Sonderdruck aus:

Schriften zum Strafrecht

Band 297

Rechtsstaatlicher Strafprozess und Bürgerrechte

Gedächtnisschrift für Edda Weßlau

Herausgegeben von

Felix Herzog, Reinhold Schlothauer
und Wolfgang Wohlers

in Verbindung mit Jürgen Wolter

Duncker & Humblot · Berlin 2016

Inhaltsverzeichnis

I. Deutsches und europäisches Strafverfahrensrecht

Predictive policing und operative Verbrechensbekämpfung

Von *Sabine Gless*

I. Einleitung

„Zunächst einmal ist festzustellen, dass häufig, wenn von einem ‚neuen Präventionskonzept' gesprochen wird, damit tatsächlich nur ein anderer Begriff für das verwendet wird, was [...] operative Verbrechensbekämpfung [ist]."[1] Mit diesem Befund umschreibt Edda Weßlau ein Grundthema vieler ihrer Arbeiten: Die Gemengelage von Polizeiarbeit und Strafverfolgung und damit verbundene Folgefragen, wenn die beiden Bereiche mit ihren unterschiedlichen Zielsetzungen zusammen treffen. Bringen etwa Maßnahmen zur Gefahrenabwehr Informationen hervor, die auch für strafrechtliche Ermittlungen von Interesse sein könnten,[2] ist fraglich, ob Erkenntnisse aus präventiv-polizeilichem Kontext für die Strafverfolgung verwendet oder verwertet werden dürfen. Denn möglicherweise können Betroffene dadurch ihre Verfahrensrechte nicht wahrnehmen oder andere rechtsstaatliche Sicherungen greifen nicht. Diese Probleme stellen sich vor allem, wenn die Polizei mit neuer Technologie ausgestattet wird, die den Justizbehörden nicht zur Verfügung steht.

So wird derzeit in Deutschland versuchsweise *predictive policing* eingesetzt.[3] Hinter dem Begriff verbirgt sich der Einsatz von Computerprogrammen, die Datenpools auf der Grundlage von Wahrscheinlichkeitsmathematik nach Mustern und Strukturen durchsuchen, um das Risiko künftiger Straftatbegehung an bestimmten Orten oder in bestimmter Weise oder durch bestimmte Personen(-gruppen) zu prognostizieren.[4] Die Polizei will etwa durch einen Abgleich der Meldungen über Ein-

---

[1] *Weßlau*, Vorfeldermittlungen: Probleme der Legalisierung „vorbeugender Verbrechensbekämpfung" aus strafprozeßrechtlicher Sicht, Berlin 1989, S. 44.

[2] Dazu etwa: *Weßlau* (Fn. 1); SK-StPO/*Weßlau*, Vor § 474 Rn. 16 ff. *Weßlau*, in: Wolter/Schenke/Hilger/Ruthig/Zöller (Hrsg.), Alternativentwurf Europol und europäischer Datenschutz, Heidelberg 2008, 329.

[3] Das LAK Bayern hat die Software „Precobs" bereits getestet; das LAK Baden-Württemberg plant entsprechende Versuche; vgl. Antwort der Bundesregierung vom 7. 1. 2015 (BT-Drs. 18/3703) auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Christine Buchholz, weiterer Abgeordneter und der Fraktion Die Linke (BT-Drs. 18/3525); *Ritter*, Wie man weiß, wo eingebrochen wird, FAZ vom 15. 12. 2015.

[4] *Perry/McInnis/Price/Smith/Hollywood*, *predictive policing.* The Role of Crime Forecasting in Law Enforcement, Santa Monica 2013, p. xiv.

bruchdiebstähle mit Straßenverkehrs- und sog. Geo-Daten vorhersagen, wo und wie sich eine Einbruchsserie fortsetzen könnte. Das ist kein ganz neues Vorgehen, sondern wurde etwa als „Regionalanalysen" in einer Vorform bereits praktiziert[5] und hört sich zunächst ganz harmlos an. Es könnte jedoch der Schritt zu einer automatisierten Auswertung von Datenbergen (sog. Data Mining) im Polizeibetrieb sein, indem Computerprogramme alle möglicherweise aussagekräftigen Daten nach Mustern auswerten, weil man davon ausgeht, dass auch straftatgeneigte Personen gewohnten und erfolgserprobten Handlungsmustern folgen. Wenn man nur genug Daten analysiere, könne man Straftaten vorhersagen, bevor sie begangen würden – so die dahinter stehende Logik.[6]

