem das Cyber Patrolling. Darunter wird das polizeiliche Beobachten, Erfassen und Vorermitteln von kriminellen Vorgängen im Internet und im Darknet nach Polizeigesetz verstanden.

Autorin

Tamara Schmid

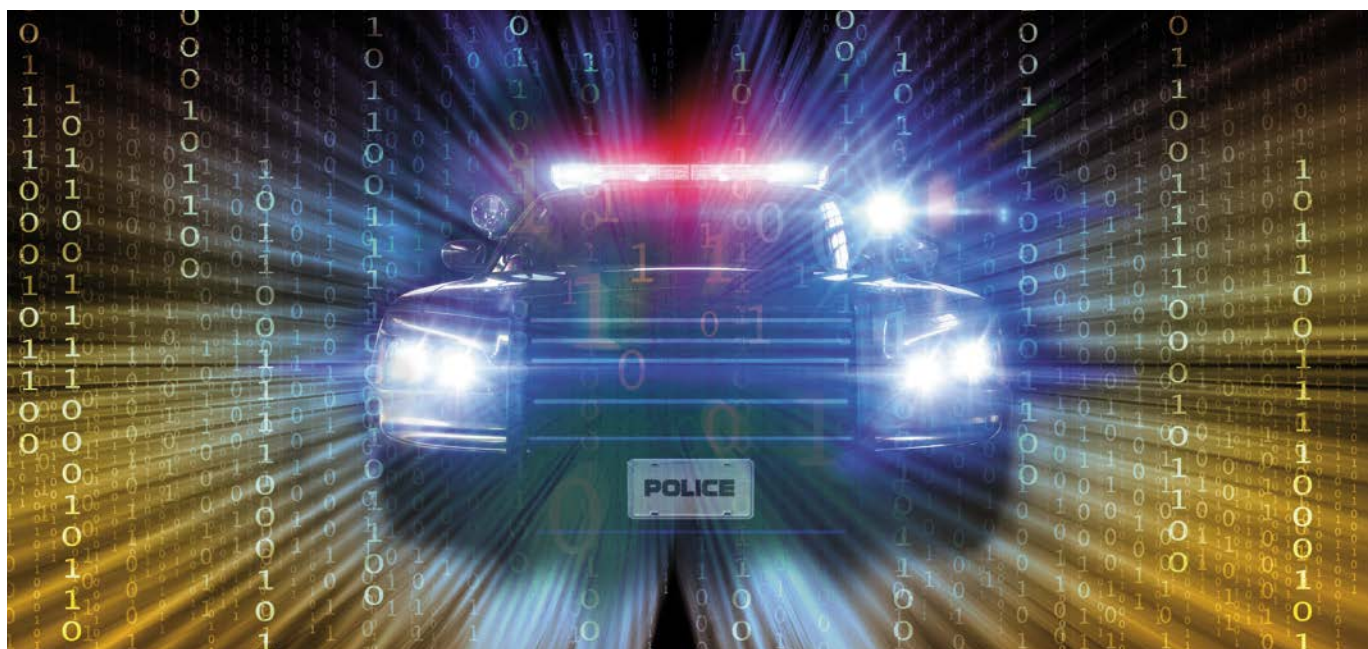
NEDIK Analytikerin,
Kantonspolizei Zürich



Im Zeitalter der Digitalisierung müssen wir uns damit auseinandersetzen, dass dem Online-Geschehen praktisch keine Grenzen gesetzt sind. Jegliche Wünsche, seien sie noch so ausgefallen, können online befriedigt werden: Ob Waffen, gefälschte Markenartikel, eine neue Identität, Betäubungsmittel oder verbotenes Bild- und Videomaterial –

wenn man weiss, wo und wie man suchen muss, kann man fast immer fündig werden. Mit dieser Tatsache müssen sich auch die Schweizer Polizeibehörden auseinandersetzen und sich dieser Herausforderung stellen. Es gilt klar zwischen Hol- und Bring-Kriminalität zu unterscheiden: Von Bürgerinnen und Bürgern angezeigt werden kriminelle Handlungen ja zumeist nur dann, wenn sie selbst geschädigt wurden. Doch zum Beispiel bei der Betäubungsmittel-Kriminalität ist das anders: Dort muss sich die Polizei selber mit Hilfe des Cyber Patrollings um Aufklärung bemühen. Bei Cyber Patrolling suchen Mitarbeitende von Strafverfolgungsbehörden gezielt nach Straftaten im Internet. Cyber Patrolling ist im Ansatz keine neue Erfindung, sondern vielmehr eine technische Anpassung an die zunehmende Digitalisierung. Straftäter sollen das Gefühl bekommen, dass sie nicht ungestraft im Internet unterwegs sein können. Das Internet ist kein rechtsfreier Raum.

Die Cybercrime-Abteilungen der Schweizer Polizeibehörden werden zurzeit aufgestockt und die Mitarbeitenden entsprechend aus- bzw. weitergebildet, um die Bekämpfung der Internetkriminalität verstärkt angehen zu können.



123RF | Montage: Weber & Partner

«Bei Cyber Patrolling suchen Mitarbeitende von Strafverfolgungsbehörden gezielt nach Straftaten im Internet.»

Die Abteilungen setzen sich jeweils aus erfahrenen Fahnder(inne)n, Ermittler(inne)n, Informatiker(inne)n sowie wissenschaftlichen Mitarbeitenden ohne Polizeiausbildung zusammen. Gemeinsam wird gegen Drogendealer, Betrüger(inne)n, aber auch Pädokriminelle im Netz ermittelt. Auch hier spielt das proaktive Cyber Patrolling eine wichtige Rolle. Denn damit wird illegales Handeln bzw. die Vorbereitung dazu erkannt und anschliessend zu verhindern versucht. Die Ermittler(innen) der Schweizer Polizeibehörden erhalten zudem regelmässig konkrete Hinweise auf illegale Handlungen im Netz. Diesen wird systematisch nachgegangen.

Fallbeispiel

Zu Beginn einer Online-Drogenfahndung werden einschlägige Online-Marktplätze darauf überprüft, ob deliktische Handlungen mit Bezug zur Schweiz erkennbar sind. Dabei orientiert man sich nicht an einer spezifischen Zielperson, sondern es wird Phänomen-spezifisch patrouilliert:

1. Bekannte Marktplätze inklusive der Händlerprofile werden gesichtet, und die spezifischen Verkaufsaktivitäten werden analysiert.

2. Aufgrund vorgegebener Kriterien werden bestimmte Händler ausgewählt, und gegen sie werden mögliche Ermittlungsschritte abgewogen.
3. Durch die vorgenommene Analyse können bereits erste Erkenntnisse zur möglichen Identität der Händler gewonnen werden.
4. Erhärten sich die Verdachtsmomente, werden Ermittlungsverfahren gegen die Händler eröffnet.

Die ersten beiden Schritte zeigen auf, was Cyber Patrolling tatsächlich ist. Punkt 3 beschreibt die damit zusammenhängenden getätigten Vorermittlungen. Diese drei Schritte müssen vorgenommen werden, um anschliessend in Schritt 4 ein erfolgversprechendes Ermittlungsverfahren führen zu können.

Koordination

Die Koordination der nationalen und internationalen Zusammenarbeit bei der Bekämpfung der Internetkriminalität ist eine zentrale Aufgabe des NEDIK. Hinweise zu illegalem Handeln kommen aus der Bevölkerung und auch immer wieder von ausländischen Polizeibehörden wie Interpol und Europol. Die Meldungen aus dem Ausland treffen

in der Schweiz zuerst beim Bundesamt für Polizei fedpol ein, von wo sie dann an die kantonalen Polizeikörpers weitergeleitet werden. Ohne intensive Kooperation zwischen den Kantonen untereinander, zwischen den Kantonen und dem Bund sowie zwischen dem Bund und dem Ausland können Ermittlungen kaum erfolgreich sein. Zur effizienten Bekämpfung der digitalen Kriminalität setzt NEDIK spezifische Analyseinstrumente ein und betreibt eine zentrale Wissensdatenbank. Ermittlungsergebnisse können so optimal mit den anderen Polizeikörpers geteilt werden.

Von zentraler Bedeutung ist die Koordination. Wie auch in anderen Ländern besteht in der Schweiz die Gefahr von Parallelermittlungen bzw. parallelem Cyber Patrolling. Eine gut funktionierende Koordinationsstelle vermindert das Risiko, dass mehrere Polizeibehörden im gleichen Fall ermitteln, und hilft, diese Ressourcen anderweitig sinnvoller zu nutzen.

Bekämpfung der Pädokriminalität

Die Kantonspolizei Bern übernimmt als Teil von NEDIK seit dem 1. Januar 2021

die Koordination des Peer-to-Peer-Monitorings sowie damit im Einzelfall einhergehende zusätzliche präventive verdeckte Massnahmen im digitalen Raum. Die Internetkriminalität und vor allem die Pädokriminalität sind transnational. Eine intensive Kooperation zwischen den einzelnen Kantonen, dem Bund und dem Ausland sind hier essentiell. Fedpol bearbeitet und triagiert für die Kantone die Verdachtsmeldungen von ausländischen Partnerbehörden – wie beispielsweise die Verdachtsmeldungen der US-Behörden zur Pädokriminalität, die sogenannten NCMEC*-Meldungen. Sobald sich ein Verdacht erhärtet, kann die jeweils zuständige kantonale Staatsanwaltschaft ein Verfahren einleiten. Im präventiven Bereich steht jeder Kanton weiterhin in der Verantwortung im Verbund mit NEDIK, eigene verdeckte Abklärungen zur Bekämpfung der Pädokriminalität zu betreiben und entsprechende polizeiliche Ressourcen aufzubauen. Die Ermittler/innen, welche präventive verdeckte Ermittlungen im Bereich Pädokriminalität betreiben, müssen über die Vorgehensweisen und Absichten der Täter Bescheid wissen. Diese sind sehr versiert und in der Regel international aktiv. Die Anpassung an das Täterprofil ist nicht nur beim präventiven Cyber Patrolling im Bereich Pädokriminalität wichtig, sondern auch bei den anderen Internetdelikten.

