Maschinen führen die Aufsicht

Offene Fragen der Kriminalprävention durch digitale Überwachungsagenten

Von Dr. **Alexander Baur**, M.A./B.Sc., Hamburg*

Die Digitalisierung stellt das Recht vor eine Vielzahl von Herausforderungen. Eine von ihnen betrifft den Einsatz digitaler Überwachungsagenten: An der Schnittstelle des öffentlichen Gefahrenabwehr- und Aufsichtsrechts zum Strafrecht entwickeln sich Instrumente, die ohne menschliches Zutun und teilweise selbstlernend nach interventionsbedürftigen Situationen und Verdachtsmomenten für Straftaten suchen. Die technische Entwicklung erreicht dabei zunehmend die Rechtspolitik und es setzt sich die Erkenntnis durch, dass eine digitalisierte Kriminalprävention neuen rechtlichen Regelungsbedarf entstehen lässt. Der Beitrag zeigt beispielhaft digitale Überwachungsagenten, ordnet sie kriminologisch ein und wirft mit ihnen einhergehende rechtliche Problematiken auf.

Digitization presents a variety of challenges for the law. One of them concerns the use of digital surveillance agents. In the context of police and regulatory law and at the threshold to criminal law new instruments are evolving. Automated and self-learning, they search for situations that warrant an intervention or constitute a crime. Law makers see the need to come up with the necessary legal framework to keep up with this technological development concerning crime prevention. This article introduces digital surveillance agents, classifies them in regard to criminological theory and discusses the resulting difficulties when creating a legal framework.

I. Elektronische Fußfesseln, smarte Videoüberwachung und digitale Geldwäschebekämpfung

Als der Europäische Gerichtshof für Menschenrechte im Dezember 2009 entschied, dass die langjährige Unterbringung von mehr als 80 Straftätern in der nachträglichen Sicherungsverwahrung menschenrechtswidrig ist und diese deswegen recht kurzfristig entlassen werden müssen,[1] löste das rechtspolitischen Handlungsdruck aus. Man mühte sich mit einiger dogmatischer Kreativität darum, diese Sicherungsverwahrten doch noch irgendwie freiheitsentziehend unterzubringen.[2] Diejenigen, die dafür nicht in Frage kamen, empfing nach ihrer Entlassung regelmäßig eine polizeirechtlich begründete „24/7-Überwachung“:[3] Mehrere Polizeibeamte im Schichtbetrieb begleiteten und beaufsichtigten den Entlassenen auf Schritt und Tritt. Nicht nur die Resozialisierungsförderlichkeit dieses Vorgehens war einigermaßen fragwürdig; es war vor allem auch nicht kostengünstig: Auf gut eine Million Euro pro Jahr summieren sich allein die Personalkosten für eine solche polizeiliche Dauerobservation.[4] Die Suche nach Alternativen führte zu einer technischen Lösung. Mit der in § 68b Abs. 1 S. 1 Nr. 12 StGB geregelten elektronischen Aufenthaltsüberwachung sollen entlassene Straftäter mit erheblichen Rückfallrisiken in Freiheit engmaschig, zuverlässig[5] und zugleich ressourcenschonend beaufsichtigt werden können. Gleichzeitig verspricht sich der Gesetzgeber von der „elektronischen Fußfessel“, dass verfassungsrechtlich problematische Stigmatisierungseffekte einer intensiven polizeilichen Beobachtung eingedämmt werden können.[6]

Der elektronischen Aufenthaltsüberwachung geht es vor allem um die Kontrolle ortsbezogener Kriminalitätsrisiken. So kann dem verurteilten Straftäter unter Strafdrohung (§ 145a StGB) das Aufsuchen solcher Orte verboten werden, die man aufgrund einer Tätereinschätzung für risikoreich hält (§ 68b Abs. 1 S. 1 Nr. 2 StGB). Nach gesetzlicher Konzeption läuft die elektronische Aufenthaltskontrolle dabei vollständig automatisiert ab. Das Überwachungssystem legt den aktuellen Aufenthaltsort des Straftäters nur bei der festgestellten Verletzung einer aufenthaltsbezogenen Weisung offen; § 463a Abs. 4 StPO untersagt ausdrücklich die dauerhafte (menschliche) Datenerhebung und Datenauswertung. Konkret bedeutet dies, dass in einem Geofencing Ge- und Verbotszonen definiert und dem System als Entscheidungsregel vorgegeben werden. Verlässt der entlassene Straftäter den vorgeschriebenen Aufenthaltsbereich, wird dies als Treffer erkannt, ein Alarm bei der Zentralen Überwachungsstelle der Länder[7] ausgelöst und der aktuelle Aufenthaltsort der überwachten Person freigegeben.

Die im Strafrecht geregelte elektronische Aufenthaltsüberwachung ist eines der prominenteren Beispiele für einen digitalen Überwachungsagenten. Sie ist aber längst kein singuläres Phänomen mehr. Digitale Überwachungsagenten werden zunehmend in der polizeilichen Gefahrenabwehr, in der Steuerverwaltung und für die staatliche Wirtschaftsaufsicht eingesetzt. Macht man sich auf die Suche, stößt man schon heute auf eine überraschende Vielzahl „digitaler Kontrolleure“: Im Bereich der Alltagskriminalität soll etwa die smarte Videoüberwachung automatisch Gefahrsituationen

* Der *Verfasser* ist Juniorprofessor für Strafrecht an der Universität Hamburg und dort Mitglied des Zentrums für Recht in der digitalen Transformation. Der Beitrag geht auf einen mehrfach gehaltenen Vortrag des *Verfassers* zurück.

[1] EGMR NJW 2010, 2495 (M. v. Deutschland).

[2] Vgl. dazu *Kinzig*, NJW 2011, 177 (181 f.).

[3] Siehe dazu VG Freiburg BeckRS 2013, 47247 = DÖV 2013, 569 (Ls.); sowie BVerfG KommJur 2013, 73. Vgl. dazu auch *Baur*, in Baur/Kinzig (Hrsg.), Die reformierte Führungsaufsicht, 2015, S. 234.

[4] Vgl. dazu VG Freiburg BeckRS 2013, 47247 = DÖV 2013, 569 (Ls.).

[5] Cum grano salis VG Freiburg BeckRS 2013, 47247 = DÖV 2013, 569 (Ls.): „Allerdings ist auch insoweit festzuhalten, dass der Kläger von Rechts wegen nicht gehalten ist, die Einsatzbereitschaft der Polizeibeamten abzuwarten oder sein Tempo gar an deren Fitnesszustand oder dem zur Verfügung stehenden Fahrradmaterial zu orientieren.“

[6] Siehe dazu BT-Drs. 17/3403, S. 19.

[7] Vgl. dazu Staatsvertrag über die Einrichtung einer Gemeinsamen elektronischen Überwachungsstelle der Länder vom 19. Mai/29. August 2011.

und Straftaten erkennen.[8] Gesetzlich ist dies unter anderem in § 21 Abs. 4 S. 1 PolG-BW als Standardmaßnahme vorgesehen und wird in Feldversuchen bereits getestet.[9] Beim sogenannten „Mannheimer Weg 2.0" sucht beispielsweise Software des Fraunhofer-Instituts in Echtzeitvideoaufnahmen nach auffälligen Verhaltensweisen. Ähnlich wie die elektronische Aufenthaltsüberwachung verwendet die Software dabei eine „kaskadierte Anonymisierung"[10]. Aufnahmen bleiben verpixelt und werden nur bei vom System erkannten Treffern automatisch scharfgestellt und dann auch zu Beweiszwecken gespeichert. Dabei soll die Trefferquote durch maschinelles Lernen über die Zeit verbessert werden. Stattet man die smarte Videoüberwachung mit einer Gesichtserkennungssoftware aus,[11] wird es denkbar, bestimmte Personen – etwa solche, die zur Aufenthaltsermittlung ausgeschrieben sind – systematisch zu entdecken. Auch Bewegungsbilder bestimmter Personen im öffentlichen Raum werden dann möglich.[12] Letzteres wird nicht nur jüngst im Zusammenhang mit dem Infektionsschutz diskutiert, sondern das Bundeskriminalamt wertet bereits heute vorliegende Aufenthaltsdaten zum Aufspüren krimineller und terroristischer Netzwerke aus.[13] Strukturell ganz ähnlich weicht im virtuellen Raum das mehr oder minder planlose „menschliche Durchklicken" des Internets nach möglichen Rechtsverstößen immer häufiger einem „digitalisierten Durchforsten" nach verdächtigen Inhalten.[14] Große Datenmengen werden dabei systematisch gesichtet und ausgewertet. Bei Auffälligkeiten schlägt auch hier das System automatisch Alarm.