Der polizeiliche Schritt in die digitale Revolution könnte dem eingangs zitierten Befund Edda Weßlaus neue Aktualität verleihen. Könnte *predictive policing* – das bereits als präventives Instrument umstritten ist – sogar von seiner präventiven Zielsetzung in eine Methode zur Verdachtsgewinnung umgebaut werden?[7] Oder bilden rechtsstaatliche Grenzen dagegen jedenfalls einen Schutzwall? Diese Fragen sind Gegenstand der folgenden Ausführungen. Sie machen einerseits das wenig fassbare Phänomen des *predictive policing* aus strafprozessualer Perspektive greifbar und untersuchen andererseits entlang einer von Edda Weßlaus Arbeiten vorgezeichneten Linie, ob tradierte Rechtsinstitute wie das Erfordernis eines Anfangsverdachts, das Eingreifen von Verwertungsverboten oder bestimmte Verfahrensrechte verhindern könnten, dass das polizeiliche Data Mining benutzt wird, um unabhängig von tatbezogenen Anknüpfungspunkten Tatverdacht zu generieren.

II. *Predictive policing* und Informationsgewinnung

Unter dem Begriff der operativen Verbrechensbekämpfung hat Edda Weßlau Methoden der Informationsgewinnung zusammengefasst, die weder auf die Aufklärung einer bestimmten, bereits begangenen Straftat noch auf die Abwehr einer konkreten Gefahr gerichtet sind".[8] Ihre Überlegungen bezogen sich vor allem auf die teilautomatisierte Informationserhebung, wie etwa Telefonüberwachung oder sog. Lauschangriffe. Sie hatte jedoch durchaus bereits die Frage der Zulässigkeit einer polizei-

[5] *Schwind/Ahlborn/Weiß*, Empirische Kriminalgeographie, Bestandsaufnahme und Weiterführung am Beispiel von Bochum („Kriminalitätsatlas Bochum"), BKA Forschungsserie Wiesbaden 1978; *Schwarzenegger/Schmohl/Thalmann/Vertone/Zanolini*, Kriminalität und kommunale Kriminalprävention in Zürich. Kriminologisches Institut der Universität Zürich 2009.

[6] Vgl. Antwort des Stadtrats Zürich auf die Anfrage des Gemeinderats Angst (GR Nr. 2014/278) im Stadtrat von Zürich vom 4.12.2014; Antwort der Bundesregierung auf eine Anfrage der Fraktion Die Linke, BT-Drs. 18/3703; *Biermann*, Die Zeit. 29.3.2015. Noch niemand hat bewiesen, dass Data Mining der Polizei hilft. http://www.zeit.de/di-gital/datenschutz/2015-03/predictive-policing-software-polizei-precobs.

[7] *Weßlau* (Fn. 1), S. 269 f.; SK-StPO/*Weßlau*, Vor § 474 Rn. 16.

[8] *Weßlau* (Fn. 1), S. 27.

lichen Generierung von Information durch Verknüpfung von Daten im Auge, wie sie beim *predictive policing* in einem Graubereich zwischen bloßer Datenvorratshaltung (Data Warehouse) und automatisierter Datenauswertung (Data Mining) praktiziert wird.[9]

Eine verbindliche Definition für die verschiedenen Instrumente des *predictive policing* fehlt bisher ebenso wie Transparenz über Daten und Programmierung. Klar scheint jedoch, dass die Polizei selbst gesammelte Daten über angezeigte Straftaten (wie Tatorte, Begehungsweisen, Opferdaten) mit öffentlichen und nicht-öffentlichen Daten (wie Geodaten, Informationen über Veranstaltungen, Nutzungsdaten des Nahverkehrs) verknüpft,[10] um sie mit spezieller Software nach Mustern und Strukturen auszuwerten. So will sie (a) das Risiko künftiger Straftatbegehung an bestimmten Orten oder in bestimmter Weise (b) durch bestimmte Personen(-gruppen) oder (c) an bestimmten Personen auf der Grundlage von Wahrscheinlichkeitsmathematik prognostizieren.[11] Hinter diesen Programmen steht die Idee, dass Menschen oftmals gewohnten bzw. erfolgserprobten Handlungsmustern folgen.[12] Der Abgleich geht über traditionelle Datenvorratshaltung oder manuelle Auswertung von Informationen hinaus, da die computergestützte Anwendung statistischer Methoden auf einen Berg scheinbar trivialer Daten jedem für sich gesehen belanglosen oder (zunächst) freiwillig öffentlich gestellten Datum einen neuen Wert gibt.[13] Welche Anforderungen man an die dafür notwendigen Rechtsgrundlagen stellt und wie man *predictive policing* unter dem Blickwinkel der Begehrlichkeiten zur operativen Verbrechensbekämpfung beurteilt, hängt jedoch maßgeblich davon ab, ob durch den Datenabgleich lediglich Gefahrenherde oder ob auch Gruppen von möglicherweise straftatgeneigten Individuen herausgefiltert werden.