Cyber Patrolling als Kriminalprävention

Die Schweizer Polizeibehörden sind nicht nur verdeckt im Internet präsent, sondern auch sichtbar. Auf verschiedenen Plattformen geben die Polizeikorps Ratschläge, wie vermieden werden kann, selbst Opfer von Internetkriminalität zu werden. Sie leisten also auch präventive Arbeit und geben Rückmeldung auf spezifische Fragen der Bevölkerung. Die Polizeikorps nehmen

auch Hinweise und Informationen über Internetkriminalität entgegen. Cyber Patrolling soll zudem dazu dienen, offene und präventive Polizeiarbeit an Orten zu leisten, an denen sich die Bürgerinnen und Bürger virtuell aufhalten, und die Öffentlichkeit zu beraten, wie sie das Internet sicher nutzen kann.

Mit der Webseite cybercrimepolice.ch ist die Polizei bei aktuellen Gefahren in Echtzeit dabei. Die Nutzerinnen und Nutzer dieser Webseite sind die besten Cyber Patrols, denn sie melden schnell und unkompliziert neue Kriminalitätsformen und helfen dabei mit, andere Internetnutzer zu sensibilisieren und zu warnen.

Kooperationen

In bereits abgeschlossenen Fällen konnte immer wieder festgestellt werden, wie wichtig die präventiven Ermittlungen bzw. das sogenannte Cyber Patrolling sind. Die Verknüpfung repressiver und präventiver Massnahmen im Bereich der Cyberkriminalität ist aus verschiedenen Gründen von grosser Bedeutung. Die zentrale Aufgabe von NEDIK ist es, die Zusammenarbeit im Ermittlungsbereich Cyberkriminalität zu fördern und zu koordinieren. Dies spiegelt sich auch im Präventionsauftrag von NEDIK, wonach die operative Präventionstätigkeit gefördert und Präventionsorganisationen bei der nationalen Cyber-Prävention unterstützt werden sollen. Aufgrund dessen hat NEDIK anfangs 2021 entschieden, dass die Zusammenarbeit

mit der Schweizerischen Kriminalprävention, welche eine der wichtigsten Präventionsorganisationen in der Schweiz ist, intensiviert werden soll. Durch den Informationsaustausch im Netzwerk werden präventive sowie repressive Massnahmen aufeinander abgestimmt, fachrelevantes Wissen ausgetauscht und Aus- und Weiterbildungsmöglichkeiten angepasst.

Die Schweizer Polizeibehörden erzielen mit dem verdachtsunabhängigen Cyber Patrolling regelmässig Erfolge. Sie können damit Personen, die sich an illegalen Geschäften beteiligen, identifizieren, lokalisieren, verhaften und strafrechtlich verfolgen. Die Verknüpfung repressiver und präventiver Massnahmen im Bereich der Cyberkriminalität ist aus den genannten Gründen von grosser Bedeutung. Mit dem Auftrag zur Förderung der Zusammenarbeit im Ermittlungsbereich Cyberkriminalität kommt NEDIK dabei eine wichtige Rolle zu. Eine koordinierte Zusammenarbeit zwischen den verschiedenen Behörden ist essentiell und muss effizient und pragmatisch sein. Der globalisierte digitale Raum erlaubt den Nutzern, sich global zu orientieren und zu vernetzen. Daher bedarf es seitens der Schweizer Polizeibehörden ebenfalls globale Ressourcen und eine vernetzte und starke interkantonale sowie internationale Zusammenarbeit. Damit kann komplexe und grenzenlose Internetkriminalität erfolgreich bekämpft werden.



123RF/Kirill Makarov

«Die Schweizer Polizeibehörden erzielen mit dem verdachtsunabhängigen Cyber Patrolling regelmässig Erfolge.»

* NCMEC = National Center for Missing and Exploited Children



Street-Art in Gloucestershire

«Der technische Zugang ist die eine Schwierigkeit, doch das Verstehen des Inhalts die andere.»

Überwachen mit Sprachmittlern – eine Praxis auf der Suche nach Standards

Die Überwachung von Kommunikation in Echtzeit ist in bestimmten Fällen technisch möglich, rechtlich erlaubt und kann helfen, Straftaten zu verhindern bzw. aufzuklären. Aber sie kann auch scheitern, wenn der Inhalt nicht verstanden wird. Die Abhängigkeit der Strafverfolgungsbehörden von Sprachmittler/innen ist in diesem Bereich enorm und dennoch ein wenig erforschter Teilbereich von Strafverfahren. Ein Forschungsprojekt der Universität Neuenburg trägt dazu bei, dies zu ändern.

Die geheime Kommunikationsüberwachung wird seit dem Einschlagen der ersten Telegraphenmasten 1840 praktiziert. Die technischen Möglichkeiten der Überwachung haben mit jeder Erfindung neuer Geräte einerseits zu-

genommen, andererseits haben Verschlüsselungstechniken den Zugang der Strafverfolgungsbehörden zu den Gesprächsinhalten auch wieder erschwert. Entsprechend aufsehenerregend ist es, wenn Zugriffe ausländischer Polizeibe-

hörden auf verschlüsselte Netzwerke wie IronChat, Sky ECC und EncroChat gelingen. Die Zahlen aus der Sky ECC-Aktion sind atemberaubend: Weltweit gibt es mehr als 170000 Nutzer mit Aufenthaltsorten in Europa, Nordamerika, Südamerika und im Nahen Osten, und die Ermittler/innen sollen ungefähr 1 Milliarde ihrer verschlüsselten Nachrichten abgefangen haben. Allein die schiere Menge lässt die Strafverfolgungsbehörden wohl an ihre Kapazitätsgrenzen stoßen.

Eine Frage, die trotz ihrer Relevanz nur selten in diesem Zusammenhang gestellt wird, ist: Was passiert, wenn die Nachrichten in einer für die zuständige Strafverfolgungsbehörde fremden Sprache ausgetauscht werden? Schnell wird klar: Der technische Zugang ist die

Autorin

Nadja Capus

Prof. Dr. iur.
Lehrstuhl für Strafrecht und Strafprozessrecht
Universität Neuenburg



zvg



«Sprachmittler/innen brauchen sehr spezifische Kompetenzen: Denn gesprochen wird in der Alltagssprache, in Dialekten, Regiolekten oder gar mit kodierten Begriffen aus dem Milieu der abgehörten Personen.» (Bild: Nicole Kidman in «Die Dolmetscherin», 2005)

eine Schwierigkeit, doch das Verstehen des Inhalts die andere. Sie ist noch grösser, wenn es nicht um abgespeicherte Textnachrichten geht, sondern um mündliche Gespräche. Der erste und wichtigste Überwacher ist dann jeweils ein/e Dolmetscher/in oder, wie wir diese Berufsgruppe bezeichnen: ein/e Sprachmittler/in. Wie sehr die Strafverfolgungsbehörden von diesen Personen abhängig sind, wird meist viel zu wenig beachtet.

Fatale Folgen mangelhafter Sprachmittlereinsätze

Die Folgen einer geheimen Kommunikationsüberwachung können fatal sein, wenn es zu wenig Sprachmittler/innen hat, wenn sie schlecht oder gar nicht ausgebildet und/oder ungenügend instruiert sind; wenn Zeit verloren geht, weil als falsch monierte Übersetzungen von einer anderen Person überprüft werden müssen; wenn Fehler passieren, die dazu führen, dass die überwachten, gespeicherten und übersetzten Sequenzen nicht als Beweismittel verwendet werden können.

So stockte nach 9/11 in den USA die gesamte FBI-Untersuchung der terroristischen Anschläge wegen ungenügender Sprachmittlerkapazitäten; in Österreich kam in einem Schlepperfall heraus, dass die Sprachmittlerin in Absprache mit der Polizei im Protokoll teilweise völlig andere Aussagen als auf dem gehörten Tonband verschriftlicht hatte, damit es «besser aussieht» (Der Standard, 6.5.2014); in der Schweiz bezeugen Gerichtsfälle missglückte Kooperationen und die Folgen mangelhafter Einsätze (z.B. Bundesgerichtsentscheide v. 28.1.2005 und v. 23.9.2013): Verurteilungen wurden aufgehoben und Fälle an die Vorinstanz zurückgewiesen mit der Auflage, diese solle für jede Aufzeichnung, die sie verwenden wolle, Informationen über die Methode erhalten, die angewendet wurde, um eine Aufzeichnung des Telefongesprächs in einer fremden Sprache in die Amtssprache zu erstellen; ausserdem solle sie die Identität jeder Person, die an dem Vorgang teilgenommen hatte, offenlegen, ebenso die Anweisungen, die jede von ihnen dazu

erhalten hatte, und schliesslich den Nachweis führen, dass jede von ihnen ausreichend über die strafrechtlichen Folgen gemäss Art. 307 StGB für die Erstellung einer falschen Meldung oder Übersetzung aufgeklärt worden sei. Sollten diese Information nicht gesammelt werden können, seien die Übersetzungsprotokolle der geheimen Kommunikationsüberwachung schlicht nicht als Beweismittel verwertbar.

Das ist – kurz zusammengefasst – der vom Bundesgericht seit 2002 in seinem Leitenstcheid BGE 129 I 85 deklarierte, rudimentäre Standard. Aber wird er in den Kantonen auch befolgt? Ist er sinnvoll? Wäre er auszubauen? Wie sieht überhaupt die Praxis aus, und wie erleben sie die involvierten Personen? Diesen und anderen Fragen widmet sich unser Forschungsprojekt.

Ein schwer zugängliches Forschungsobjekt

Dolmetscher-, Übersetzer- und Sprachmittlerdienste in Strafverfahren sind keine Seltenheit. Ein/e Dolmetscher/in übermittelt mündlich unter Zeitdruck

das in der Ausgangssprache Gesprochene oder auch Geschriebene in die Zielsprache. Die Tätigkeit des Übersetzens hingegen meint beispielsweise die direkte schriftliche Übersetzung von abgehörten Gesprächen oder auch die Übersetzung von Geschriebenem. Im Kontext der geheimen Kommunikationsüberwachung kann es sich um beides handeln, weshalb wir den Begriff Sprachmittlung verwenden. Obwohl es sich um eine Tätigkeit in einer wichtigen Phase einer Strafuntersuchung handelt, wurde sie bisher erst durch eine Handvoll Primärstudien ausserhalb der Schweiz untersucht, denn die Geheimhaltungsinteressen sind selbstverständlich enorm.

Der Schweizerische Nationalfonds finanziert seit Dezember 2019 unser transdisziplinäres Projekt zur Erforschung der Entstehung und Verwertung von Sprachmittlungsbeiträgen im Rahmen der geheimen Kommunikationsüberwachung, und seither haben uns mehrere Polizeibehörden und Staatsanwaltschaften verschiedener Kantone, nicht hingegen die Bundesanwaltschaft, im Rahmen fruchtbarer Kooperationen Zugang gewährt zu diesem nur schwer zugänglichen Forschungsgebiet.