Verlässt man die Alltagskriminalität und lenkt den Blick auf die Steuer-, Geldwäsche- und allgemein die Wirtschaftskriminalität, dann nimmt die Zahl digitaler Überwachungsagenten weiter zu. Mit Hilfe automationsgestützter Systeme beurteilt die Finanzverwaltung, ob in einem Fall weiterer Ermittlungs- und Prüfungsbedarf besteht (§ 88 Abs. 5 AO). Die Financial Intelligence Unit (FIU)[15] des deutschen Zolls nutzt „automatisierte Grundrecherchen"[16] auf der Grundlage des § 30 Abs. 2 GwG zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Begleitet wird dies durch die bei der OECD angesiedelte Financial Action Task Force on Money Laundering (FATF), die im November 2018 öffentlich eine internationale Digitalisierungsoffensive ausrief.[17] Das europäische Amt für Betrugsbekämpfung (OLAF) kündigte bereits 2011 eine noch tiefergehende Vernetzung der verfügbaren Datenbestände innerhalb der europäischen Mitgliedstaaten an – verbunden mit der Entwicklung digitaler Auswertungsstrategien.[18] Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und die Markttransparenzstelle überwachen Transaktionen an den Kapitalmärkten und der Energiebörse mittels mathematisch-statistischer Verfahren, die etwa auf strafbaren Insiderhandel hindeuten könnten.[19]

II. Kriminologische und kriminalpräventionsrechtliche Einordnung

1. Einsatz digitaler Überwachungsagenten in unterschiedlichen Präventionsparadigmen

Aus der Sicht einer effektiven Kriminalprävention haben digitale Überwachungsagenten eine beachtliche Schlagkraft. Setzt man sie ein, dann ist erstens eine Intervention oder strafrechtliche Reaktion nicht länger das Ergebnis mehr oder minder beliebiger Verhaltensstichproben oder einer bedingt verlässlichen Hinweisgabe durch Anzeigeerstatter. Zweitens werden auch solche Verhaltensweisen erkennbar, die aufgrund ihrer Komplexität und ihrer wenig sichtbaren Folgen kaum oder allenfalls mit der Hilfe involvierter Personen und anderer Mitwisser bekannt würden. Der Einsatz digitaler Agenten ersetzt damit Entdeckungs-, Aufklärungs- und Nachweiszufälligkeiten durch systematische Überwachungsprozesse.[20]

Eine automatisierte Überwachung wird in unterschiedlichen kriminalpräventiven Zusammenhängen genutzt.[21] Die vorwiegend gefahrenabwehr- und aufsichtsrechtlich gestaltete Verhinderungsprävention will drohende Rechtsgutsverletzungen durch gezielte Eingriffe von außen faktisch verhin-

[8] Vgl. dazu *Bäcker*, Kriminalpräventionsrecht, 2015, S. 417 ff.; siehe dazu auch *Roggan*, NVwZ 2019, 344 (346).
[9] Siehe u.a. *Schneider/Schindler*, ZD-Aktuell 2017, 05902.
[10] Vgl. dazu *Martini*, DÖV 2019, 732 (734); *Wendt*, ZD-Aktuell 2018, 06122.
[11] Vgl. dazu *Spiecker genannt Döhmann*, K&R 2014, 549 (550); *Hornung/Schindler*, ZD 2017, 203 (208); *Jandt*, ZRP 2018, 16; *Roggan*, NVwZ 2019, 344 (346). Zum Einsatz automatisierter Gesichtserkennung im Strafverfahren siehe *Wendt*, ZD-Aktuell 2018, 06364.
[12] Vgl. dazu *Roggan*, NVwZ 2019, 344 (346): Verhaltensanalysen.
[13] Vgl. zur Bedeutung von Bewegungsbildern für die Terrorismusbekämpfung BT-Drs. 18/11163, S. 128.
[14] Siehe dazu *Bäcker*, in: Hoffmann-Riem (Hrsg.), Big Data – Regulative Herausforderungen, 2018, S. 167 (171); vgl. dazu schon früh *Weßlau*, ZStW 113 (2001), 681 (704 ff.); vgl. dazu auch aus kriminologischer Sicht *Williams/Burnap/Sloan*, British Journal of Criminology 57 (2017), 320.
[15] Zur Gründung und Arbeitsweise der FIU vgl. eingehend *Barreto da Rosa*, in: Herzog, Geldwäschegesetz, Kommentar, 3. Aufl. 2018, Vorb. zu Abschn. 5 Rn. 1 ff.
[16] Jahresbericht FIU 2018, S. 12; vgl. dazu auch im Überblick *Barreto da Rosa* (Fn. 15), § 30 Rn 10 ff.
[17] Siehe dazu u.a. *Lewis*, Remarks at AI & Blockchain Summit, 21 November 2019, abrufbar unter http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-digital-id-nov-2019.html (20.5.2020).
[18] KOM (2011) 376 endg., S. 7.
[19] Vgl. dazu *Brosig*, Benchmark-Manipulation, 2018, S. 247; *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 4 (50, 55); zur Arbeit der US-amerikanischen SEC vgl. *Bauguess*, The Role of Big Data, Machine Learning, and AI in Assessing Risks: A Regulatory Perspective, 2017, abrufbar unter https://ssrn.com/abstract=3226514 (28.5.2020).
[20] Ähnlich *Spiecker genannt Döhmann*, K&R 2014, 549 (550): „die Zufälligkeit wird planvoll umgelenkt".
[21] Ähnlich *Spiecker genannt Döhmann*, K&R 2014, 549 (550).

dern und schon im Vorfeld einer Schadensverursachung unmöglich machen oder wenigstens schadensvertiefende Prozesse frühzeitig abbrechen.[22] Digitale Überwachungsagenten sollen dafür systematisch die Voraussetzungen schaffen, indem sie zuverlässig Informationen für aufsichtsrechtliches Eingreifen und gefahrenabwehrrechtliche Gegenwirkung bereitstellen. Ihre Aufgabe ist die Erzeugung notwendigen Interventionswissens. Sie werden eingesetzt, um verdichtete Gefahrenlagen frühzeitig zu erkennen und Ansatzpunkte für eine wirksame Intervention aufzuzeigen.[23] Ergibt beispielsweise die systematische Auswertung von Aufenthaltsdaten Hinweise auf eine bevorstehende Straftat, kann diese durch polizeiliches Einschreiten unterbunden werden.

Digitale Überwachungsagenten können aber auch zur Strafverfolgungsvorsorge verwendet und in Beziehung zu einer primär straf- und ordnungswidrigkeitenrechtlich verankerten Abschreckungsprävention gesetzt werden. In diesem Präventionsparadigma sollen verhaltensrelevante Entscheidungsprozesse und Motivationszusammenhänge durch die Androhung von Sanktionen gelenkt und dadurch die Auftretenswahrscheinlichkeit unerwünschter Verhaltensweisen von vornherein reduziert werden. Ein wirksamer Abschreckungsmechanismus setzt dabei nicht nur voraus, dass die für Fehlverhalten angedrohten Sanktionen spürbar sind, sondern fordert vor allem eine hohe Wahrscheinlichkeit, dass diese Sanktionen in der Praxis auch zur Anwendung gebracht werden können. Letzteres ist nur dann möglich, wenn einschlägige Verhaltensweisen entdeckt und Tatverantwortung zugeschrieben werden kann. Werden sämtliche sanktionierbaren Verhaltensweisen zuverlässig bekannt und sind sie sicher nachweisbar, so sollte dies zu einer maximalen Abschreckung und damit zu einer höchstmöglichen Normbefolgungsbereitschaft führen.[24] Digitale Überwachungsagenten im Abschreckungsparadigma setzen just an dieser Stelle an. Sie erhöhen die Wahrscheinlichkeit, dass sanktionierbares Verhalten entdeckt wird und legen zugleich den Grundstein für den Tatnachweis.

Die Zuordnung eines digitalen Überwachungsagenten zu einem der beiden Präventionsparadigmen ist nicht immer eindeutig und hängt vom jeweiligen Verwendungszusammenhang seiner Vorarbeiten ab.[25] Ergebnisse der smarten Videoüberwachung sind so zunächst einmal Anlass für konkrete gefahrenabwehrrechtliche Interventionen. Sie können aber auch in einen strafrechtlichen Kontext gerückt werden, indem ihre Verdachtsmeldung ein Ermittlungsverfahren in Gang setzt und dort mit ihren gespeicherten Informationen der Tatnachweis geführt wird. Teilweise sind digitale Überwachungsagenten sogar planvoll an der Pforte zum Strafrecht platziert und übernehmen dort die Rolle eines „Initiativermittlers". Sie erheben und verarbeiten tatverdachtsunabhängig relevante Informationen, um so die Voraussetzungen für strafprozessuale Ermittlungsmaßnahmen und strafrechtliche Sanktionen zu schaffen.[26] Besonders eindrücklich lässt sich dies in der Geldwäschebekämpfung beobachten. Dort werden Geldwäscheverdachtsmeldungen an die Strafverfolgungsbehörden weitergereicht (§ 32 Abs. 1 S. 1 GwG), wo sie den Ausgangspunkt strafrechtlicher Ermittlungen bilden – und zwar nicht nur bezüglich § 261 StGB, sondern auch und gerade im Hinblick auf die hinter der Geldwäsche stehenden Vortaten.[27] In dieser (Doppel-)Funktionalität unterscheidet sich die Arbeit digitaler Überwachungsagenten aber keineswegs von anderen Maßnahmen im Grenzbereich von Polizei- und Strafrecht.[28] Die problematische Legitimität gezielter „Tatverdachtsgenerierungen"[29] stellt sich gleichermaßen bei traditionellen Formen strafrechtsbezogener, operativer Vorfeld-, Struktur- und Initiativermittlungen.[30] Die Problematik wird durch den Einsatz digitaler Überwachungsagenten allenfalls ein gutes Stück verschärft, weil durch sie eine systemati-

[22] Vgl. dazu *Spiecker genannt Döhmann*, K&R 2014, 549 (550).