In den USA setzt man *predictive policing* zu beiden Zwecken ein,[14] einerseits um *hot spots* für bestimmte Straftaten zu lokalisieren, andererseits um einzelne strafge-

---

[9] Noch hat sich keine klare Terminologie für die verschiedenen Instrumente des automatisierten Datenabgleichs etabliert, vgl. dazu *Hackenberg*, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 42. Ergänzungslieferung 2015, Teil 16.7 Big Data, Rn. 7 ff.

[10] Das dahinter stehende Data Mining durchläuft regelmäßig folgende Phasen: (1) erster Zugriff auf Datenmenge, (2) Identifikation von Mustern, (3) Vergleich der Muster untereinander, (4) Vorhersage künftiger Muster; dazu ausführlich *Perry/McInnis/Price/Smith/Hollywood* (Fn. 4), p. xiv.

[11] *Perry/McInnis/Price/Smith/Hollywood* (Fn. 4), p. xiv.

[12] Letztlich steht dahinter das gleiche Konzept der Nutzung von Wahrscheinlichkeitsprognosen, das Internet-Warenhäuser mit einer personalisierten Werbestrategie verfolgen: „Kunden, die diesen Artikel gekauft haben, gefällt auch jenes Produkt …".

[13] Dazu etwa bereits früh BVerfG Urteil vom 15. 12. 1983 – 1 BvR 209/83 oder in jüngerer Zeit: BverfGE 120, 274, 344 ff.; *Simon/Taeger* JZ 1982, 143.

[14] Etwa „PredPol" (http://www.predpol.com); allgemein zu *predictive policing:* http://i-hls.com/2015/12/fighting-crime-with-big-data/; kritisch: *Ferguson*, Emory Law Journal (2002) 259.

neigte Personen zu identifizieren.[15] Der allmähliche Einsatz solcher Programme in Großbritannien,[16] Deutschland[17] und in der Schweiz[18] dient nach Presseberichten bisher nur dem Ziel, eine Art „Kriminalitätswetterkarte" auf der Grundlage polizeilicher Erkenntnisse aus Vortagen mit Hilfe eines Abgleichs mit Geodaten, Veranstaltungsterminen, Fahrgastaufkommen des öffentlichen Nahverkehrs etc. zu erstellen.[19] So scheint die europäische Variante als recht banale Form der Informationsgenerierung. In Wahrheit realisiert sich hier aber auch ein erster Schritt zu einem alltäglichen *Data Mining* in der Polizeiarbeit.[20] Würde man damit gewonnene Erkenntnisse für die Strafverfolgung nutzen, indem man auch nur ein personalisiertes Moment hinzufügt, etwa Telekommunikationsverbindungsdaten, ergäbe sich ein ganz neues Bild. Denn dann könnten die Behörden feststellen, wessen Mobiltelefon in einer bestimmten, räumlich bezeichneten Funkzelle in einem bestimmten Zeitraum „eingebucht" war. Eine solche Funkzellenabfrage[21] könnte eine Kriminalitätswetterkarte in eine Art „Schatzkarte" verwandeln, auf der einzelne Gruppen oder Individuen kartiert sind. Ob sich vielleicht bereits heute ohne das Hinzufügen eines personalisierten Moments etwas für die Strafverfolgung aus *predictive policing* ergeben könnte, ist nicht bekannt, da nur wenig über die aktuellen technischen Parameter bekannt ist. So kann kaum beurteilt werden, ab wann die Dichte nicht-personalisierter Daten eine individualisierbare Kartierung erlauben könnte, etwa indem Daten des öffentlichen Nahverkehrs mit dem Stromverbrauch in bestimmten Straßenzügen und Bargeldeinzahlungen auf bestimmten Bankfilialen mit dem Auftreten von Raubüberfällen (mit Skimaske und Pistole) abgeglichen würden und damit die Gruppe der wahrscheinlich als Täter in Betracht kommenden Personen auf die Bewohner einer überschaubaren Anzahl von Wohnungen eingegrenzt werden könnte.