Um die Tätigkeit der Sprachmittler/innen näher untersuchen zu können, werden Interviews mit ihnen und mit polizeilichen Ermittlerinnen und Ermittlern in einem Teil dieser Kantone sowie eine schweizweit angelegte Online-Umfrage durchgeführt, an welcher von der Polizei als Sprachmittler/innen rekrutierte Personen Informationen zu ihrer Ausbildung, ihren Sprach- und Übersetzungskompetenzen und ihren Berufserfahrungen geben. Diese Erhebungen werden durch Untersuchungen ergänzt, mit welchen die Tätigkeit vor Ort direkt beobachtet wird. Zusätzlich fokussiert das Projekt die Arbeitsprodukte der Sprachmittler/innen: Anhand einer Analyse von 22 Strafakten aus vier Kantonen wird aus rechtswissenschaftlicher und rechtssoziologischer Sicht erhoben, wie die Arbeit der

Sprachmittler in Strafuntersuchungen einfließt und dokumentiert ist. Schliesslich erfolgt auch noch eine translationswissenschaftliche Untersuchung von Audioaufnahmen und den dazugehörenden Protokollen. Hierbei wird der Fokus auf die Strategien und Arbeitsweisen von Sprachmittler(inne)n gelegt. Die Entwicklungsphasen eines Beweismittels, welches aufgrund eines abgehörten Gespräches entsteht und als Beweismittel in schriftlicher Form in einem Verfahren gewürdigt wird, werden dargestellt.

Vorläufige Resultate

Offensichtlich hat sich das Problembewusstsein in den vergangenen Jahren verbessert und sowohl auf europäischer als auch auf kantonaler Ebene – leider nicht auf Bundesebene – zu Bemühungen geführt, die Qualität von Sprachdienstleistungen und deren Einbettung in Strafrechtsverfahren mit Blick auf Dokumentation, Überprüfbarkeit und Anfechtungsmöglichkeiten zu verbessern. Allerdings macht eine unserer Untersuchungen klar, dass diese Bemühungen in erster Linie auf die sichtbarsten aller Dolmetscher/innen zielen, nämlich die, welche in Gerichtsverfahren oder in Einvernahmen anwesend sind, wobei die Sprachmittleraktivität jedoch ganz andere translatorische Transferstrategien und Kompetenzen erfordert, die sehr spezifisch sind: Denn gesprochen wird in der Alltagssprache, in Dialekten, Regiolekten oder gar mit kodierten Begriffen aus dem Milieu der abgehörten Personen, und abgehört wird unter Beizug technischer Hilfsmittel unter teilweise schwierigen Umständen, was die akustische Wahrnehmung beeinträchtigen kann. Das gilt auch für den Umstand, dass es sich um Telefon-Dialoge oder (bei Mikrofonplatzierungen in Fahrzeugen oder Lokalen) auch um Gespräche zwischen mehreren Personen handelt, welche der/die Sprachmittler/in während des Zuhörens nicht sieht. Daher steht vor allem die Zuhörkompetenz im Vordergrund, wenn es darum geht,

unterschiedliche Stimmen oder einen Sprachwechsel zu erkennen. Die hohe Spontaneität des Arbeitsauftrages erfordert von Sprachmittler/innen neben der hybriden Transfertätigkeit zudem hohe Antizipationsfähigkeit und fachliches Hintergrundwissen. Angesichts dieser Vielfalt erstaunt die allgemeine (und vom Bundesgericht gestützte) Annahme, dass bereits mit Zweisprachigkeit die notwendigen Kompetenzen für diese sehr spezielle und herausfordernde Tätigkeit abgedeckt werden könnten.

Die rechts- und translationswissenschaftliche Auseinandersetzung mit Informationen und Beweisen, die dieser Aktivität entspringen, wird – so zeigt die Analyse der Literatur, der Bundesgerichtsrechtsprechung und der Akten – diesen Besonderheiten nicht gerecht. Unsere (allerdings aktuell erst zur Hälfte abgeschlossene) Aktenanalyse zeigt, dass die vom Bundesgericht aufgestellten Gültigkeitskriterien in der Praxis grösstenteils nicht erfüllt werden. So wird z.B. die Identität der Dolmetscher in den Akten nicht erwähnt, die Angaben zur verwendeten Übersetzungsmethode und die den Sprachmittlern erteilten Anweisungen tauchen in den analysierten Akten überhaupt nicht auf. Relativ selten sind Hinweise, dass die Sprachmittler/innen über Art. 307 StGB, noch seltener der Hinweis, dass sie über Art. 320 StGB aufgeklärt wurden.

Hervorzuheben ist, dass die Sprachmittler an einem heiklen Schnittpunkt zwischen Sachverhaltserhebung und Rechtsinterpretation handeln, weshalb informelle Kooperationsformen rasch erhebliche Bedeutung erlangen können. Die Rollenzuteilung von Seiten der Behörden, die Eigeneinschätzung der Sprachmittler/innen sowie die Art und Weise der Instruktion betreffend Fall und Arbeitsweise divergieren allerdings nach unseren noch nicht beendeten Erhebungen erheblich.

Interessanterweise betreibt das Bundesgericht, das – wie gesehen – in der Setzung erster Standards eine wichtige Rolle eingenommen hat, eine Recht-

sprechung, die einerseits fordert, dass die Identität der Sprachmittler/innen, ihre Instruktion und die Umsetzung ihrer Arbeit sichtbar gemacht wird. Andererseits sorgt sie dafür, dass ihr Beitrag zur Erhebung und Selektion der als verfahrensrelevant erachteten Informationen sowie ihre hohe Verantwortung in die Unsichtbarkeit gedrängt werden. Viele für die ermittelnden Personen unverzichtbaren Informationen müssen daher auf dem informellen Wege zwischen Sprachmittler(inne)n und Polizei übermittelt werden.

Ausblick

Wir haben gesehen: Die aus mangelhaften Sprachmittlungseinsätzen resultierenden Probleme können Kosten verursachen, zum Verlust von Beweisen führen, be- oder entlastendes Material

abschwächen und damit zum Scheitern von Strafverfahren beitragen oder Verzögerungen verursachen, die das Verjährungsrisiko erhöhen. Unser transdisziplinäres Forschungsprojekt, das im November 2022 nach drei Jahren Laufzeit enden wird, hat zum Ziel, zur Schliessung der genannten Forschungslücken beizutragen und im Austausch mit Vertretern der Praxis Erkenntnisse zu erarbeiten, die der Polizei und Staatsanwaltschaft helfen, eine «good practice» bei der Auswahl und dem Einsatz von Sprachmittlern bei der geheimen Kommunikationsüberwachung zu entwickeln. Ziel ist es auch, den Gerichten eine Orientierung zu geben, welche Standards in Sachen Beweiserhebung und -verwertung anzustreben sind. Zum Gelingen dieses Forschungsprojekts trägt die grosszügige Koope-

ration der Polizeibehörden, Staatsanwaltschaften und der Gerichte bei.

Weiterführende Informationen

finden sich auf der Internetseite *Centre romand de recherche en criminologie* der Universität Neuenburg: www.unine.ch/crrc/intercept-interpret.

Auskunft geben die leitende Professorin Dr. Nadja Capus (nadja.capus@unine.ch, 032 718 13 05 oder 079 536 50 52), Dr. Damian Rosset (damian.rosset@unine.ch), Dr. Cornelia Griebel (cornelia.griebel@unine.ch), Dr. Ivana Havelka (ivana.havelka@unine.ch), MLaw Elodie Bally (elodie.bally@unine.ch).

Electronic Monitoring (EM) – Der Einsatz der elektronischen Überwachung in der Schweiz

Electronic Monitoring wird heute in der Schweiz hauptsächlich für den Vollzug von Freiheitsstrafen eingesetzt. Verstösse gegen behördliche Auflagen werden dabei in der Regel nachträglich festgestellt, und die Absprachefähigkeit der verurteilten Person kann damit getestet werden. Die elektronische Überwachung ist in seiner heutigen Anwendung also eine alternative Sanktionsform und dient nicht dazu, Straftaten zu verhindern. Doch es gibt einige Neuerungen.

Bereits seit dem Jahr 1999 übernimmt die elektronische Fussfessel in der Schweiz beim Vollzug von Freiheitsstrafen teilweise die Funktion der Justizvollzugsanstalt. Im Rahmen eines Pilotversuchs wurde damals sechs

Kantonen die Bewilligung erteilt, gewisse Freiheitsstrafen mittels elektronischer Überwachung zu vollziehen. Am Pilotversuch beteiligten sich die Kantone Basel-Stadt, Basel-Land, Bern, Genf, Tessin und Waadt. Ab dem Jahr

2003 kam der Kanton Solothurn dazu. Die Rückmeldungen der Kantone, welche sich am Pilotversuch beteiligt hatten, waren nach rund zehn Jahren Einsatz von EM generell positiv. Ab dem 1. Januar 2018 wurde die elektronische Überwachung im Strafgesetzbuch und damit im Bundesrecht vorgesehen. Seit diesem Zeitpunkt sind die Kantone verpflichtet, EM als Vollzugsform für Freiheitsstrafen anzubieten.

Die elektronische Überwachung kann unter gewissen Bedingungen für

Autorin/Autor

Janine Repetti-Dittes

Geschäftsführerin
Verein Electronic
Monitoring



zv9

Alain Hofer

Stellvertretender
Generalsekretär,
Konferenz der Kantonalen
Justiz- und
Polizeidirektorinnen
und -direktoren
(KKJPD)



zv9



«Die elektronische Überwachung kommt nur in Frage, wenn nicht zu erwarten ist, dass die verurteilte Person flieht oder weitere Straftaten begeht.»

den Vollzug von kurzen Freiheitsstrafen von 20 Tagen bis zu 12 Monaten zum Einsatz kommen (sogenanntes Front-door-EM). Zudem kann EM am Ende von langen Freiheitsstrafen zur Vorbereitung der bedingten Entlassung für die Zeitdauer von drei bis zwölf Monaten eingesetzt werden (sogenanntes Back-door-EM). Die elektronische Überwachung kommt nur in Frage, wenn nicht zu erwarten ist, dass die verurteilte Person flieht oder weitere Straftaten begeht. Zusätzlich muss die überwachte Person eine dauerhafte Unterkunft und eine geordnete Tagesstruktur (Arbeit, Ausbildung) haben und mit der Vollzugsform und dem Vollzugsplan einverstanden sein. Zudem muss sie sich als absprachefähig erweisen, und die erwachsenen Personen im gleichen Haushalt müssen mit der Vollzugsform einverstanden sein. Muss damit ge-

rechnet werden, dass von einer Person weiterhin Gefahr ausgeht, kommt EM im Freiheitsentzug nicht zum Einsatz.