[23] Vgl. dazu u.a. *Mann/Fontana*, JA 2013, 734.

[24] Kriminologisch folgt dies unter anderem aus der Deterrence Theory, wonach eine hohe subjektiv wahrgenommene Sanktionsgewissheit kriminalitätsdämpfend wirkt; vgl. dazu im Überblick *Paternoster/Bachman*, in: Cullen/Wilcox (Hrsg.), The Oxford Handbook of Criminological Theory 2015, S. 649.

[25] Mit Blick auf die Videoüberwachung vgl. *Zöller*, NVwZ 2005, 1235 (1239).

[26] *Kölbel*, in: Knauer/Kudlich/Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 2, 2016, § 160 Rn. 13; *Zabel*, ZIS 2014, 340 (343).

[27] Vgl. dazu auch für den Bereich der Zoll- und Außenhandelskriminalität die entsprechenden Mechanismen in §§ 23a ff. ZFdG. Diese Verwischung lässt sich freilich auch andernorts beobachten und ist möglicherweise ein neuer Grundmechanismus strafrechtlicher Prävention.

[28] Vgl. dazu jüngst BVerfG NVwZ 2019, 381 (386); siehe dazu auch *Roggan*, NVwZ 2019, 344 (347 f.); *Hornung/ Schindler*, ZD 2017, 203. Siehe dazu auch aus kriminologischer Sicht *Chan/Bennett Moses*, British Journal of Criminology 57 (2017), 299 (305 f. und 315).

[29] Ähnlich *Gless*, in: Herzog/Schlothauer/Wohlers (Hrsg.), Rechtsstaatlicher Strafprozess und Bürgerrechte, Gedächtnisschrift für Edda Weßlau, 2016, S. 165 (166); zu Recht wird darin verbreitet eine dritte Form polizeilicher Tätigkeit gesehen, vgl. u.a. *Wohlers*, GA 2014, 676 (680). Vgl. dazu auch VGH Baden-Württemberg, NVwZ-RR 2015, 26 (28).

[30] Siehe dazu grundlegend *Keller/Griesbaum*, NStZ 1990, 416 (417 ff.); *Weßlau*, ZStW 113 (2001), 681 (704 ff.); *Zabel*, ZIS 2014, 340 (343 f.); *Wohlers*, GA 2014, 467 (678); vgl. auch *Kölbel* (Fn. 26), § 160 Rn. 13 ff.; aus steuerstrafrechtlicher Sicht vgl. *Pflaum*, in: Knauer/Kudlich/Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 3-2, 2018, AO § 397 Rn. 6; zur problematischen Grenzziehung bei operativen Fallanalysen in der Geldwäschebekämpfung siehe *Barreto da Rosa* (Fn. 15), § 30 Rn. 14. Jedenfalls eine anlasslose Ermittlung „ins Blaue hinein" („fishing expeditions") soll unzulässig sein, vgl. zuletzt BverfG NVwZ 2019, 381 (388); für das Schweizer Recht vgl. *Gless* (Fn. 29), S. 177; siehe dazu auch *Hornung/ Schindler*, ZD 2017, 203 (208). Zur strafprozessualen „Tatverdachtsschwelle" siehe BVerfG NJW 2014, 3085; BVerfG NJW 2018, 3571; *Hoven*, NStZ 2014, 361.

sche Suche nach Tatverdacht ohne Ressourcenbegrenzung und mit hoher Verarbeitungstiefe möglich wird.[31]

2. Arbeitsstrategien digitaler Überwachungsagenten

Für ihre Präventionsarbeit folgen digitale Überwachungsagenten zwei unterschiedlichen Arbeitsstrategien. In der Signalentdeckungsstrategie[32] sollen sie einzelne relevante Verhaltensweisen zuverlässig erkennen. Sie haben das Ziel, unter minimalem Ressourceneinsatz[33] die Wahrscheinlichkeit zu maximieren, dass möglichst alle „Treffer" entdeckt werden. Flächendeckende Aufsicht und lückenlose Kontrolle werden machbar, weil die dafür notwendige Anzahl menschlicher Akteure auf ein Mindestmaß gesenkt wird. So ersetzt die elektronische Aufenthaltsüberwachung nach § 68b Abs. 1 S. 1 Nr. 12 StGB rund ein Dutzend Polizeibeamte bei der „Datenerhebung" vor Ort und reduziert obendrein durch die automatisierte Treffererkennung die Mitarbeiterzahl, die man für eine fortlaufende Echtzeitauswertung des Geofencing bräuchte. Eine Folge dieser Ressourcenersparnis ist es, dass nicht länger limitierte Überwachungskapazitäten auf bestimmte Sachverhalte hin fokussiert werden müssen. Es kann systematisch und nicht mehr nur stichprobenhaft nach bestimmten Verhaltensweisen gesucht werden.

Die Komplexität der Entscheidungsregeln, denen die digitalen Agenten bei der Signalentdeckung folgen, ist mäßig. Bei der elektronischen Aufenthaltsüberwachung führt die Verletzung einer klar definierten Regel – der verbotene Aufenthalt an einem bestimmten Ort – zu einem Treffer. Etwas komplexer sind die Entscheidungsregeln der smarten Videoüberwachung, weil die zu entdeckenden Verhaltensweisen weniger klar zu bestimmen sind. Als Treffer ist definiert, was Interventionsbedarf im öffentlichen Raum entstehen lässt.[34] Im Feldversuch „Mannheimer Weg 2.0" sondiert der digitale Überwachungsagent dementsprechend visuelle Inhalte auch auf neutrale Verhaltensweisen hin wie Rennen, Treten, Schlagen oder Auf-dem-Boden-Liegen.[35]

Auch in der Mustererkennungsstrategie geht es um eine drastische Erhöhung der auswertbaren Datenmengen. Anders als in der Signalentdeckungsstrategie sollen jedoch nicht einfache Treffer systematisch entdeckt werden. Vielmehr ist digitalen Agenten eine qualitativ andere und anspruchsvollere Aufgabe übertragen. Ihr Ziel ist es, in unübersichtlichen Datenmengen und in einer Vielzahl für sich genommen aussageloser Datenfragmente relevante Muster ausfindig zu machen. Unter einem rechtlichen Blickwinkel erinnert das an eine Rasterfahndung;[36] kognitionstheoretisch geht es um eine gestalttheoretische Herausforderung:[37] Im Rauschen unverdächtiger Alltagshandlungen soll ein bedeutungsvoller Zusammenhang erkannt werden. Die Mustererkennungsstrategie kommt deswegen dort zum Einsatz, wo bestimmte Verhaltensweisen außerordentlich schwer zu erkennen sind, weil sie durch die Verknüpfung unverdächtiger Teilhandlungen verschleiert werden. So sind etwa Steuerhinterziehungs-, Korruptions- und Geldwäschenetzwerke selten auf einen Blick zu erkennen und meist nur über einzelne „red flags" aufzuspüren.[38] Aber auch im Bereich der Alltagskriminalität können komplexe Mustererkennungen präventiv wirkungsmächtig sein. Beschränkt man etwa die Verarbeitung von Aufenthaltsdaten nicht auf die Entdeckung klar definierter Regelverstöße, sondern wertet diese systematisch aus, lassen sich kriminalpräventiv aufschlussreiche Bewegungsbilder zeichnen.

Die Entscheidungsregeln, denen digitale Überwachungsagenten bei der Mustererkennung folgen, sind naturgemäß von hoher Komplexität und müssen dynamisch sein. Ihre Effektivität hängt zudem entscheidend davon ab, dass nicht offengelegt wird, welche einzelnen Verhaltenskomponenten musterrelevant sind. Denn wären die Entscheidungsregeln transparent, könnten sie leicht umgangen werden, indem eine einzelne Handlung gezielt durch eine andere, funktional äquivalente ersetzt wird.