Klar ist: Selbst wenn nur Daten aus Polizeiberichten mit anderen nicht-personalisierten Daten verknüpft und durch spezifische Prognosealgorithmen ausgewertet werden, handelt es sich bereits um eine Form der Datenverarbeitung, die – trotz Verknüpfung lauter scheinbar unverfänglicher Informationen – Muster ergibt, durch die Gruppen und Individuen aufgrund ihrer Handlungsmuster herausgefiltert werden können. Unklar ist, welcher Rechtsgrundlagen es für diese grundrechtsrelevanten

---

[15] Vgl. dazu: New York Times vom 24.9.2015, abrufbar unter http://www.ny-times.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html.

[16] Etwa PredPol in Trafford, einem Vorort von Manchester, vgl. http://disco-very.ucl.ac.uk/1344080/3/JDIBriefs_PredictiveMappingSChaineyApril2012.pdf.

[17] Vgl. *Singelnstein*, NStZ 2012, 605 mit Verweis auf Drs. 17/8544.

[18] *Schwarzenegger/Schmohl/Thalmann/Vertone/Zanolini*, Kriminalität und kommunale Kriminalprävention in Zürich. Kriminologisches Institut der Universität Zürich 2009.

[19] Vgl. dazu: *Legnaro/Kretschmann*, KrimJ 2015, 94 ff.; *Singelnstein*, NStZ 2012, 605; sowie zur Möglichkeit der Verknüpfung mit Daten, die durch Private gesammelt wurden: *Mantelero/Vaciago*, Cri 2013, 161 ff.

[20] Zur Nutzung von Data Mining im Bereich der Terrorismusbekämpfung oder allgemein durch Nachrichtendienste, vgl. etwa *Steinbock*, 40 Georgia Law Reviw [2005] 1, at 5.

[21] Vgl. dazu § 100g StPO; *Singelnstein*, NStZ 2012, 593 ff.; *Bär*, MMR 2008, 215 ff.

Eingriffe bedürfte[22] und wie die Schnittstellen zum Strafverfahren ausgestaltet sein müssten,[23] damit Generierung, mögliche Nutzung und anschließender Verbleib der neu hervorgebrachten Daten adäquat geregelt sind.

Jenseits der Überlegungen zu konkreten Anforderungen an mögliche Ermächtigungsgrundlagen bleibt ohnedies fraglich, in welchem Rahmen polizeiliches Data Mining in der alltäglichen Polizeiarbeit überhaupt flächendeckend eingesetzt werden dürfte.[24] Denn in Deutschland und auf europäischer Ebene vertritt die Rechtsprechung eine restriktive Haltung gegenüber anlasslosem automatisiertem Datenabgleich. Wenn etwa das BVerfG die präventiv polizeiliche Rasterfahndung mit Rücksicht auf das Grundrecht auf informationelle Selbstbestimmung[25] (und verwandte Grundrechte[26]) nur bei einer konkreten Gefahr für hochrangige Rechtsgüter (wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person) als zulässig ansieht, nicht aber bei einer allgemeinen Bedrohungslage,[27] erscheint zweifelhaft, welcher Anwendungsraum für *predictive policing* bleibt.[28]

III. *Predictive policing* und Verdachtsgewinnung

Gleichwohl stellt sich mit Blick auf Edda Weßlaus Befund die Frage: Könnte *predictive policing* nicht nur ein neues Präventionskonzept, sondern eine neue Form operativer Verbrechensbekämpfung sein?[29] Dürfte durch polizeiliches Data Mining künftig Tatverdacht gewonnen werden, unabhängig von tatbezogenen Anknüpfungspunkten durch Sammeln und Auswerten der Daten?[30]

---

[22] *Gluba*, Kriminalistik 2014, 347 ff.

[23] In Zürich etwa verweist man für den Einsatz des *predictive police*-Programms PRECOB auf die allgemeinen Grundlagen für polizeiliche Datenerhebung, da PRECOB nicht individualisierte Aktivitäten oder einzelne Kommunikationsvorgänge registriere (siehe Antwort des Stadtrats Zürich auf die Anfrage des Gemeinderats Angst (GR Nr. 2014/278) im Stadtrat von Zürich vom 4.12.2014); zur Bedeutung einer spezifischen Rechtsgrundlage für automatisierten Datenabgleich: *Kudlich*, GA 2011, 195; *Singelnstein/Putzer*, GA 2015, 566; *Valerius*, JR 2007, 276.