Die angestrebten Ziele und Vorteile des Vollzugs von Freiheitsstrafen mittels elektronischer Überwachung liegen auf der Hand: Bei kurzen Freiheitsstrafen bis zu einem Jahr entfällt die Stigmatisierung, welche der Vollzug von Freiheitsstrafen in einer Vollzugsanstalt mit sich bringt, zu einem grossen Teil. Die verurteilte Person wird für den Vollzug einer verhältnismässig kurzen Freiheitsstrafe nicht aus ihren Alltagsstrukturen gerissen. Sie kann weiterhin einer Arbeit nachgehen und verbleibt in ihrem beruflichen und privaten Umfeld. Gleichzeitig darf die überwachte Person ihr Zuhause nur zu vorgegebenen Zeiten verlassen und muss die Freizeit im Hausarrest verbringen. Der Strafcharakter der Freiheitsstrafe bleibt da-

mit gewahrt. Am Ende einer langen Freiheitsstrafe kann die elektronische Überwachung eine kontrollierte Wiedereingliederung in die Gesellschaft erleichtern. Für die Allgemeinheit fallen damit auch deutlich geringere Vollzugs- und Wiedereingliederungskosten an.

Anwendungsfelder der elektronischen Überwachung

Inzwischen ist die elektronische Überwachung aber längst nicht mehr nur ein Thema im Bereich des Justizvollzugs als Vollzugsform für Freiheitsstrafen. Die schweizerische Strafprozessordnung sieht die elektronische Überwachung seit dem 1. Januar 2011 zur Überwachung von Ersatzmassnahmen als Alternative für die Untersuchungs- und Sicherheitshaft vor; im Strafgesetzbuch wurde die elektronische Überwachung am 1. Januar 2015 für den

Vollzug von Kontakt- und Rayonverboten eingeführt; ab dem 1. Januar 2022 sieht zudem das Zivilrecht die elektronische Überwachung zum Schutz gewaltbetroffener Personen vor. Weitere Anwendungsfelder werden derzeit diskutiert. So ist die elektronische Überwachung auch im Rahmen der polizeilichen Massnahmen zur Bekämpfung von Terrorismus vorgesehen, und auch im Bereich der ausländerechtlichen Zwangsmassnahmen wird der Einsatz von EM diskutiert.

Technische Anforderungen und Überwachungsarten

Mit den neuen Anwendungsfeldern haben sich auch die Anforderungen und Erwartungen an die Technik verändert. So wird beim Vollzug von Freiheitsstrafen in der Regel nicht überwacht, wo sich die verurteilte Person genau befindet, wenn sie nicht zu Hause ist. Über-

prüft wird nur die Tatsache, ob sich die Person zu den vorgegebenen Zeiten zu Hause aufhält oder nicht, es gibt also eine An- und Abwesenheitskontrolle an einem bestimmten Ort. Dazu braucht es beispielsweise keine GPS-Überwachung, um die genaue Position zu ermitteln. Gemessen wird einzig die Distanz zwischen dem Sender, welcher fest mit der verurteilten Person verbunden ist, und dem Empfänger, der im Haus der überwachten Person installiert wird. Über das Telefonnetz wird das Signal an die zuständige Stelle weitergeleitet, wo die eingegangenen Daten mit den programmierten Daten der überwachten Person verglichen werden. Stimmen die Abwesenheiten nicht mit den festgelegten Zeit überein, wird ein Alarm ausgelöst. Der Sender, welcher die überwachte Person trägt, ist technisch so konstruiert, dass eine Manipulation oder Entfernung sofort

einen Alarm auslöst. Diese sogenannte RF (=radio frequency)-Überwachung wird in der Schweiz aktuell am häufigsten eingesetzt.

Bei den anderen Anwendungsbe-reichen stellen sich teilweise andere Anforderungen an die Technik. Bei der zivilrechtlichen Anwendung der elektronischen Überwachung zum Schutz gewaltbetroffener Personen wird beispielsweise gefordert, dass der Aufenthaltsort der überwachten Person fortlaufend ermittelt und aufgezeichnet werden kann. Dies ist nur mit einer GPS-Überwachung möglich. Diese GPS (=global positioning system)-Überwachung ermöglicht eine kontinuierliche Aufenthaltskontrolle und die Erstellung von Bewegungsprofilen. Technisch existieren verschiedene Lösungen, wie eine GPS-Überwachung gewährleistet werden kann. Bei einer Überwachung mit GPS entsteht auch eine zusätzliche



«Künftig soll der Anwendungsbereich der elektronischen Überwachung ausgeweitet werden, und zwar vor allem im Zuständigkeitsbereich der Polizei. Im Zentrum steht dabei der präventive Einsatz gegen häusliche Gewalt und Stalking.»

präventive Wirkung. Die überwachte Person muss sich bewusst sein, dass sie durch die jederzeit mögliche Lokalisation ihres Aufenthaltsortes einem deutlich höheren Entdeckungsrisiko ausgesetzt ist.

Technische Grenzen bei der GPS-Überwachung ergeben sich dadurch, dass der Satellitenempfang an bestimmten Orten eingeschränkt ist, z.B. innerhalb von grossen Einkaufszentren, in Kellern oder Tunnels. An diesen Orten, welche für GPS-Signale unzugänglich sind, kann das System durch das Mobilfunknetz ergänzt werden. Dabei wird der jeweilige Aufenthaltsort über die Distanz zum nächsten Mobilfunkmast berechnet. Die Genauigkeit der Ortung variiert jedoch je nach Deckungsgrad der Gegend mit Mobilfunkmasten.

Bei der Aufenthaltskontrolle mittels GPS-Technologie können die Bewegungen der überwachten Person entweder retrospektiv (sogenannte passive Überwachung) oder in Echtzeit (sogenannte aktive Überwachung) verfolgt werden. Bei der passiven Überwachung werden die Bewegungsdaten hauptsächlich zu Bürozeiten von der zuständigen Behörde geprüft. Bei der aktiven Überwachung wird das Ziel einer Echtzeit-Lokalisierung rund um die Uhr verfolgt. Nach Eingang einer Alarmmeldung kann dabei umgehend eine vordefinierte Intervention ausgelöst werden. Diese Alarmmeldungen werden dabei von einer Überwachungszentrale bearbeitet. Die vordefinierte Reaktion kann die Form einer telefonischen Kontaktaufnahme mit der überwachten Person bis hin zur Einleitung von polizeilichen Interventionen bestehen. Durch den Einsatz der elektronischen Überwachung darf jedoch nicht suggeriert werden, dass dadurch Straftaten zuverlässig verhindert werden könnten. Beim Einsatz von aktiver Überwachung besteht die Gefahr, dass das System Erwartungen weckt, welches es nicht erfüllen kann. Der Einsatz einer aktiven Überwachung ist daher vorsichtig zu planen und immer dann problematisch,

wenn ein Verstoß gegen die Auflagen eine unmittelbare Polizeiintervention nötig macht, um mögliche Straftaten zu verhindern.

Stand der interkantonalen Zusammenarbeit

Im Rahmen der Anwendung der elektronischen Überwachung hat sich gezeigt, dass es sinnvoll ist, wenn nicht jeder Kanton für seine Einzelfälle eigene Strukturen aufbaut und betreibt. Die Konferenz der kantonalen Justiz- und Polizeidirektoren (KKJPD) hat deshalb bereits im Jahr 2013 die Arbeiten zur Harmonisierung des Vollzugs der elektronischen Überwachung in Auftrag gegeben. Im Herbst 2019 erfolgte schliesslich die Gründung des Vereins «Gesamtschweizerisches Electronic Monitoring – Investition und Betrieb». Zwischenzeitlich sind 22 Kantone dem Verein beigetreten. Ziel des Vereins ist es, den Mitgliedskantonen ein einheitliches System für die elektronische Überwachung anzubieten. Dies soll mit einer ganzheitlichen Betrachtung aller Bedürfnisse der Kantone für die verschiedenen Anwendungen geschehen.

In der Herbstversammlung der KKJPD im November 2020 wurde von den Mitgliedskantonen entschieden, dass vorderhand keine gemeinsame Überwachungszentrale im Rahmen des heutigen Projekts betrieben werden soll. Eine aktive Überwachung ist mit dem neuen System daher in einer ersten Phase nicht flächendeckend möglich. Die KKJPD hat gleichzeitig festgehalten, dass die ausgeschriebene Technik es jedoch möglich machen müsse, eine solche dereinst ans System anzuschliessen. Damit sei es möglich, die aktive Überwachung zu einem späteren Zeitpunkt reibungslos einzuführen, dann nämlich, wenn genügend Erfahrungen von den Kantonen vorlägen, die bereits heute mit einer Überwachungszentrale zusammenarbeiten und aktive Überwachung betreiben.

Im Februar 2021 wurde eine öffentliche Ausschreibung durchgeführt, um einen technischen Betreiber zu finden,

der eine Gesamtlösung gemäss den Anforderungen und Bedingungen anbietet, die in der Konzeptionsphase des Projekts gemeinsam mit den Kantonsvertretern und verschiedenen Interessengruppen erarbeitet wurden. Derzeit werden die Geräte der verschiedenen Anbieter in drei Pilotkantonen ausgiebig getestet. Das neue System soll im Laufe des Jahres 2022 in allen Kantonen eingerichtet werden und spätestens ab dem 1. Januar 2023 zum Einsatz kommen.

Fazit und Ausblick

Die elektronische Überwachung wird heute in der Schweiz hauptsächlich im Freiheitsentzug eingesetzt. Hauptzweck ist dabei, Verstösse gegen behördliche Auflagen nachträglich festzustellen und die Absprachefähigkeit mit der verurteilten Person zu testen. Verstösse werden den zuständigen Stellen zur Kenntnis gebracht und – falls notwendig – sanktioniert. Die elektronische Überwachung ist in seiner heutigen Anwendung also eine alternative Sanktionsform und dient nicht dazu, Straftaten zu verhindern.