3. Steigerung des Überwachungsdrucks durch Digitalisierung?

Die Frage, wie sich digitale Überwachungsagenten auf den Überwachungsdruck und die Eingriffsintensität auswirken, scheint sich klar beantworten zu lassen: Durch sie wird das Netz kriminalpräventiver Sozialkontrolle systematisch enger geflochten. Am gedanklichen Endpunkt steht die Vorstellung, dass sämtliche zur Verfügung stehenden Daten systematisch erhoben und nach auffälligen Signalen oder verdächtigen Mustern durchsucht werden. Das lässt den Überwachungsdruck in Breite und Tiefe wachsen.[39] Was aus kriminalpräventiver Sicht durchaus erwünscht ist, schafft aber zweifellos verfassungsrechtlich Problematiken. Denn das Wissen um eine engmaschige und systematische Überwachung hat nicht nur intendierte Auswirkungen auf unerwünschte Verhaltensweisen, sondern kann – insbesondere, wenn sie von Verdachtslosigkeit und großer Streubreite gekennzeichnet ist –

[31] So schon die Unkenrufe bei *Weßlau*, ZStW 113 (2001), 681 (704). Zum Grundsatzproblem wird der Einsatz digitaler Agenten für die Tatverdachtsgenerierung aber nur, wenn man einen „von einem Menschen konkret gehegte[n] Tatverdacht" für strafprozessrechtliches Vorgehen voraussetzt; vgl. dazu *Gless* (Fn. 29), S. 174.

[32] Vgl. dazu grundlegend *Green/Swets*, Signal Detection Theory and Psychophysics, 1966.

[33] Zur smarten Videoüberwachung vgl. LT-Drs. BW 16/2741, S. 22.

[34] Vgl. *Roggan*, NVwZ 2019, 344 (346).

[35] Siehe dazu *Martini*, DÖV 2019, 732 (734); *Wendt*, ZD-Aktuell 2018, 06122.

[36] Ebenso *Gless* (Fn. 29), S. 170. Vgl. dazu bereits *Simon/Taeger*, JZ 1982, 140.

[37] Vgl. dazu grundlegend *Wertheimer*, Zeitschrift für Psychologie und ihre Grenzwissenschaften 4 (1923), 301.

[38] Für die Geldwäschebekämpfung vgl. *Pieth*, European Journal of Law Reform 365 (2002), 365 (371).

[39] So bereits früh zur kriminalpolizeilichen und „elektronisch" arbeitenden Rasterfahndung *Simon/Taeger*, JZ 1982, 140. Vgl. dazu auch jüngst BVerfG NVwZ 2019, 381 (382 f.).

auch die legitime Grundrechtsausübung über die Maße beeinträchtigen.[40]

Richtigerweise darf an dieser Stelle aber nicht pauschalisiert werden. Vielmehr braucht es eine differenzierte Betrachtung der Arbeitsweise digitaler Überwachungsagenten und der kriminalpräventiven Wirkungszusammenhänge, in denen sie eingesetzt werden.[41] Erst eine solche Einordnung erlaubt es, die Eingriffsintensität digitaler Überwachungsmaßnahmen mit denen menschlicher Überwachungsmaßnahmen sinnvoll zu vergleichen. Es zeigt sich dann, dass der Ersatz menschlicher Kontrolleure durch digitale Überwachungsagenten die Eingriffsintensität nicht zwangsläufig erhöhen muss, sondern auch unverändert lassen oder im Einzelfall sogar senken kann. Dementsprechend lassen sich drei Kategorien bilden, deren Eingriffsintensität jeweils anders einzuschätzen ist: Zu unterscheiden sind digitale Kontrollagenten, digitale Aufsichtsagenten und digitale Mustererkennungsagenten.

III. Kategorien digitaler Überwachungsagenten

1. Digitale Kontrollagenten

Digitale Überwachungsagenten der ersten Kategorie dienen primär der Abschreckungsprävention. Sie werden eingesetzt, um begrenzte Verhaltensbereiche auf bestimmte Signale hin zu kontrollieren und folgen der Signalentdeckungsstrategie. Dabei sind sie auf einzelne Personen oder Orte fixiert und ihr Einsatz wird gezielt bekannt gemacht. Die Entscheidungsregeln, denen solche Kontrollagenten folgen, sind meist denkbar simpel, statisch und leicht nachvollziehbar. Sie sind entweder bekannt oder werden transparent nach außen kommuniziert; bisweilen sind die Entscheidungsregeln auch gesetzlich vorgegeben. Die Regeln stehen dabei in einem direkten Zusammenhang mit demjenigen Verhalten, dessen Auftretenswahrscheinlichkeit minimiert werden soll. Ein erkannter Treffer ist stets ein Verstoß, der mit Hilfe des Kontrollagenten eindeutig belegt werden kann. Der wesentliche Präventionsmechanismus dieser digitalen Überwachungsagenten ist es damit, durch eine präzise Intensivierung des Überwachungsdrucks das wahrgenommene Entdeckungsrisiko für unerwünschte Verhaltenskomponenten zu erhöhen und so dafür zu sorgen, dass diese von vornherein unterbleiben. Idealtypische Fälle sind die elektronische Aufenthaltsüberwachung des Strafrechts oder auch die jüngst diskutierte automatische Kennzeichenerfassung zur gezielten Identifikation von Verstößen gegen lokale Dieselfahrverbote.[42]

Die problematischen Nebenwirkungen dieser Spielart einer digitalisierten Überwachung sind überschaubar. Die Rechtfertigungsanforderungen für die Ersetzung menschlicher Kontrolleure durch digitale Agenten sind deswegen eher gering. Zwar mag die digitalisierte Verarbeitung die Häufigkeit und Breite von Überwachungseingriffen erhöhen, weil sie eine lückenlose Überwachung unter minimalem Ressourceneinsatz ermöglicht. Aber noch nicht einmal eine solche Ausweitung der Überwachung in die Breite muss unbedingt mit einer massiven Erhöhung des Überwachungsdrucks einhergehen. Die Alternative zu einer systematischen Überwachung besteht nämlich darin, stichprobenhaft nach unerwünschten Verhaltensweisen zu suchen. Sollen gezogene Verhaltensstichproben valide sein und abschreckend wirken, müssen sie aber im Gegensatz zu einer systematischen Überwachung heimlich und unangekündigt durchgeführt werden. Dass heimliche Verhaltensstichproben zwangsläufig weniger Überwachungsdruck verursachen, scheint zumindest nicht ganz eindeutig zu sein.[43]

Der Überwachungsdruck wird zudem weiter gesenkt, indem die digitale Datenauswertung dafür sorgt, dass überhaupt nur solche Verhaltensweisen bekannt werden, die zuvor festgelegte und bekanntgemachte Regeln verletzten.[44] Alle anderen Verhaltensweisen werden vom digitalen Überwachungsagenten zwar geprüft, aber als nicht einschlägig sofort verworfen und in der Folge ignoriert. Sie bleiben unbeachtet und können keine Folgeentscheidungen auslösen.[45] Dadurch entsteht die Sicherheit für den Überwachten, dass alle Verhaltensweisen ohne Zusammenhang zur kontrollierten Regel nicht bekannt werden. Dies reduziert den Überwachungsdruck im Vergleich zum Einsatz menschlicher Kontrolleure. Denn der Überwachte, der um die Überwachung weiß und die nachvollziehbaren Entscheidungsregeln des digitalen Agenten kennt, hat es selbst in der Hand, ob er dessen Aufmerksamkeit erregt: Was unverdächtig ist, bleibt systematisch im Dunkeln; bekannt wird nur, was auch Anlass zum Bekanntwerden bietet. Wer nicht ein Recht gegen die systematische Aufdeckung und für eine Chance auf Nichtentdeckung einer Straftat konstruieren möchte, kann gegen den offengelegten Eingriff durch Überwachungsagenten dieser ersten Kategorie an sich wenig einwenden.[46]

---

[40] Vgl. dazu u.a. BVerfG NJW 2006, 1939 (1944), mit zahlreichen weiteren Nachweisen. Siehe auch *Spiecker genannt Döhmann*, K&R 2014, 549 (550).

[41] Für eine Differenzierung nach Komplexität auch *Hoffmann-Riem*, AöR 142 (2017), 1 (30).

[42] Siehe dazu *Kipker*, MMR-Aktuell 2019, 414287; vgl. dazu auch BVerfG NVwZ 2019, 381; *Roggan*, NVwZ 2019, 344; *Mann/Fontana*, JA 2013, 734 (737).

[43] Mit Blick auf die elektronische Aufenthaltsüberwachung nach § 56 BKAG vgl. BT-Drs. 18/11163, S. 122; zustimmend *Ruthig*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Aufl. 2019, BKAG § 56 Rn. 1.

[44] Vgl. dazu *Ruthig* (Fn. 43), BKAG § 56 Rn. 10.

[45] Vgl. dazu auch *Spiecker genannt Döhmann*, K&R 2014, 549 (555).