[24] *Singelnstein/Putzer*, GA 2015, 566; vgl. bereits die in Zusammenhang mit der sog. Rasterfahndung vorgebrachten Bedenken: *Simon/Taeger*, JZ 1982, 144.

[25] BVerfGE 65, 1, 43; BVerfG, Beschl. vom 14.12.2000 – 2 BvR 1741/99, abgedruckt in: NJW 2001, 879, 881; vgl. a. BVerfG Beschl. vom 12.4.2005 – 2 BvR 1027/02, abgedruckt in: DStRE 2005, 791, 794.

[26] Siehe etwa zum Grundrecht auf die Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen: BVerfG, Urteil vom 27.2.2008 – 1 BvR 370/07.

[27] BVerfG, Beschl. vom 4.4.2006 – 1 BvR 518/02 zu § 31 Polizeigesetz von Nordrhein-Westfalen von 1990, s. vor allem a.a.O., Rn. 138.

[28] Vgl. zur Beurteilung der Rasterfahndung *Teyssen/Goetze*, NStZ 1986, 529 ff.

[29] *Weßlau* (Fn. 1), S. 44.

[30] *Weßlau* (Fn. 1), S. 269 f. SK-StPO/*Weßlau*, Vor § 474 Rn. 16.

Technisch gesehen, scheint das unproblematisch.[31] Software-Agenten, die auf der Grundlage von Wahrscheinlichkeitsmathematik Muster erkennen, die Prognosen erlauben, können ebenso zurückblicken und Muster (und dadurch Personen oder Personengruppen) identifizieren, die zuvor keiner Strafverfolgungsbehörde aufgefallen sind. Sie werden dann einfach zu selbständig agierenden „Rasterfahndern". Das hat man – jenseits der Verfolgung von Terrorismus – bereits früh etwa im flächendeckenden Abgleich kassenärztlicher Abrechnungen zur Aufdeckung mutmaßlicher Betrügereien im Gesundheitswesen genutzt.[32] Heute setzt man es bei der Verfolgung von Geldwäsche ein.[33] *In concreto* hängt alles von der Programmierung und den zur Verfügung gestellten Daten ab.[34] Die Tür zu „retrospective policing" oder „recollective justice" durch automatisierte Ermittlungen gegen Unbekannt existiert also und – wie Edda Weßlau treffend bemerkt hat – sobald ein Instrument einmal zur Verfügung steht, findet es auch Verwendung.[35]

Rechtlich gesehen, erscheint uns die in die Vergangenheit gerichtete Rasterung aller möglicherweise relevanten Daten jedoch höchst problematisch, weil es unserer tradierten Vorstellung von Strafverfolgung in einem liberalen Rechtsstaat widerspricht, wenn ohne den Anlass eines Tatverdachts durch polizeiliche Entscheidung in die Vergangenheit blickende Software-Agenten Gruppen von Personen oder Individuen aufgrund von „Handlungsmustern" in das Visier der Behörden heben.

1. Vor- und Nachteile heißer Spuren

Edda Weßlau hat früh auf die Gefahren einer ausufernden Strafverfolgung durch automatisierten Datenabgleich aufmerksam gemacht,[36] als vielen eine Bedrohung durch das Zusammenführen scheinbar belangloser Informationen noch harmlos erschien. Mit dem Anwachsen der – vergleichsweise leicht auswertbaren – Daten in unserer digitalisierten Lebensumgebung treten die Risiken klarer hervor. Traditionelle Methoden der polizeilichen Überwachung waren *per se* nur begrenzt einsetzbar, weil sie einen von einem Menschen verantworteten, im Umfang definierten und gesteuerten Eingriff voraussetzen. Demgegenüber produzieren beim *Data Mining* auf Mustersuche vorprogrammierte Software-Agenten selbständig Ergebnisse, indem sie aus einer Vielzahl von Daten Muster menschlicher Handlungen herausfiltern. Dass diese anschließend sinnstiftend durch Menschen auf interessante Handlungsmuster interpretiert werden müssen, begrenzt die Gefahren nicht unbedingt. Denn

---

[31] *Hackenberg* (Fn. 9), Teil 16.7 Big Data, Rn. 7 ff.

[32] Vgl. dazu ausführlich: *Teyssen/Goetze*, NStZ 1986, 529 ff.

[33] Dazu etwa *Pieth*, European Journal of Law Reform 2002, 365 ff.