Künftig soll der Anwendungsbereich ausgeweitet werden, und zwar vor allem im Zuständigkeitsbereich der Polizei. Im Zentrum steht dabei der präventive Einsatz gegen häusliche Gewalt und Stalking. Hier sollen der Einsatz der elektronischen Überwachung in Abstimmung mit anderen Instrumenten des Gewaltschutzes geprüft und Erfahrungen gesammelt werden. Dabei wird insbesondere die Kombination von elektronischen Überwachungsmaßnahmen mit einem wirkungsvollen Bedrohungsmanagement als erfolgsversprechend erachtet.

Durch den Verein Electronic Monitoring soll den Kantonen ein einheitliches und zweckdienliches System für die elektronische Überwachung zur Verfügung gestellt werden. Das Ziel muss es sein, dass die elektronische Überwachung und die damit verbundenen technischen Möglichkeiten immer dort zum Einsatz kommen, wo sie einen echten Mehrwert generieren.

«Man muss immer abwägen.»

Ein Gespräch mit Jürg Halter über die Frage, wie private und staatliche Überwachung mit der Corona-Krise, der Digitalisierung, der Demokratie, dem Wunsch nach einfachen Antworten und mit Sprache an sich zusammenhängt.



© by Rob Lewis

Der mehrfach ausgezeichnete Schriftsteller und Sprachkunst-Performer Jürg Halter lebt und arbeitet in Bern. Er äussert sich sowohl in den klassischen als auch in den sozialen Medien regelmässig zu gesellschaftspolitischen Themen. Zuletzt erschien sein Gedichtband «Gemeinsame Sprache» im Dörlemann Verlag.

Jürg Halter, Anfang des Jahres waren Sie im Literaturclub des SRF zu Gast und haben eine Neuübersetzung von George Orwells «1984» vorgestellt, des wohl berühmtesten Romans zum Thema «Überwachung». Was interessiert Sie an dieser Thematik?

In dem 1949 erschienenen Roman von Orwell wird beispielhaft gezeigt, wo es hinführen kann, wenn ein Staat alles und jeden, jede Äusserung kontrolliert, denn darin werden alle Menschen rund um die Uhr überwacht. Von Teleschirmen aus bekommen sie Anleitungen, wann sie zu Bett gehen sollen, wann sie

aufstehen sollen, sie werden bei der Arbeit überwacht, und es gibt eine Gedankenpolizei, die mithilfe der Teleschirme Gesichtsausdrücke interpretiert, erkennt, ob jemand z.B. gerade etwas gedacht hat, was sich gegen den Staat richtet oder gegen eines seiner Gesetze. Die Leute werden dann aus dem Schlaf gerissen, verhaftet und verschwinden einfach. Oder sie kriegen eine Gehirnwäsche und werden anschliessend, sozusagen geläutert, oder besser: gehirnamputiert, in die Gesellschaft zurückgeführt. Einerseits könnte man sagen, das sei eine Übertreibung,

andererseits bezieht sich Orwell natürlich auf reale Diktaturen, die es damals gab, vor allem auf den Stalinismus und natürlich auch auf Hitlerdeutschland. Das Faszinierende und Erschreckende an diesem Roman ist, wie aktuell er immer noch ist.

... oder wieder ist oder eigentlich zum ersten Mal in genau dieser technischen Grössenordnung, denn z.B. die Überwachung der Mikromimik wäre ja vielleicht bald technisch zu leisten.

Genau. Der Roman reflektiert einerseits die Zeit, in der er entstand, und ist andererseits auch deshalb so erschreckend, weil er einen Blick in die Zukunft gewagt hat, der in vielem unheimlich treffend ist. Und noch beklemmender wird es vielleicht, wenn man bedenkt, dass die Technologie heute viel weiter ist, als es damals mit aller Phantasie vorstellbar war. Zum Beispiel bei den «Deep Fakes», also dass man mithilfe weniger Videoaufnahmen eines Menschen ihn etwas sagen lassen kann, was er nie gesagt hat, und aufgrund dessen entsprechend belasten könnte. Ein grosser Unterschied zur Überwachungspraxis im Roman ist auch, dass sich heute viele Menschen freiwillig oder vermeintlich freiwillig selbst überwachen, mit ihren Smartphones und -watches, die sie z.B. beim Joggen mittragen und die dann Puls, Herzfrequenz usw. messen und an die Versicherung übermitteln, die dann Prämiensenkungen gewährt, gegebenenfalls. Aber die meisten Daten, die heute von und über uns gesammelt werden, über unsere Smartphones, Computer usw., sind Daten, die erst in Zukunft potentiell für oder gegen uns verwendet werden können; der grösste Teil ist noch gar nicht ausgewertet.

Nun leben wir ja in der Schweiz in einer der – man ist fast geneigt zu sagen – letzten verbliebenen Demokratien, weit entfernt von einer dystopischen Gesellschaft à la Orwell. Wie stark also sehen Sie das Problem für uns? Wie sehr sind wir gefährdet, dass sozusagen durch die

Hintertür der Technik ganz plötzlich demokratische Errungenschaften ausgehebelt werden?

Ich sehe grundsätzlich zwei Arten möglicher Bedrohungen: einerseits durch globalisierte Technologie-Riesen, die unablässig Daten sammeln, andererseits durch den Staat, hier aber eher durch seine Passivität. Denn gegenüber internationalen Konzernen zeigt sich der Staat oft völlig machtlos, obwohl es gesetzliche Möglichkeiten gäbe, die Überwachung durch Technologiekonzerne einzuschränken. Aber das funktioniert nur, wenn z.B. die gesamte EU entsprechende Beschlüsse fasst; ein Land allein kann da wenig machen. Eine Hauptgefahr besteht auch in der gutgläubigen Haltung vieler Menschen, die sich oft in dem Satz manifestiert, dass «wenn man nichts falsch macht, einem auch nichts passieren kann». Aber die Frage ist doch immer: Wer definiert, was falsch und was richtig ist? Da kann es schnell bei einem Systemwechsel passieren, dass das, was man eben noch als richtig empfand, plötzlich als falsch taxiert wird, und dann wird's richtig gefährlich. Die Digitalisierung wird meiner Meinung nach immer noch viel zu positiv verkauft, nämlich fast ausschliesslich als Vergrösserung der Freiheit. Doch durch die Digitalisierung wird der Mensch immer gläserner, und das macht ihn auch immer verletzlicher. Und wenn der einzelne Mensch immer verletzlicher wird, dann werden die ganze Gesellschaft und die Demokratie an sich mehr und mehr gefährdet, denn Demokratie lebt eben von Vertrauen.

Wie genau ist der Zusammenhang von fortschreitender Digitalisierung und abnehmendem Vertrauen? In der Corona-Krise war und ist zu beobachten, dass das Vertrauen in die Massnahmen des Staates vielerorts nicht mehr gegeben ist. Auch prominente Kollegen von Ihnen aus der Kulturszene äussern sich skeptisch, sehen Verschwörungen oder sprechen sogar von einer Corona-Diktatur. Was sagen Sie dazu?

Grundsätzlich haben viele Menschen die Tendenz, wenn ihnen ein Mikrofon mit einer Frage hingehalten wird, dass sie darauf antworten, obwohl sie gar nicht die Kompetenz dazu haben. Kulturschaffende sind ja auch nicht gegen Dummheit gefeit und genauso anfällig wie andere für zu einfache Antworten, Feindbilder und Verschwörungstheorien. Es gibt zwar einige Staaten, die man schon vor der Corona-Krise nicht mehr als Demokratien bezeichnen konnte, die die Massnahmen zur Bekämpfung der Krise zum Anlass genommen haben, die Freiheit der Bürger noch weiter einzuschränken. Das ist tatsächlich passiert. Hingegen hier in der Schweiz von einer Corona-Diktatur zu reden, ist ein Witz, denn die Massnahmen waren im Grossen und Ganzen gut nachvollziehbar und wurden verständlich kommuniziert. Es können aber auch nicht alle Massnahmen auf Anhieb immer stimmig und alternativlos sein, die Krise ist für alle neu, und man muss flexibel reagieren. Dass der Staat, den viele ausser beim Steuerzahlen gar nicht mehr bewusst wahrnehmen, innerhalb kurzer Zeit wieder so viel Macht erhalten hat, kam überraschend, aber anders lässt sich auf eine Naturkatastrophe wohl nicht reagieren. Hätte man über die Massnahmen erst Volksabstimmungen durchgeführt, wären die Todeszahlen viel höher und die Katastrophe viel grösser. Doch viele Menschen suchen einfache Erklärungen, wittern böse Mächte im Hintergrund, glauben, dass die Pandemie nur ein Ablenkungsmanöver sei usw. Solche Verschwörungstheorien gab es schon immer, aber durch die Digitalisierung können sie sich viel schneller ausbreiten, und Menschen, die daran glauben, sind viel schneller miteinander verbunden.

Welche Rolle spielen die Medien dabei?

Die Medien, die natürlich auch auf die eigenen Klickzahlen schauen, konzentrieren sich oft auf die lautesten Stimmen, obwohl diese selten grössere Teile der Bevölkerung repräsentieren.

Da sehe ich natürlich auch eine Verantwortung der Medien, die z.B. den Begriff Skepsis, der eigentlich klar definiert ist, oft falsch verwenden. Wer die Existenz oder die Gefährlichkeit des Virus leugnet, der ist eben kein Skeptiker, sondern ein Leugner. Wer hingegen die Massnahmen argumentativ nachvollziehbar kritisiert, ist ein Skeptiker. Aber in den Medien werden diese Begriffe oft durcheinandergebracht. Den Medien würde ich sagen: Schenkt denjenigen Menschen, die bereit sind, sich kritisch zu äussern, aber ihre Kritik auch mit rationalen Argumenten begründen können, mehr Aufmerksamkeit als denen, die lügen und Verschwörungstheorien verbreiten. Leute, die ernsthaft sagen, wir lebten hier in einer Diktatur, würde ich übrigens gerne einen Flug nach Weissrussland oder nach Nordkorea spendieren, damit sie dort versuchen, ihre Vorstellung von Freiheit zu leben!

Oder nach Österreich? Scherz beiseite. Es scheint so, als habe man sich früher leichter darauf einigen können, was ein Faktum ist und was nicht, und anschliessend darüber diskutiert, wie die Fakten zu bewerten seien. Heute scheint zu jedem Faktum auch ein alternatives Faktum zu gehören, jeder kann glauben, was er will, aber es als Faktenwissen deklarieren. Wie kommt das?