[46] Nach verfassungsrechtlicher Einordnung soll jedoch auch eine Kontrolle, die zu einem Nichttreffer führt und deren Daten nach kürzester Zeit gelöscht werden, bereits ein Eingriff in die informationelle Selbstbestimmung sein, vgl. BVerfG NVwZ 2019, 381 (383 f.); siehe dazu auch *Schnieders*, NVwZ 2019, 396 f. Zu einem anderen Ergebnis kommt man auch, wenn man nur die Entdeckung von Straftaten durch menschliche und in ihrer Leistung beschränkte Kontrolleure als grundsätzlich legitim empfinden möchte; vgl. dazu auch *Spiecker genannt Döhmann*, K&R 2014, 549 (551).

2. Digitale Aufsichtsagenten

Digitale Überwachungsagenten der zweiten Kategorie suchen allgemein nach interventionswürdigem und sanktionierbarem Verhalten. Ihr Einsatz wird in aller Regel ebenfalls offengelegt. Von den Kontrollagenten unterscheiden sich Aufsichtsagenten aber unter anderem dadurch, dass ihre Entscheidungsregeln weniger transparent, komplexer und nicht selten dynamisch sind. Zwar geht es auch ihnen vor allem um die systematische Entdeckung bestimmter Signale. Diese sind allerdings weniger eindeutig definiert. Sie markieren daher den Übergang von der Signalentdeckung zur Mustererkennung. Dies bedeutet auch, dass nicht jeder vom Aufsichtsagenten berichtete Treffer zwangsläufig ein tatsächlich interventionsbedürftiges oder sanktionswürdiges Verhalten ist. Überwachungsergebnisse sind auch deswegen stärker fehlerbehaftet, weil Aufsichtsagenten primär darauf gerichtet sind, potentielle Gefahren und Verdachtsmomente zu erkennen und nicht klar definiertes Fehlverhalten zu berichten. Beispiele für digitale Agenten der zweiten Kategorie sind die smarte Videoüberwachung oder auch digitale Instrumente zur systematischen Kontrolle von Internetinhalten.

Digitale Aufsichtsagenten werden in Interventions- und Abschreckungszusammenhängen gleichermaßen eingesetzt. Sie beaufsichtigen bislang nur eher eng umgrenzte und kriminalpräventiv besonders relevante Räume. Um unerwünschte Verdrängungseffekte zu vermeiden, liegt es aus rein kriminalpräventiver Sicht aber nahe, ihre Aufsichtsbereiche nach Möglichkeit flexibel auszudehnen.[47] Der Einsatz dieser Art digitaler Agenten senkt im Vergleich mit einer menschlichen Überwachung den entstehenden Überwachungsdruck nicht zwangsläufig.[48] Zwar ist auch hier in gewisser Weise eine Regulierung durch ein automatisches „Aus- und Wegblenden" möglich, wodurch Eingriffe jedenfalls selektiver werden[49] und ihre Streubreite reduziert werden kann.[50] Da die Entscheidungsregeln von Aufsichtsagenten aber weniger simpel und transparent sind,[51] kann von den Überwachten nicht länger präzise abgesehen werden, wann sie die Voraussetzungen eines Treffers erfüllen. Anders als bei der einfachen Mechanik der Kontrollagenten ist nicht mehr sicher zu sagen, unter genau welchen Bedingungen digitale Aufmerksamkeit erregt wird. Da der Überwachungsdruck nicht länger auf ein klar bestimmtes Zielverhalten gerichtet ist, wirkt er diffuser und die Steuerbarkeit des digitalen Agenten durch das Verhalten des Überwachten ist vermindert.

3. Digitale Mustererkennungsagenten

Die Aufgabe digitaler Überwachungsagenten der dritten Kategorie ist es, in einer Vielzahl von Handlungsfragmenten auffällige Handlungsmuster zu erkennen.[52] In ihren Arbeitsabläufen folgen sie der Mustererkennungsstrategie. Beispiele für Mustererkennungsagenten sind operative Fallanalysen in der Geldwäschebekämpfung oder die automatisierte Erstellung von Bewegungsbildern.

Auch wenn die von Mustererkennungsagenten produzierten Ergebnisse in Sanktionszusammenhängen verwendet werden können, dienen sie doch primär der Interventionsprävention.[53] Ihr Einsatz wird nicht zu Abschreckungszwecken offengelegt, sondern sie werden heimlich verwendet. Die Entscheidungsregeln, denen sie folgen, bleiben – zur Wahrung ihrer Effektivität – ebenfalls im Verborgenen; sie sind hochkomplex und meist auch dynamisch. Die Opazität digitaler Mustererkennungsagenten ist dementsprechend hoch und der entstehende Überwachungsdruck streut breit.[54] Denn unter welchen Bedingungen ein Verhaltensfragment zum relevanten Teil eines gesuchten Verhaltensmusters wird, soll für den Überwachten gar nicht absehbar sein.[55] Um eine Verhaltenssteuerung durch gezielten Überwachungsdruck geht es Mustererkennungsagenten in aller Regel nicht oder wenigstens nicht primär.

Im Vergleich zu einer menschlichen Überwachung steigert die Digitalisierung hier den Überwachungsdruck:[56] Zunächst einmal ist die Überwachung heimlich und ihre Entscheidungsregeln sind nicht transparent. Sie sind von einer Komplexität, die selbst bei Offenlegung kaum durchschaubar wäre. Der entstehende Überwachungsdruck[57] wird dabei

[47] Im Zusammenhang mit dem Mannheimer Weg 2.0 wird beispielsweise der Einsatz von Drohnen diskutiert, siehe dazu *Martini*, DÖV 2019, 732 (734); vgl. dazu auch *Büllesfeld*, Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze zur Kriminalitätsvorsorge, 2002, S. 50 ff.; *Spiecker genannt Döhmann*, K&R 2014, 549 (550); *Zöller*, NVwZ 2005, 1235 (1239).

[48] So aber *Spiecker genannt Döhmann*, K&R 2014, 549. Vgl. dazu auch VG Hannover, Urt. v. 9.6.2016 – 10 A 4629/11; krit. insoweit *Schneider/Schindler*, ZD-Aktuell 2017, 05902.

[49] *Spiecker genannt Döhmann*, K&R 2014, 549 (551).

[50] *Spiecker genannt Döhmann*, K&R 2014, 549 (552).

[51] So auch *Hornung/Schindler*, ZD 2017, 203 (206).

[52] Zu dieser Kategorie digitaler Überwachungsagenten vgl. auch *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 4 (50, 60); mit Blick auf die Betrugsprävention *Schulz*, in: Gola (Hrsg.), Datenschutz-Grundverordnung, Kommentar, 2. Aufl. 2018, DS-GVO Art. 6 Rn. 257. Zu ihrer wachsenden Verbreitung vgl. *Bäcker* (Fn. 14), S. 169; siehe dazu auch aus kriminologischer Sicht *Chan/Bennett Moses*, British Journal of Criminology 57 (2017), 299 (310).

[53] Dies dürfte wenigstens rechtstatsächlich auch für die Geldwäschebekämpfung gelten. Dort führt das digitale Überwachungsergebnis zwar geradewegs ins Strafrecht, wird aber vor allem auch zur weiteren Aufklärung und Kriminalprävention mithilfe strafprozessualer Ermittlungsbefugnisse genutzt.

[54] In diese Richtung auch *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 4 (50, 55); vgl. zum gesteigerten Überwachungsdruck durch heimliche Maßnahmen auch BVerfG NVwZ 2019, 381 (389).

[55] Teilweise werden explizit Geheimhaltungspflichten formuliert (z.B. § 88 Abs. 5 S. 4 AO); vgl. dazu *Rätke*, in: Klein, Abgabenordnung einschließlich Steuerstrafrecht, Kommentar, 14. Aufl. 2018, AO § 88 Rn. 104 f.

[56] Einschränkend *Spiecker genannt Döhmann*, K&R 2014, 549, weil die Auswertung großer Datenmengen es ermöglichen könne, zunächst auf die Auswertung personenbezogener Daten zu verzichten.

[57] Vgl. dazu auch BVerfG NVwZ 2019 381 (383).

nicht bewusst aufgebaut und gezielt zur Abschreckung und Vermeidung bestimmter Verhaltensweisen eingesetzt, sondern ist eine Nebenfolge bei der Generierung von Interventionswissen. Zudem wird durch den Einsatz digitaler Überwachungsagenten der dritten Kategorie eine Tiefe und eine Qualität in der Mustererkennung erreicht, die bei einer traditionellen Verarbeitung kaum möglich wären; die Analysefähigkeiten gehen über die menschlicher Auswerter bei Weitem hinaus.[58] Nicht zuletzt geben Mustererkennungsagenten nur Hinweise auf potentielle Gefahren und möglichen Tatverdacht. Sie ähneln darin Aufsichtsagenten, liefern aber häufig noch weniger eindeutige Informationen und nur vage Ansatzpunkte für weitere Aufklärungsmaßnahmen.