[34] Vgl. dazu „Privacy Expert: Time Traveling Robots could punish ‚future crimes'", http://www.infowars.com/privacy-expert-time-traveling-robots-could-punish-future-crimes/ (besucht am 20.1.2016).

[35] *Weßlau* (Fn. 1), S. 241 ff.

[36] Etwa *Weßlau* (Fn. 1), S. 305; *dies.*, ZStW 113 (2001) 687 ff.

damit kombinieren sich menschliche Erkenntnishorizonte (mit all ihren Vor- und Nachteilen) mit den schier unbegrenzten Möglichkeiten von Software-Agenten, Korrelationen zu finden,[37] z. B. dass Raubüberfälle im Stadtzentrum mit einem erhöhten Fahrgastaufkommen eines bestimmten Linienbusses korrelieren oder mit der Besucherzahl im zentral gelegenen städtischen Kunstmuseum oder bei Querabgleich mit Bonus-Karten-Daten des innerstädtischen Supermarktes mit dem Verkauf von Alcopops oder mit den Öffnungszeiten einer Suppenküche für Hilfsbedürftige. Diese einfachen Beispiele zeigen, dass der automatisierte Datenabgleich durch Software-Agenten *per se* eine sehr viel grössere Streubreite und eine sehr viel höhere Fehlerquelle hat als etwa eine Rasterfahndung. Anders als bei traditionellen Methoden der Informationsgewinnung steht beim *predictive policing* nicht zu Beginn eine Frage, die ein Mensch mit Blick auf einen Einzelfall formuliert hat, vielmehr findet die vollautomatisierte Suche Antworten auf Fragen, die vorher kein Mensch gestellt hat.[38]

So kann etwas oder jemand ins Visier der Strafverfolgungsbehörden geraten, weil es „ins Bild passt", nicht weil es dafür einen konkreten Anlass gibt.[39] Das könnte von Vorteil sein, weil sich Strafverfolgungsbehörden nicht auf „die üblichen Verdächtigen" kaprizieren. Allerdings geht ein auf Wahrscheinlichkeitsprognosen basiertes Polizeikonzept ebenfalls von „kriminalistischer Erfahrung" aus und verteilt dann Ressourcen auf mutmaßliche Kriminalitätsschwerpunkte, örtlich und personell. Denn es gibt keine gänzlich neutrale Analyse – Datensätze müssen bestimmt, eine Programmierung vorgegeben werden.[40]

Aus dieser Sicht ist naheliegend, dass Personen, die Gruppen angehören, die als „kriminogen" wahrgenommen werden, mehr Kontrollen und Eingriffe zugemutet würden – bis zur offensichtlichen rechtlichen Unzulässigkeit, etwa wegen des Diskriminierungsverbots.[41] Gleichzeitig fehlen valide Überprüfungsmechanismen dafür, wie sinnvoll und legitim bestimmte Mustersuchen sind und ob sie insgesamt (grund-)rechtsschonend durchgeführt werden können etc.[42] Programmierungen und Datenpools sind intransparent,[43] es fehlen Kontrollgruppen – insgesamt ergibt sich

---

[37] Zu kuriosen Korrelationen vgl. http://tylervigen.com/spurious-correlations.

[38] Vgl. dazu *Esposito*, in: Hildebrandt/de Vries, Privacy (eds.), Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology, Abingdon, Oxon 2013, S. 128.

[39] Einsatzmöglichkeiten ergeben sich in allen möglichen Lebensbereichen, vgl. zum „Fingerprinting" durch Beobachtung von Nutzerverhalten im Internet: *Herrmann/Fuchs/Federrath*, Fingerprinting Techniques for Target-oriented Investigations in Network Forensics, in: Sicherheit 2014: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI). LNI 228, GI 2014, 375 ff.

[40] *Perry/McInnis/Price/Smith/Hollywood* (Fn. 4), p. xix.

[41] Dazu bereits: *Weßlau* (Fn. 1), S. 50; *Masing*, NJW 2012, 2306; mit Blick auf das „racial profiling": *Drohla*, ZAR 2012, 411 ff.

[42] Dazu etwa: *van Brakel/de Hert*, Cahiers Politiestudies 2011, 180 (abrufbar unter: http://www.vub.ac.be/LSTS/pub/Dehert/378.pdf).