Die digitale Technik gibt vielen Leuten das Gefühl, sie dürften jetzt dabei mitreden, wo früher nur die sogenannten Eliten mitreden durften. Das ist einerseits positiv, andererseits höchst problematisch, denn dadurch ist die Hemmschwelle, sich zu äussern, extrem gesunken. Früher musste man sich z.B. bemühen, einen Leserbrief zu schreiben, mit der Schreibmaschine oder per Hand, ihn dann noch zu frankieren und einzuschicken, das waren mehrere Hürden. Und dann gab es immer noch eine Redaktion, die entschieden hat, ob er gedruckt werden soll oder nicht. Heute macht man einen Klick, und das Ding ist veröffentlicht. Das ist natürlich verlockend. Jede und jeder wird zum

eigenen Medium. Dabei kommt es zu vielen Widersprüchen: Menschen, die ihrerseits ständig persönliche Fakten und Fotos von sich in sozialen Netzwerken preisgeben und sich dann über die Registrierung in Restaurants empören, weil sie sich in ihrer Freiheit bedroht fühlen. Ich denke, diese Widersprüchlichkeit ist uns aber allen nicht ganz fremd: Zwischen dem Pochen auf Anonymität und Privatsphäre einerseits und dem eigenen Verhalten andererseits, mit dem wir uns selbst hintergehen.

Was den Komplex Fakten vs. Behauptungen, Meinungen, Fake News usw. angeht, finde ich diese Entwicklung grundsätzlich problematisch, weil auch hier nicht differenziert wird: Denn man kann ja sowohl hinter der Wissenschaft stehen und an Fakten glauben und trotzdem bestimmte wissenschaftliche Entwicklungen auch kritisch sehen. Also wenn man z.B. eine Studie liest, wo es um Zuckergehalt in Lebensmitteln geht, und sich dann etwas eingehender informiert und merkt, dass hinter dieser Studie der Auftrag eines Nahrungsmittelkonzerns steht, dann sollte man die Studie vielleicht etwas kritischer sehen. Man muss immer abwägen. Doch viele Menschen wollen eindeutige Antworten und halten Widersprüche nicht aus. Als gäbe es immer nur richtig oder falsch, dafür und dagegen, entweder oder.

Da ist es ja wieder, das binäre Prinzip der digitalen Welt: Ja oder Nein, Nullen und Einsen! Kluge Leute haben schon in den siebziger und achtziger Jahren befürchtet, dass die Durchdringung unseres Lebens und Denkens mit Digitalität uns schliesslich zu Opfern derselben werden lässt. Dahingehend, dass wir uns gar nicht mehr vorstellen können, dass es auch ein «Sowohl als auch», ein «Weder noch» und ein «Vielleicht» auszuhalten gilt.

Das ist der entscheidende Punkt, dass die Digitalisierung tatsächlich einen Einfluss auf das Denken an sich hat. Das zeigt sich z.B. auch im Ausbil-

dungssystem mit Multiple-Choice-Tests: Man muss nicht mehr selbst formulieren und abwägen können, sondern man kann einfach das oder das klicken, fertig. Das ist gefährlich, weil eine Demokratie, die diesen Namen auch verdient, von Vielseitigkeit und Differenzen lebt, von der Toleranz und dem Respekt anderen Meinungen und Ansichten gegenüber. Aber auch davon, dass man bei gewissen Sachen einen Konsens findet, z.B. in Bezug auf das Funktionieren der Demokratie selbst! Davon lebt ein Rechtsstaat. Doch die Digitalisierung, so wie sie sich bis jetzt entwickelt hat, hat eben sehr stark die Tendenz, dass man sich immer für die eine oder die andere Seite entscheiden zu müssen glaubt. Das führt letztlich zu einer Zersplitterung der Gesellschaft in immer dichtere Bubbles Gleichdenkender.

Jean Ziegler hat Sie einmal eine «wichtige politische Stimme» in unserem Land genannt. Was ist der Zusammenhang zwischen Ihrer Tätigkeit als Schriftsteller und Sprachkünstler und Ihrem politischen Engagement?

Da Sprache mein Medium ist, versuche ich mir immer bewusst zu machen, zu was Sprache alles fähig ist, also nicht nur in der Kunst, sondern insgesamt in der Gesellschaft. Sprache ist ja oft auch das Medium, mit dem eine Demokratie zuerst angegriffen und auch verteidigt wird. Sprache wird als Propagandamittel benutzt, und deshalb interessiert es mich nicht nur, schöne Bücher oder Gedichte zu schreiben, sondern auch allgemein: Was wird von wem wie gesagt oder nicht gesagt; was wird benannt, und was wird umschifft in einer Formulierung. Deshalb analysiere ich z.B. auch gerne die Reden von Politikern oder Konzernchefs. Gerade mit dem, was nicht gesagt wird, wird ja oft mehr gesagt als mit dem, was gesagt wird. Auch Juristen sind oft sehr sprachbewusste Menschen, weil es in ihrer Sprache entscheidend ist, wie man etwas formuliert. Nehmen wir zum Beispiel den Begriff «Gefährder»:

das ist ja ein sehr schwammiger Begriff, und je nach System oder je nachdem, wie das definiert ist, kann man als einen «Gefährder» schon jemanden verstehen, der einfach kritisch denkt. Und man könnte den Begriff dann auch dahingehend definieren, dass so jemand überwacht werden muss.

Geht es nur um Aussagen, die schwammig bzw. gar nicht formuliert werden? Oder sind wir nicht schon noch einen Schritt weiter, dass viele Begriffe einfach neu besetzt werden? Es gibt diesen Satz, der Adorno zugeschrieben wird: «Ich habe kein Angst vor der Wiederkehr der Faschisten als Faschisten, aber vor ihrer Wiederkehr als Demokraten.» Genau das ist ja jetzt gerade z.B. beim Begriff «Terrorismus» zu beobachten: Die Diktatoren und Autokraten um uns herum werfen den friedlichen Demonstranten, investigativen Journalisten und sonstigen politischen Gegnern inzwischen schon reflexartig «Terrorismus» vor, denn wer Terroristen verhaften lässt, kann ja nichts falsch machen. Eigentlich ist es aber nur eine dreiste Neubesetzung des Begriffs, keine schwammig, sondern eine präzise formulierte Lüge. Wie kommt man dagegen an?

Ich sehe eine grosse Gefahr darin, wenn Begriffe umgedeutet werden, im schlimmsten Fall in ihr Gegenteil, um dadurch Freiheitsrechte einzuschränken. Das kann auf ganz verschiedenen Ebenen passieren, also z.B. in Bezug auf die zunehmende Überwachung, dass man sie als Verteidigung der Freiheit beschreibt und die Hälfte der Wahrheit einfach weglässt. Meine Aufgabe als Schriftsteller bzw. jemand, der sich öffentlich kritisch äussert, sehe ich darin, genau hinzuhören – und zu benennen –, was eigentlich gesagt wird. Um unliebsame Kritik abzutun, werden ja oft Begriffe gewendet, um die Kritiker zu diskreditieren, als böse darzustellen, oder unangenehme Fakten werden sprachlich verwässert. So dass man etwa die Kritik an der Einschränkung von Freiheit dann ihrerseits

als Angriff auf die Freiheit umdeutet. Dagegen kommt man allenfalls an, indem man nicht müde wird, sprachliche Manipulationen und Verdrehungen als solche zu benennen und die Menschen darüber aufzuklären.

Noch eine persönliche Frage: Fühlen Sie sich eigentlich überwacht?

Ich weiss, dass ich mich sehr überwachbar mache, allein schon durch die Computer, die ich nutze, und immer wenn ich mich mit dieser Thematik beschäftige, erschrecke ich, wie stark ich wahrscheinlich wirklich schon überwacht werde. Dafür, dass ich weiss, wie viele Daten ich preisgebe, gehe ich eigentlich sehr unvorsichtig damit um. Deshalb finde ich's eben auch falsch, wenn der Staat diese Verantwortung an die Bürger abgibt. Es ist die Aufgabe des Staates, die Technologiekonzerne so einzuschränken, dass sie gar nicht die Möglichkeiten haben, mehr über die Menschen zu erfahren, als es gesetzlich erlaubt ist. Die Idee von der Eigenverantwortung der Nutzer halte ich für eine Illusion. Und auch für den Staat braucht es unabhängige Stellen, die ihn überwachen, was er mit den Daten von uns Bürgern eigentlich macht. Wenn der Staat überwacht, muss er auch überwacht werden. Je mehr und tiefer ein Staat überwacht, desto paranoider ist er ja, desto weniger Vertrauen hat er in seine Bürger.

Überwachung ist gut, Vertrauen ist besser?

Um Überwachung zu begründen, werden ja oft Sicherheitsinteressen genannt. Es ist immer ein Abwägen zwischen Sicherheit und Freiheit. Die absolute Sicherheit ist vielleicht möglich, aber dann gibt's keine Freiheit mehr. Es geht eben nicht um ein «Entweder oder», sondern um ein «Sowohl als auch»! Bei dieser Frage bin ich natürlich grundsätzlich dafür, dass sie demokratisch und transparent verhandelt wird.

Jürg Halter, vielen Dank für das interessante Gespräch!



Beschmierter BAG-Plakat in der Berner Altstadt im April 2021

Bürger/innen und die Polizei: Wer darf wen in der Öffentlichkeit filmen?

In der Schweiz sind polizeiliche Bodycams umstritten und kommen noch nicht standardmässig zum Einsatz. Videoaufnahmen der Polizei fallen – anders als in den USA – grundsätzlich nicht unter das Öffentlichkeitsprinzip. Gleichzeitig ist das Filmen von Polizeieinsätzen für Bürger/innen, zuweilen auch für Journalist(inn)en riskant; sie müssen mit Repressionen rechnen. Eine verstärkte und differenzierte Rechtsprechung könnte in Zeiten allgegenwärtiger Kameras für alle Seiten von Vorteil sein.