IV. Vorgaben für die Entstehung und Verwertung digitaler Überwachungsergebnisse

1. Rechtlicher Regelungsbedarf für digitale Überwachungsagenten

Neben der umfangreich behandelten verfassungsrechtlichen Eingriffsdogmatik und den grundlegenden Rechtfertigungsbedingungen[59] ist die Frage nach der Arbeitsweise und den qualitativen Standards digitaler Überwachungsagenten von zentraler Bedeutung. Denn unabhängig davon, welcher Kategorie ein digitaler Überwachungsagent zuzurechnen ist, welcher Arbeitsstrategie er folgt und unter welchem Präventionsparadigma er eingesetzt wird, muss er bestimmten qualitativen Mindestanforderungen genügen. Nur der Einsatz hinreichend zuverlässiger digitaler Überwachungsagenten ist zu rechtfertigen. Digitale Agenten mit hoher Fehleranfälligkeit sind entweder schon gar nicht geeignet oder erhöhen zumindest massiv die Streubreite fehlgehender Überwachungseingriffe. Bereits daraus entsteht eine Regelungsbedürftigkeit, die sich weiter verdichtet, je umfassender digitalen Agenten die Suche nach rechtlich bedeutsamen Auffälligkeiten überantwortet wird. Dann bestimmen sie nämlich über die Präventions- und Sanktionierungspraxis zunehmend mit und bewegen sich damit in einem genuin rechtlich geprägten Entscheidungsbereich. Sie definieren zwar nicht verbindlich, was erlaubt ist und was nicht; sie entscheiden aber faktisch darüber, indem sie möglicherweise systematisch Überwachungskorridore potentiell interventions- und sanktionswürdigen Verhaltens schaffen.[60]

Die notwendige rechtliche Regulierung hält mit den technischen Entwicklungen bislang kaum Schritt.[61] Nur vereinzelt gibt es überhaupt gesetzliche Vorgaben, die sich dann darauf beschränken, den Einsatz digitaler Überwachungsagenten ausdrücklich vorzusehen und für zulässig zu erklären. Eine Antwort auf die Frage, welchen qualitativen Standards digitale Überwachungsagenten genügen und wie ihre Arbeitsabläufe beschaffen sein müssen, ist bislang die Ausnahme. Wenn es dazu Regelungsansätze gibt, dann sind diese meist vage und wirken in der Auswahl ihrer Regelungsaspekte einigermaßen beliebig. So macht etwa § 6 Abs. 4 GwG rudimentäre Vorgaben zu einem „Aktualisierungsgebot" für die Ausgestaltung digitaler Datenverarbeitungssysteme privater Glücksspielbetreiber: Diese müssen Mechanismen umfassen, die zweifelhafte oder ungewöhnliche Transaktionen erkennen – und zwar unter einer fortlaufenden Zugrundelegung des jeweils „öffentlich verfügbaren oder im Unternehmen verfügbaren Erfahrungswissens über die Methoden der Geldwäsche". Ein Stück weiter geht das Steuerrecht in seinen Regulierungsbemühungen. Für das automatische Risikomanagementsystem des § 88 Abs. 5 AO werden in Satz 3 immerhin einzelne Vorgaben zur Arbeitsweise (Nr. 1: auch Zufallsauswahl nicht risikobehafteter Fälle) und für das Zusammenwirken mit menschlichen Prüfern (Nr. 2 und Nr. 3) geregelt sowie eine systematische Prüfung der Zielerfüllung vorgeschrieben (Nr. 4).[62]

Für die weitere rechtliche Regulierung ist schließlich zu bedenken, dass besonders ausgefeilte Aufsichts- und Mustererkennungsagenten schon heute häufig nicht von staatlichen Akteuren unterhalten werden, sondern ihr Einsatz privaten Dritten aufgegeben oder zumindest faktisch nahegelegt wird.[63] So führt man den Anstieg von Geldwäscheverdachtsmeldungen unter anderem auf eine fortschreitende Automatisierung bei den großen Kreditinstituten zurück.[64] Wenn ein

[58] *Bäcker* (Fn. 14), S. 171.

[59] Siehe zuletzt BVerfG NVwZ 2019, 381 (384) mit zahlreichen weiteren Nachweisen.

[60] Zur Filterfunktion der FIU in der Geldwäschebekämpfung krit. *Barreto da Rosa* (Fn. 15), Vorb. zu Abschnitt 5 Rn. 9 f.; vgl. dazu auch *Spiecker genannt Döhmann*, GRUR 2019, 341 (349); vgl. dazu auch *Hoffmann-Riem*, AöR 142 (2017), 1 (35).

[61] Sie rücken allerdings zusehends auf die Agenda der (internationalen) Rechtspolitik und sind Gegenstand einer Vielzahl (unverbindlicher) Richtlinien. Anfang des Jahres beschäftigte sich das European Parliament Committee on Civil Liberties, Justice and Home Affairs in einer Expertenanhörung mit den Potentialen und Gefahren einer digitalisierten Kriminalprävention (Hearing on Artificial Intelligence in Criminal Law, Sitzung v. 20.2.2020, vgl. dazu LIBE-OJ [2020] 2334). Bereits im letzten Jahr stellte die European Commission for the Efficiency of Justice ein „European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" und das United Nations Interregional Crime and Justice Research Institute stellte Überlegungen zu „Artificial Intelligence and Robotics for Law Enforcement" vor. Die kanadische Regierung verabschiedete ungefähr zur selben Zeit ausformulierte Leitlinien zum Automated Decision-Making, die sich an vielen Stellen auf eine digitalisierte Kriminalprävention erstrecken lassen.

[62] Vgl. dazu *Rätke* (Fn. 55), AO § 88 Rn. 98.

[63] Für die unternehmensinterne Korruptionsprävention vgl. auch *Bisges*, MMR 2009, XX; zur Bedeutung elektronischer Risikoanalysen für die Bekämpfung der die Terrorismusfinanzierung vgl. *Teichmann/Park*, NK 2018, 419 (426 f.); zum Einsatz in der Wirtschaftsprüfung vgl. *Töller/Herde*, WPg 2012, 598.

[64] Jahresbericht FIU 2018, S. 13; krit. zu dieser Erhöhung von Verdachtsmeldungen Privater bei der Geldwäschebekämpfung *Walther*, in: Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Handbuch, 5. Aufl. 2017, § 42 Rn. 501.

künftiger „Darknet-Paragraph“ (§ 126a StGB-E) die Zugänglichmachung von Leistungen zur Begehung von Straftaten pönalisiert,[65] werden die Plattformanbieter wohl ebenfalls auf digitale Überwachungsagenten setzen, um ihrer daraus resultierenden Überwachungspflicht[66] gerecht zu werden.[67] Diese Auslagerung der digitalen Überwachungsarbeit an Private mag aus Gründen ihrer Sachnähe durchaus kriminalpräventiven Vorteil versprechen. Gleichzeitig macht sie da, wo die Überwachungskomplexitäten und -dynamiken am größten sind, die Regulierung am schwierigsten.

2. Von der Regulierung des Inputs zur systematischen Prüfung des Outputs

Bislang wird die Arbeit digitaler Überwachungsagenten weitgehend über den Datenzugang reguliert. In einem inputbezogenen Ansatz wird datenschutzrechtlich gesteuert, auf welche Informationen digitale Überwachungsagenten zugreifen dürfen. Diese Strategie allein kann aber allenfalls bei einfach gehaltenen digitalen Überwachungsagenten genügen.[68] Nur Kontrollagenten mit ihren klar strukturierten Entscheidungsregeln sind gut über den Dateninput zu steuern.[69] Bei Aufsichts- und vor allem Mustererkennungsagenten versagt diese Art der Regulierung zusehends. Denn je vielschichtiger und autonomer die Entscheidungsregeln eines digitalen Überwachungsagenten sind, desto geringer ist die Bedeutung, die einer einzelnen Information noch zukommt.[70] Die Effektivität eines ausgefeilten Mustererkennungsagenten wird selten davon abhängen, ob ihm einzelne Daten vorenthalten werden oder nicht. Vielmehr ist davon auszugehen, dass er über die Zeit lernt, Datenlücken durch alternative Verarbeitungswege zu kompensieren. Für eine sinnvolle rechtliche Regulierung reicht ein inputbezogener Ansatz dann nicht mehr aus. Mit wachsender Komplexität und Dynamik digitaler Überwachungsagenten werden deshalb ganzheitliche Regelungsansätze erforderlich. Diese müssen zunächst den Überwachungszugriff steuern und begrenzen, sodann die Verarbeitungsprozesse regulieren und schließlich über eine Sichtung des Outputs die Umsetzung der aufgestellten Vorgaben systematisch prüfen.