[43] Vgl. zur Bedeutung gesetzlicher Eingrenzung *Bergemann*, NVwZ 2015, 1705 f.

ein neues Risikoszenario für Fehler.[44] Es ist deshalb bereits aus dieser Warte fraglich, ob der mathematische Ansatz, der bei Internet-Warenhäusern sehr gut zu funktionieren scheint, auch für die tägliche Polizeiarbeit tauglich ist. Vor allem aber muss man fragen, ob ein solcher Ansatz zulässig und rechtspolitisch erwünscht ist. In den USA werden unerwünschte Effekte einer Diskriminierung bestimmter Bevölkerungsgruppen oder Wohngebiete bereits in der Tagespresse diskutiert, bis hin zur Schilderung individueller Schicksale von Straftätern, die in Risikogruppen festgeschrieben erscheinen.[45]

Aus europäischer Sicht trägt *predictive policing* genau jene Gefahr einer *maßlosen Überwachung in sich*, die nach den klaren Worten von BVerfG[46] und EuGH[47] in einem liberalen Rechtsstaat nicht zulässig ist, unter anderem weil sie jene diffuse Bedrohlichkeit durch Datenspeicherung verbreitet,[48] die den einzelnen von einer unbefangenen Grundrechtsausübung und einer selbstbestimmten Lebensweise abhalten könnte, weil unklar ist, wie Behörden gespeicherte Daten nutzen.

Predictive policing erscheint wie ein *Orwell'sches* Schreckensszenario, weil die Tendenz zur Totalüberwachung gewissermaßen systeminhärent ist. Denn Wahrscheinlichkeitsprognosen benötigen eine möglichst umfassende Datenbasis, um hohe Qualität zu erreichen. Erst seit unsere digitalisierte Lebenswelt einen hinreichend großen Datenpool generiert, „prognostizieren" Software-Agenten besser[49] als ein auf Statistikauswertung und anekdotische Lebenserfahrung angewiesener Mensch.[50] Die Größe des Datenpools erhöht natürlich auch die Erfolgschancen einer Straftatentdeckung beim Zurückblicken. Die in diesem Szenario gezeichneten Gefahren gehen weit über das Strafrecht hinaus. Mit polizeilichem Data Mining verbinden sich neue, jedoch nicht unbekannte Ängste vor Diskriminierung bestimmter Personengruppen (definiert durch Wohnort, Freizeitaktivität, sozialen Status o. a.).[51] Bestimmte Formen von *predictive policing* könnten dahin führen, dass Menschen aus

---

[44] Zu solchen „Wahrnehmungsrisiken" sowie zum „selektiven Datentransfer": *Weßlau*, FS Hilger, Heidelberg 2003, S. 62 und 65 sowie 66 ff.

[45] New York Times vom 24.9.2015, abrufbar unter http://www.ny-times.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html.

[46] Vgl. BVerfG, Beschl. vom 4.4.2006 – 1 BvR 518/02, Rn. 117 mit zahlreichen weiteren Hinweisen.

[47] EuGH vom 8.4.2014, verb. Rs C-293/12 und C-594/12 (Digital Rights Ireland), Rn. 26 ff.; EuGH vom 6.10.2015, Rs C-362/14 („Schrems") Rn. 39 ff.

[48] BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08, Rn. 242.

[49] *Perry/McInnis/Price/Smith/Hollywood* (Fn. 4), p. xiii; <http://www.rand.org/con-tent/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf>.

[50] Siehe dazu einerseits: *The Economist. 20 July 2013.* „Don't even think about it." http://www.economist.com/news/briefing/21582042-it-getting-easier-foresee-wrongdoing-and-spot-likely-wrongdoers-dont-even-think-about-it, und andererseits: *Biermann*, Die Zeit. 29.3.2015. Noch niemand hat bewiesen, dass Data Mining der Polizei hilft. http://www.zeit.de/digital/datenschutz/2015-03/predictive-policing-software-polizei-precobs.

[51] SK-StPO/*Weßlau*, Vor § 474 Rn. 4; *Limbach*, AnwBl. 2002, 454; *Mager*, Terrorismusbekämpfung zwischen Freiheit und Sicherheit, Kiel 2005, S. 53 ff.

Angst, in eine Risikogruppe zu gelangen, ihre Meinungsfreiheit erst gar nicht mehr wahrnehmen. Polizeiarbeit würde dann gesellschaftliches Zusammenleben bestimmen. Diese Gefahren werden bereits debattiert.[52]

Über diese Risiken einer operativen Verbrechensbekämpfung mit Hilfe von *predictive policing* wird bis jetzt jedoch kaum gesprochen.[53] Die folgenden Überlegungen beschränken sich auf drei Schlaglichter, die Edda Weßlau wichtig waren.