Kennen Sie «Audit the Audit», den amerikanischen YouTube-Kanal, der sich mit dem «Right and Wrong of Police Interactions» befasst? Auf Grundlage von Videoaufnahmen wird dort bewertet, wie sich die beteiligten Personen – Polizist(inn)en und sonstige Beamtinnen und Beamte einerseits und Bürgerinnen und Bürger andererseits – bei den verschiedensten Einsätzen verhalten. Die Interaktionen werden mit Verweis auf gesetzliche Grundlagen und einschlägige Rechtsprechung kommentiert. Abschliessend werden die beteiligten Personen benotet. So kann eine Polizistin, die sich rechtskonform und vorbildlich verhält, die Höchstnote A+ erhalten, während ein Bürger, der sich falsch verhält, mit F als ungenügend bewertet wird.

Autor

Martin Steiger

Lic. iur. HSG
Anwalt für Recht im
digitalen Raum,
Zürich



«Right to Record the Police» in den USA

Die Videoaufnahmen stammen von Smartphones und Videokameras von Bürger(inne)n sowie von Bodycams und Dashcams der Polizist(inn)en. In den USA dürfen Bürger grundsätzlich Einsätze der Polizei filmen, selbst wenn sie direkt betroffen sind, zum Beispiel bei einer Verkehrskontrolle. Gleichzeitig filmen viele Polizeikörpers ihre Einsätze standardmässig mit eigenen Kameras. Diese Aufnahmen gelten als «Public Record» und sind grundsätzlich öffentlich zugänglich. Das Gleiche gilt für Fotografien und Tonaufnahmen. Den rechtlichen Hintergrund bilden der *Freedom of Information Act (FOIA)* auf Bundesebene sowie vergleichbare Gesetze in den amerikanischen Bundesstaaten. Das Filmen der Polizei ist ein «First Amendment Right» und Teil der Meinungs- bzw. Redefreiheit in den USA («Freedom of Speech»). Mit «First Amendment Audits» prüfen – ganz unterschiedlich «sympathisch» auftretende – Aktivistinnen und Aktivisten, ob ihre Redefreiheit in dieser Hinsicht gewährleistet ist.

Die Bedeutung solcher Videoaufnahmen zeigte kürzlich der Tod von George Floyd bei einem Polizeieinsatz in Minneapolis. Die Aufnahmen von Zeuginnen und Zeugen sowie der Polizei sorgten weltweit für Aufsehen und bildeten eine wichtige Grundlage für das Strafverfahren.

In der Schweiz sind polizeiliche Bodycams politisch umstritten und kommen noch nicht standardmässig zum Einsatz. Videoaufnahmen der Polizei fallen – anders als in den USA – grundsätzlich nicht unter das jeweilige Öffentlichkeitsprinzip bei Bund und Kantonen.

Gleichzeitig ist das Filmen von Polizeieinsätzen in der Schweiz riskant. Wer Polizistinnen im Einsatz filmt, muss als Bürger/in, aber auch als Journalist/in, mit Repressionen rechnen. Es kommt immer wieder vor, dass Personen, die Polizeieinsätze filmen, festgehalten und gezwungen werden, Videoaufnahmen zu löschen oder gar ihr Smartphone herauszugeben. Am 1. Mai 2021 wurden Medienschaffende in Zürich teilweise bei der Berichterstattung behindert.

Recht vs. Realität beim Filmen in der Öffentlichkeit

Unabhängig von Polizeieinsätzen gewinnt das Filmen in der Öffentlichkeit an Bedeutung. Einerseits verfügen fast alle Menschen mit ihrem Smartphone über eine leistungsfähige und jederzeit griffbereite Kamera, andererseits kann mit Videoaufnahmen aus der Öffentlichkeit auf TikTok und anderen Social Media-Plattformen viel Aufmerksamkeit erzielt werden. Dafür stehen beispielhaft die inzwischen zahlreichen «Szene isch»-Kanäle. Auch Dashcams in Fahrzeugen werden immer beliebter. Im Onlinehandel umfasst diese Kategorie inzwischen über 100 jederzeit lieferbare Produkte.

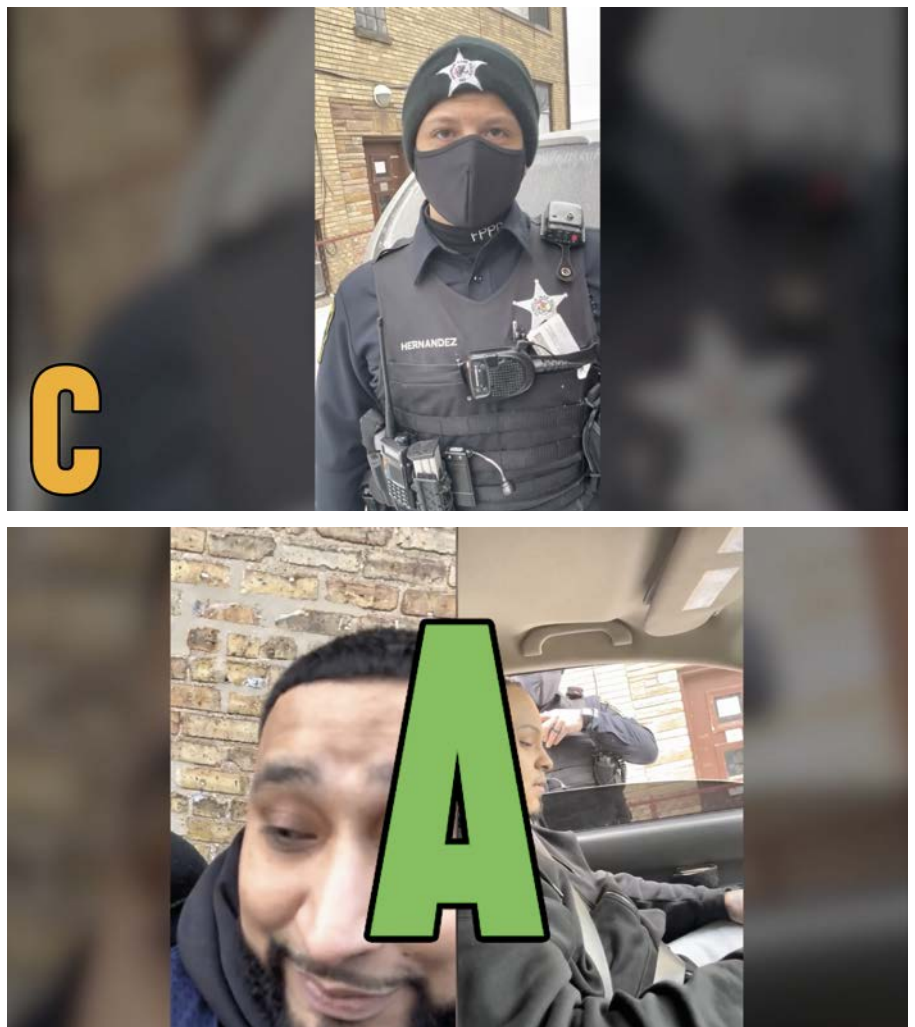
Die Realität, dass in der Öffentlichkeit gefilmt wird und solche Aufnahmen veröffentlicht werden, kollidiert mit der bestehenden schweizerischen Rechtsordnung. Nicht nur Polizist(inn)en dürfen

darauf zählen, die Rechtsprechung gegen das Filmen ihrer Einsätze häufig auf ihrer Seite zu haben. Genauso verhindert die Rechtsprechung bislang, dass Dashcam-Aufnahmen für die Verfolgung von Übertretungen und Vergehen – und damit für den allergrössten Teil der mutmasslichen Straftaten im Strassenverkehr – verwertet werden dürfen. Allein schon das Filmen ohne anschließende Veröffentlichung kann den Datenschutz und den Persönlichkeitsschutz insbesondere mit dem «Recht am eigenen Bild» verletzen. Seit dem Google-Street-View-Urteil des Bundesgerichts von 2012 ist klar, dass selbst Personen, die «Beiwerk» sind, bei digitalen Aufnahmen grundsätzlich einverstanden sein müssen, gefilmt zu werden.

Die hohen Hürden für betroffene Personen, gegen unerwünschte Videoaufnahmen vorzugehen, führt dazu, dass der Persönlichkeitsschutz fast nur durch verteidigte Beschuldigte in Strafverfahren thematisiert werden kann. Das dürfte ein Grund sein, wieso viele Polizist(inn)en versuchen, das Filmen ihrer Einsätze von Anfang an zu verhindern. Dazu trägt bei, dass das «Recht am eigenen Bild» keinen strafrechtlichen Schutz genießt, sondern auf dem Zivilweg durchgesetzt werden muss, was – politisch ausdrücklich gewollt – aufwendig ist und nicht ohne anwaltliche Begleitung funktioniert.

Wachsende Bedeutung von Filmen in der Öffentlichkeit

Die wachsende Bedeutung von Videoaufnahmen aus der Öffentlichkeit – insbesondere von Polizeieinsätzen – wird immer stärker wahrnehmbar. So zeigt sich beispielsweise, dass die Polizei gegen mutmassliche Rechtsverstösse bei Kundgebungen sehr unterschiedlich vorgeht: Bei Kundgebungen aus dem linken politischen Lager kommt es immer wieder zu erheblicher Repression – auch gegen Medienschaffende –, während bei einigen Kundgebungen gegen Massnahmen zum Schutz von Menschen gegen COVID-19 mit Verweis auf die angebliche «Verhältnismässig-



«Kennen Sie *Audit the Audit*, den amerikanischen YouTube-Kanal, der sich mit dem *Right and Wrong of Police Interactions* befasst?»

keit» nicht nur weitgehend auf ein solches Vorgehen verzichtet wurde; die Polizeikräfte mussten sich zum Teil regelrecht von Demonstrierenden vorführen lassen, andernorts hingegen kam es teilweise zu Verbrüderungsszenen. Videoaufnahmen ermöglichen die Diskussion über diese Ungleichbehandlung. Diese Diskussion sollte im demokratischen Rechtsstaat selbstverständlich sein, erfolgt aber zu häufig erst aufgrund von «Beweisen» in Form von veröffentlichten Videoaufnahmen. Sie hilft unter anderem jenem Teil der Polizei, der mit dem gewählten Vorgehen nicht einverstanden ist, sich aber nicht kritisch äussern kann oder möchte. Bei öffentlichen Polizeieinsätzen erscheint mir klar, dass diese gefilmt

werden dürfen, solange die Persönlichkeit der beteiligten Polizist(inn)en nicht widerrechtlich verletzt wird. Rechtlicher Massstab ist, dass es ein überwiegendes öffentliches Interesse an einer wirksamen Kontrolle der Tätigkeit der Polizei gibt. Dabei gibt es keinen Grund, Medienschaffende unnötig zu privilegieren, denn im digitalen Raum kann jede/r Bürger/in jederzeit zur/m Medienschaffenden werden, während bei traditionellen Medien die Grenzen zwischen beruflichen und privaten Rollen verschwimmen. Das Filmen und Veröffentlichlichen findet dort seine Grenze, wo einzelne Polizisten als Personen ohne begründeten Anlass zu ihrem Nachteil in den Fokus gerückt werden, das heisst, allein aufgrund ihrer Tätigkeit



«In Bezug auf Polizeieinsätze sollte – gesetzlich oder gerichtlich – klargestellt werden, dass es grundsätzlich ein «Right to Record the Police» nach amerikanischem Vorbild gibt.» (Bild: 1. Mai 2021 in Zürich, YouTube-Video von Harp Lover)

für die Polizei. Einzelne Polizist(inn)en verfügen zwar über eine grosse Machtfülle und stehen für das staatliche Gewaltmonopol, zählen im Einsatz aber grundsätzlich zum Kollektiv der Polizei. Umgekehrt sollen Polizist(inn)en ihre Einsätze – unter klaren Rahmenbedingungen – mit Bodycams filmen dürfen, allenfalls sogar filmen müssen. Dort, wo gefilmt werden muss, sollten die Aufnahmen grundsätzlich dem Öffentlichkeitsprinzip unterliegen. Die Rechte der gefilmten Personen könnten bei der Herausgabe geprüft und angemessen gewährleistet werden.