Zunächst scheint es also ratsam, gezielt Räume zu bestimmen, in denen schon gar keine Informationen erhoben werden dürfen.[71] Erwägenswert ist es weiterhin, bestimmte erhobene Informationen von den Entscheidungsregeln auszunehmen und die Verarbeitung von Inhalten, die als illegitim eingeschätzt werden, zu verbieten.[72] So ließe sich in Entsprechung zur Diskussion um die Zulässigkeit des Racial Profiling[73] etwa an ein Verbot solcher Verarbeitungsstrategien denken, die auf die Herkunft und Abstammung abstellen. Wie gut sich ein solches Verarbeitungsverbot praktisch implementieren lässt, scheint jedoch einigermaßen zweifelhaft. Denn es ist – wie gesagt – zu vermuten, dass zumindest einige digitale Überwachungsagenten „verbotene“ Informationswege über die Zeit durch andere funktional äquivalente ersetzen und durch korrelativ vergleichbar aussagekräftige Faktoren kompensieren können. Erfolgversprechender und wichtiger dürfte es sein, eine Absicherung vorzuschreiben, die verhindert, dass digitale Überwachungsagenten über die Zeit in verzerrende Verstärker- und Selbstbestätigungszirkel geraten.[74] Es muss also sichergestellt werden, dass selbstlernende Überwachungsagenten über die Zeit nicht nur noch nach spezifischen Konstellationen Ausschau halten und anderes, ebenso relevantes Verhalten systematisch ignorieren. Soll dies verhindert werden braucht es Prüfungsroutinen, deren Aufgabe es ist, einem digitalen Labeling und einem schrittweisen Entfernen von gesetzlichen Vorgaben systematisch entgegenzuwirken.[75] Ein weiterer zunehmend bedeutsamer Regelungsgegenstand ist schließlich der erlaubte Aktivitäts-

[65] Vgl. dazu Referentenentwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 27.3.2019, S. 76 ff. (abrufbar unter https://kripoz.de/2019/04/04/referentenentwurf-eines-zweiten-gesetzes-zur-erhoehung-der-sicherheit-informationstechnischer-systeme-it-sicherheitsgesetz-2-0-it-sig-2-0/).

[66] So zutreffend *Kubiciel/Mennemann*, jurisPR-StrafR 8/2019, Anm. 1; *Oehmichen/Weißenberger*, KriPoZ 2019, 174 (177). Vgl. dazu auch *Spiecker genannt Döhmann*, GRUR 2019, 341 (349).

[67] Vgl. dazu *Weidemann*, FAZ v. 25.3.2020, S. 13, zur digitalen Überwachung von Internetinhalten durch Facebook („Maschinen führen Aufsicht“).

[68] Vgl. dazu *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 4 (50, 62). Siehe auch *Bäcker* (Fn. 14), S. 170; vgl. dazu auch *Hoffmann-Riem*, AöR 142 (2017), 1 (6 und 38).

[69] So nehmen etwa § 463a Abs. 4 S. 1 Hs. 2 und § 56 Abs. 2 S. 2 BKAG bestimmte Bereiche von der elektronischen Aufenthaltsüberwachung aus und untersagen hilfsweise die Nutzung von Daten, die innerhalb der Wohnung erhoben worden sind.

[70] Umgekehrt gibt es kaum noch ein „belangloses Datum“, vgl. BVerfGE 65, 1 (45); 120, 274 (344 ff.); BVerfG NVwZ 2019, 381 (383); ebenso *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 4 (50, 51); mit Blick auf das Strafprozessrecht *Gless* (Fn. 29), S. 167; *Weßlau*, ZStW 113 (2001), 681 (689).

[71] Vgl. dazu u.a. *Ruthig* (Fn. 43), BKAG § 56 Rn. 3; im Ergebnis ebenso *Spiecker genannt Döhmann*, K&R 2014, 549 (555).

[72] Vgl. *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 4, (50, 61); vgl. auch *Martini*, JZ 2017, 1017 (1019); *Schweitzer/Fetzer/Peitz*, Digitale Plattformen. Bausteine für einen künftigen Ordnungsrahmen, ZEW Discussion Paper No. 16-042, 2016, S. 12 f.

[73] Vgl. dazu *Liebscher*, NJW 2016, 2779; *Pettersson*, ZAR 2019, 301.

[74] Zur Gefahr von „feedback loops“ vgl. *Bennett Moses/Chan*, Policing and Society 28 (2018), 806 (810); zum „racial bias“ vgl. u.a. *Gless* (Fn. 29), S. 172; *Martini*, JZ 2017, 1017 (1018).

[75] Einen Schutz gegen „algorithmenbasierte Zuschreibungen“ fordern *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 4 (50, 55). Für den Einsatz von Kontrollalgorithmen *Martini*, JZ 2017, 1017 (1022); vgl. dazu auch aus strafprozessualer Sicht *Gless* (Fn. 29), S. 171.

grad eines digitalen Überwachungsagenten. Mit einer wachsenden technischen Verfeinerung wird die Frage zu beantworten sein, ob digitale Überwachungsagenten nur passiv beobachten oder auch selbst aktiv nach bestimmtem Verhalten suchen oder dieses gar provozieren dürfen. Die Problematik könnte sich schon in absehbarer Zeit bei der Bekämpfung des Cybergroomings (§ 176 Abs. 4 Nr. 3, Abs. 6 S. 2 StGB) stellen, wenn dort Socialbots und Dialogroboter[76] als tatprovozierende „Fallensteller" eingesetzt werden, indem sie Chat-Profile potentieller Opfer simulieren und kommunikativ bedienen.

Bei steigender Undurchsichtigkeit eines digitalen Überwachungsagenten wird es schwieriger, dessen Entscheidungsregeln unmittelbar zu regulieren und auf die Einhaltung rechtlicher Vorgaben hin zu prüfen.[77] Zwangsläufig muss daher bei den Arbeitsergebnissen der digitalen Überwachungsagenten angesetzt werden und die Treffsicherheit, Präzision und rechtliche Vertretbarkeit ihrer Überwachungsergebnisse in den Fokus rücken. Über die Ergebnisse lassen sich problematische Entscheidungsregeln nämlich zumindest in Teilen rekonstruieren. So kann der Output digitaler Überwachungsagenten systematisch nach auffälligen Mustern durchsucht und diese zum Anlass genommen werden, bestimmte Teilbereiche der Entscheidungsregeln näher in den Blick zu nehmen und gegebenenfalls zu korrigieren. Zumindest in einfach gelagerten Konstellationen kann auch eine zufallsbasierte Fallauswahl helfen, die händisch geprüft und zur Effektivitätseinschätzung des digitalen Überwachungsagenten mit dessen Ergebnis abgeglichen wird.[78] Denkbar sind daneben stichprobenhafte retrospektive Analysen getroffener Überwachungsentscheidungen. Einen vielversprechenden Weg könnten schließlich experimentell-prospektive Prüfungen weisen. Dafür werden fiktive Fallvignetten konstruiert und dem digitalen Überwachungsagenten systematisch zur Entscheidung vorgelegt. Alternativ werden die Sachverhalte tatsächlich getroffener Überwachungsentscheidungen systematisch um bestimmte Faktoren variiert. Letzteres kann im Sinne einer Selbstprüfungsroutine auch automatisiert erfolgen.

Für solche Output-Prüfungen braucht es Maßstäbe. Es müssen also Präzisions- und Zuverlässigkeitserwartungen formuliert und Grenzen einer mindesterforderlichen Sensitivität und Spezifität digitaler Überwachungsagenten – also Verteilungsquoten zwischen entdeckten Treffern (richtig-positiv und richtig-negativ) und Fehlalarmen[79] (falsch-positive und falsch-negativen) – normativ verbindlich gemacht werden.

3. Verwertungsregeln für Überwachungsergebnisse

Werden interventionsbedürftige und verdächtige Verhaltensweisen durch den Einsatz digitaler Überwachungsagenten systematisch entdeckt, hat dies Auswirkungen auf gefahrenabwehrrechtliche und strafrechtliche Folgeentscheidungen. So werden durch digitale Überwachungsagenten auch kleinere und bagatellhafte Interventionsanlässe und Rechtsverstöße regelhaft ins Netz gehen – also solche Verhaltensweisen, nach denen man sonst aus Ressourcengründen nicht suchte, die nicht angezeigt würden und die dementsprechend folgenlos blieben. Für das Gefahrenabwehrrecht bedeutet dies, dass es ermessensleitende Maßgaben braucht, wie begrenzte Interventionsressourcen mit unbegrenztem Interventionswissen umzugehen haben. Im Strafrecht gerät das Opportunitätsprinzip unter erhöhten Druck. Denn es fällt eine wichtige Ebene im Kriminalitätstrichter[80] weg, wenn digitale Überwachungsagenten systematisch das Dunkelfeld aufhellen. In der Folge wird eine Vielzahl von tatbestandsmäßigen, aber in der Sache nicht strafwürdigen Verhaltensweisen bekannt. Ein möglicher Lösungsweg für diese Problematik deutet sich im Steuerrecht an. Nach § 88 Abs. 5 S. 2 AO soll das dort vorgesehene automatisierte Risikomanagementsystem so austariert sein, dass es die Folgen für die Wirtschaftlichkeit der Verwaltung berücksichtigt und beispielsweise Bagatellfälle außen vor lässt.[81] Die Auswahl, welche Auffälligkeiten zu Interventions- und Sanktionszwecken offengelegt werden, wird so in Teilen ebenfalls dem digitalen Agenten überantwortet. Schlägt man diesen Weg ein, wächst freilich die Bedeutung qualitätssichernder Maßnahmen noch einmal signifikant.

Insbesondere für strafrechtliche Verwertungszusammenhänge stellt sich die Frage, unter welchen Voraussetzungen strafprozessuale Ermittlungsmaßnahmen und eine spätere Verurteilung auf die Ergebnisse digitaler Überwachungsagenten gestützt werden dürfen.[82] Denn es ist nicht zu unterschätzen, in welchem Umfang digitale Überwachungsagenten als Tatverdachtslieferanten den weiteren Gang eines Verfahrens prägen, indem sie bereits zu einem frühen Zeitpunkt wirkungsmächtige Sachverhaltshypothesen und Präjudize aufstellen.[83] Manches spricht hier dafür, auf digitale Überwachungsagenten die bestehenden Grundsätze des Sachverständigenbeweises zu übertragen. Es ist also zu fordern, dass die Vorarbeit digitaler Überwachungsagenten in eigener Verant-

[76] Zu den kommunikativen Möglichkeiten vgl. *Sieber*, Dialogroboter, 2019.

[77] Ebenso *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 4 (50, 61 f.); *Hoffmann-Riem*, AöR 142 (2017), 1 (3 und 29); *Martini*, JZ 2017, 1017 (1018 f.); *Spiecker genannt Döhmann*, GRUR 2019, 341 (349).

[78] So etwa nach § 88 Abs. 5 S. 3 Nr. 1 und 4 AO; vgl. dazu *Rätke* (Fn. 55), AO § 88 Rn. 98.

[79] Vgl. dazu *Bäcker* (Fn. 14), S. 171; *Schnieders*, NVwZ 2019, 396 (397).

[80] Vgl. dazu anstelle vieler *Eisenberg/Kölbel*, Kriminologie, 7. Aufl. 2017, § 26 Rn. 2.

[81] *Rätke* (Fn. 55), AO § 88 Rn. 95.

[82] Vgl. dazu auch *Bäcker* (Fn. 14), S. 170.

[83] Vgl. dazu *Hoffmann-Riem*, AöR 142 (2017), 1 (36). Ein ähnliches Problem zeichnet sich schon heute beim Umgang mit den Ergebnissen digitaler Aufklärungsagenten ab. Bei umfangreichen elektronischen Datenauswertungen lässt sich auch kaum noch absehen, ob diese ein vollständiges Sachverhaltsbild zeichnen; vgl. schon früh und grundlegend *Weßlau*, ZStW 113 (2001), 681 (706); *Momsen*, in: Beck/Meier/Momsen (Hrsg.), Cybercrime und Cyberinvestigations, 2015, S. 67 (75); mit Blick auf eine Belastung für das Schweigerecht des Beschuldigten *Gless* (Fn. 29), S. 178.

wortung gewürdigt und nach Kräften plausibilisiert wird.[84] Ein Ermittlungs- oder Tatrichter muss dafür erstens davon ausgehen dürfen, dass der digitale Überwachungsagent für einen konkreten Fall im Einklang mit rechtlichen Vorgaben und Qualitätsstandards gearbeitet hat und zweitens die Entstehung des Überwachungsergebnisses retrospektiv wenigstens in groben Zügen nachvollziehen können.[85] Dafür müssen die für den Einzelfall zur Anwendung gebrachten Entscheidungsregeln vom digitalen Überwachungsagenten – so gut es geht – dokumentiert, zugänglich und verständlich gemacht werden.[86]

V. Ausblick

Der Einsatz digitaler Überwachungsagenten hat das Potential, die Kriminalprävention grundlegend neu aufzustellen und zu verändern. Dafür spricht nicht nur ihre immense kriminalpräventive Schlagkraft, sondern auch ihre ökonomischen Gesetzmäßigkeiten. Ressourcengrenzen spielen für sie kaum eine Rolle – im Gegenteil: Je mehr Sachverhalte von einem Agenten digital überwacht werden, desto effizienter wird sein Einsatz. Ob bei der elektronischen Aufenthaltsüberwachung die Aufenthaltsdaten von 200 oder 2.000 verurteilten Straftätern digital ausgewertet werden oder eine smarte Videoüberwachung an einem oder an zehn Orten eingesetzt wird, macht bei den Kosten kaum noch einen merklichen Unterschied.[87] Digitale Überwachungsagenten sind daher unter ökonomischen Gesichtspunkten auf Wachstum und Verbreitung getrimmt. Der Flaschenhals ist dann nicht länger die Überwachung,[88] sondern die sich anschließende Intervention[89] und Sanktionierung.[90] Um auch hier für Entlastung zu sorgen, scheinen Interventions- und Sanktionierungsagenten eine nahliegende Lösung.[91] Erste Schritte sind bereits getan: Bestimmte Inhalte im Internet können automatisch blockiert werden,[92] indem aus einer „Red Flag“ ein „Stop“ wird. Und auch die Sanktionierung massenhafter Rechtsverstöße fordert schon heute kaum noch eine intensive Weiterbearbeitung: Entdeckt ein Kontrollagent den Verstoß gegen ein Dieselfahrverbot, ist es ein Leichtes, ihn im zweiten Schritt sogleich den Bußgeldbescheid an den Fahrzeughalter fertigen zu lassen.

Spätestens eine solche Verknüpfung digitaler Überwachung und digitaler Intervention rückt merklich von einer Kriminalprävention in ihrem klassischen Sinne ab. Letztere ist nämlich ursachenorientiert. Sie baut auf theoretischen und im besten Fall empirisch geprüften Entstehungsannahmen auf. Eine kriminologisch fundierte Kriminalprävention gibt deswegen immer auch Hinweise, wie einem erkannten Problem langfristig begegnet werden kann. Digitale Überwachungsagenten sind dazu nicht in der Lage. Sie nutzen keine Kausalannahmen für ihren kriminalpräventiven Beitrag, sondern bauen ihn auf unverstandene Korrelationen.[93] Aus der Perspektive einer verstehenden Kriminalprävention können digitale Überwachungsagenten deshalb nur ein kleines Spektrum kriminalpräventiver Möglichkeiten bedienen. Die Hebel, die sie ansetzen helfen, sind immer einfach und selten subtil: Verhinderung und Abschreckung.

[84] Vgl. dazu u.a. BGH NJW 1982, 2882; siehe auch *Ott*, in: Hannich (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl. 2019, StPO § 261 Rn. 87; vgl. dazu *Hoffmann-Riem*, AöR 142 (2017), 1 (36).

[85] Vgl. dazu grundlegend BGH NJW 1955, 1642 (1644): „Der verfahrensrechtliche Ausgangspunkt für die Beurteilung liegt darin, daß der Tatrichter zu einem eigenen Urt. auch in schwierigen Fachfragen verpflichtet ist. Er hat die Entsch. auch über diese Fragen selbst zu erarbeiten, ihre Begründung selbst zu durchdenken. Er darf sich dabei vom Sachverständigen nur helfen lassen.“

[86] Vgl. *Momsen* (Fn. 83), S. 91: Offenlegung von Filterkriterien. Siehe auch *Ernst*, JZ 2017, 1026 (1031); *Martini*, JZ 2017, 1017 (1020). Vgl. dazu ferner aus datenschutzrechtlicher Perspektive *Spiecker genannt Döhmann*, GRUR 2019, 341 (347); diesbezüglich skeptisch *Hoffmann-Riem*, AöR 142 (2017), 1 (32 f.).

[87] Zu den Fallzahlerwartungen vgl. *Baur* (Fn. 3), S. 318; zur Ausweitung des Anwendungsbereichs siehe *Baur*, KriPoZ 2017, 119.

[88] Ähnlich bereits *Weßlau*, ZStW 113 (2001), 681.

[89] Vgl. dazu *Spiecker genannt Döhmann*, K&R 2014, 549 (550); *Teichmann/Park*, NK 2018, 419.

[90] Siehe auch Jahresbericht FIU 2018, S. 13: „[…] das erhöhte Meldeaufkommen [stellt] eine große Herausforderung für die […] Strafverfolgungsbehörden dar.“

[91] Zu möglichen Bedenken bezüglich Art. 22 DSGVO vgl. u.a. *Martini*, JZ 2017, 1017 (1020 und 1022).

[92] Vgl. dazu *Hoffmann-Riem*, AöR 142 (2017), 1 (20 und 34 f.: „Rechtschutz durch Design“).

[93] Vgl. *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 4 (50, 57).