Rechtssicherheit für das Filmen in der Öffentlichkeit

Für das Filmen in der Öffentlichkeit durch Bürger/innen im Allgemeinen muss Rechtssicherheit mindestens in ausgewählten Bereichen geschaffen werden. So könnte die Verwendung von Dashcams im Interesse der Verkehrssicherheit konstruktiv reguliert werden. Die Kritik an Videoaufnahmen bzw. Videoüberwachung ist meist berechtigt, weil das Wissen oder nur schon das Gefühl, gefilmt zu werden, das menschliche Verhalten beeinflusst. Ein solcher

«Überwachungsdruck» ist in einer freien Gesellschaft weitgehend, aber nicht immer unerwünscht – so zum Beispiel nicht im Strassenverkehr. Eine Regulierung von Dashcams könnte unter anderem bedeuten, dass ausschliesslich ausgewählte Ereignisse im Bereich von wenigen Minuten gespeichert und durch Behörden verwertet werden dürfen. Das anlasslose Speichern von stundenlangen Aufnahmen, wie es heute üblich ist, wäre hingegen verboten.

Mehr Rechtsprechung würde auch zur Klärung beitragen, wer in der Öffentlichkeit unter welchen Voraussetzungen wen filmen darf. Rechtsprechung, die den gesellschaftlichen Wandel und angesichts von allgegenwärtigen Smartphones offensichtlich veränderten gesellschaftlichen Konsens dokumentiert, ist wesentlich wirksamer als ein aussichtsloses Verbot. Wer gar nicht filmen dürfen soll, findet dennoch Mittel und Wege. So lernen Demonstrierende zunehmend, dass es nicht klug ist, aus einer Kundgebung heraus und mit einem privaten Smartphone Videoaufnahmen zu erstellen. Wer beim Filmen in einer Kundgebung auf Nummer sicher gehen möchte, streamt

seine Aufnahmen zumindest live im Internet, um eine Sicherstellung durch die Polizei zu verhindern, oder filmt versteckt. Wenn das Ziel ist, eine Kundgebung ungefährdet und umfassend zu dokumentieren, bietet es sich an, spezialisierte Teams mit genügend Distanz einzusetzen – analog zum Vorgehen der Polizei bei bestimmten Ereignissen.

In Bezug auf Polizeieinsätze sollte – gesetzlich oder gerichtlich – klargestellt werden, dass es grundsätzlich ein «Right to Record the Police» nach amerikanischem Vorbild gibt. Wer Einsätze nicht stört und weder sich noch andere gefährdet, muss filmen dürfen. Für das Veröffentlichen gelten die gängigen persönlichkeitsrechtlichen Massstäbe, das heisst, im Streitfall ist eine Interessenabwägung vorzunehmen. Betroffenen Personen sollte erleichtert werden, den Rechtsweg zu beschreiten. So würden einerseits die Rechte einzelner Personen wirksam geschützt und andererseits die Rechtspraxis durch differenzierte Rechtsprechung geschärft. Polizist(inn)en sollten selbstverständlich auf die Unterstützung ihrer Polizeikörpers zählen können, wenn sie sich zur Wehr setzen möchten.

Bei Erdmännchen und Hunden ...

... lässt sich gut beobachten, wie es aussieht, wenn man hochkonzentriert und wachsam ist, aber nichts versteht. Erdmännchen überblicken mit schnellen, zuckenden Richtungswechseln die gesamte Prärie, dann schlafen sie vor Erschöpfung ein und fallen um. Hunde bellen empört, wissen aber nicht, was gerade passiert ist: Denn es sah ja nur so aus, als sei das Stöckchen geworfen worden. Zu einer gelungenen Überwachung gehört mehr.

Dass einer wacht, während die anderen schlafen, ist wahrscheinlich eine stammesgeschichtliche Notwendigkeit und kann also grundsätzlich positiv gesehen werden. Hier wurzelt der Sicherheitsaspekt der Überwachung: Der Wächter wacht stellvertretend für die Schlafenden, er hat eine Schutzfunktion. Er muss Gefahren erkennen können, und er muss auch wissen, was zu tun ist, wenn Gefahr droht – zuallererst muss er die Schlafenden wecken. Bei dieser Art von schützender Wachsamkeit denkt man an den Nachtwächter, den Wachtmeister, an die gute, alte Polizeiwache. Wie auf einem Gemälde aus dem 19. Jahrhundert.

Das ist das «wach» in Überwachung. Das «über» in Überwachung könnte zwar theoretisch ein «zu viel» bezeichnen, wie bei «überschwemmen» oder «übertreiben», doch es meint wohl eher das Flächendeckende, das Totale des Gegenstands, wie bei «überblicken» oder «überwölben». Natürlich kann man das Überblicken auch übertreiben, und tatsächlich fragt man sich, ob es genug «Seltene Erden» gibt, um die derzeitige Praxis der Datenerhebung noch die nächsten Jahrzehnte durchzuhalten. Wobei Datenerhebung an sich noch keine Überwachung ist, sondern nur eins ihrer Instrumente. Überwachung beginnt dort, wo jemand z.B. anhand solcher Daten über einen anderen etwas Bestimmtes wissen will – mit dem Ziel (und der Macht!), ihn in irgendeiner Form zu sanktionieren, wenn er gefunden hat, was er gesucht hat.

Und das ist das Problem: Wenn Drogenfahnderteams Drogenhändlerteams überwachen, wünscht man ihnen die beste Technik und die versiertesten Sprachmittler/innen (S. 13 ff.), damit es keine Missverständnisse gibt und die Drogenhändler

gefasst und angeklagt werden können. Wenn hingegen in totalitären Staaten die Datenkrake dazu missbraucht wird, um Andersdenkende und politische Gegner/innen ausfindig machen, verhaften und foltern zu können, wünscht man sich vielleicht, dass die Technik nie so weit fortgeschritten wäre. Wohl noch jede technische Errungenschaft kann sinnvoll eingesetzt oder missbraucht werden.

Dabei ist noch ein anderer Aspekt von Bedeutung, nämlich ob die Überwachten *wissen*, dass sie überwacht werden, oder nicht. Im Strassenverkehr beispielsweise liefern sich Blitzanlagen und Blitzanlagen-Warnanlagen seit Jahren ein Kopf-an-Kopf-Rennen. Überwachte, die wissen, dass sie überwacht werden, könnten auch Strategien entwickeln, die Überwachenden irrezuführen oder sogar in eine Falle zu locken. Wie das geht, zeigen z.B. die Serien «The Wire» und «Narcos» eindrücklich, hier bezogen auf die Thematik des Drogenhandels. In der DDR haben regimiekritische Künstler und Künstlerinnen, die ebenfalls wussten, dass die Zensur ihre Texte kontrollieren würde, sogenannte «rosa Elefanten» eingebaut, also Inhalte, die so offensichtlich regimiekritisch waren (und deshalb auch immer der Zensur zum Opfer fielen), dass die viel subtilere Regimiekritik im nächsten Satz dann regelmässig von der Zensur übersehen wurde.

Wer eine Migros-Cumulus- oder eine Coop-Supercard besitzt, muss momentan noch keine Angst haben, dass aufgrund der letzten Einkäufe plötzlich die Polizei vor der Tür steht. Er/sie sollte sich trotzdem immer bewusst sein, dass sämtliche Einkaufsvorgänge auf unbestimmte Zeit nachgehalten werden. Wer dann immer nur «M-Budget»- und «Prix Garantie»-Produkte gekauft hat, könnte als Geizhals oder auch als arm gelten, und das könnte zum Problem werden, wenn die Schweiz eines Tages gezielt sowohl gegen den Geiz (übrigens eine Eigenschaft von Reichen) als auch gegen die Armut in der eigenen Bevölkerung vorgehen wollte. Was aber in der nächsten Zeit wohl nicht zu befürchten ist.

Volker Wienecke

Kontakt: redaktion@skppsc.ch

NEUES AUS DER SKP

Relaunch der Zivilcourage-Kampagne

2019 lancierte die SKP die Kampagne «Zivilcourage-Kompass». In kurzen Videos schilderten Korpsangehörige aus der ganzen Schweiz, wie man in verschiedensten Situationen zivilcourageig handeln kann und soll. Das Thema hat bis heute nichts an Aktualität eingebüsst. Die SKP hat sich daher entschieden, die Kampagne wieder auf-

zunehmen. Ab Anfang Juni bis Ende 2021 steht wöchentlich eines der Videos aus «Zivilcourage-Kompass» im Fokus. In den sozialen Medien werden nebst bestehenden Videos auch Umfragen zu den verschiedenen Verhaltensoptionen veröffentlicht. Begleitet wird der Relaunch von eigens neu geschaffenen Schwarz-weiss-Illustrationen.



DER REIM AUF CRIME



ZU VERKAUFEN:
3 alte, aber top
funktionierende
Überwachungskameras

Zeichnung: Agnes Weber



Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
Postfach
CH-3001 Bern

www.skppsc.ch