2. Begrenzende Funktion des Anfangsverdachts

Es stellt sich zunächst ganz grundsätzlich die Frage, ob *predictive policing* überhaupt, wenn es für die Polizeiarbeit zugelassen würde, hinüber in die Strafverfolgung wachsen könnte. Bekanntlich soll im liberalen Rechtsstaat die begrenzende Funktion des Tatverdachts einen Schutzwall zwischen Prävention und Strafverfolgung ziehen.[54] Edda Weßlau hat sich immer wieder mit der Frage beschäftigt, ob durch polizeiliche Präventionsmaßnahmen Tatverdacht ohne tatbezogene Anknüpfungspunkte generiert werden dürfe.[55] Sie hat damit den Finger auf eine empfindliche Stelle unseres Strafverfahrens gelegt. Denn allgemein wird das Dogma der begrenzenden Funktion des Tatverdachts (noch) hoch gehalten, obwohl schon aufgrund des Gesetzeswortlautes unklar ist, wie und wo eine Grenze gezogen werden muss.[56] Die Strafprozessordnung setzt weder in § 152 II noch in § 160 I StPO einen individualisierten Verdacht voraus. Wenn ein Verdacht gegen Unbekannt reicht, können repressive Ermittlungen im Grunde schon dann einsetzen, wenn Behörden (notfalls unter Zuhilfenahme kriminalistischer Erfahrung) vernünftigerweise annehmen dürfen, dass in einer bestimmten Gegend oder von einem nicht näher definierten Personenkreis in einer bestimmten Zeitspanne bestimmte Straftaten (kassenärztlicher Abrechnungsbetrug, Einbruchsdiebstähle, Erwerb von Pornographie etc.) begangen worden sind. Dass auch heute schon manche strafrechtlichen Ermittlungen jenseits *tatbezogener Anknüpfungspunkte*[57] aufgenommen werden, ist nicht erst seit jenen Verfahren bekannt, die plötzlich prominente Personen ins Visier von Strafverfolgungsbehörden rückten.[58] Wenn „Kriminalitätswetterkarten" mit dem Ziel aufaddiert würden, Gruppen strafgeneigter Personen festzustellen, könnte man Korrelationen in die Zukunft

[52] *Simon/Taeger*, JZ 1982, 140 ff. Vgl. zu den Auswirkungen in den USA: New York Times vom 24. 9. 2015, abrufbar unter http://www.nytimes.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html.

[53] Vgl. aber bereits: *Weßlau* (Fn. 1), S. 305.

[54] Ausführlich *Zabel*, ZIS 7/2014, 340 ff.

[55] *Weßlau* (Fn. 1), S. 269 f. SK-StPO/*Weßlau*, Vor § 474 Rn. 16.

[56] Vgl. etwa: KK/*Fischer*, 7. Aufl., München 2013, Vor §§ 158 ff. Rn. 172 ff.

[57] Vgl. zu den allgemeinen Definitionen: BGH 21.4.1988, NJW 1989, 96; LR/*Beulke*, § 152 StPO Rn. 23.

[58] Große öffentliche Aufmerksamkeit hat hier vor allem das Strafverfahren gegen *Edathy* erlangt, vgl. dazu etwa BVerfG Beschl. vom 15.8.2014 – 2 BvR 969/14; *Fischer*, Die Zeit, 27.2.2014, Nr. 10, S. 4; *Hoven*, NStZ 2014, 361 ff.

oder in die Vergangenheit verfolgen; in beiden Fällen folgten Strafverfolgungsbehörden Plausibilitätserwägungen, gegründet auf ihre kriminalistische Erfahrung.[59] Wenn – anknüpfend an das Beispiel oben – über eine Funkzellenabfrage der Abgleich von Fahrgästen in dem Linienbus im fraglichen Zeitraum mit Kunden eines innerstädtischen Supermarktes zu einer Gruppe von Personen führte, von denen man eine Alibi-Auflistung für die Tatzeiten aller angezeigten Raubüberfälle verlangte, so widerspricht das nicht § 152 II und § 160 I StPO an sich.

Dass der Anfangsverdacht keinen Schutzwall zwischen digitalisierten Präventionsinstrumenten und Strafverfolgung bauen kann, wurde bereits zu Beginn der computergestützten Rasterung klar: Als flächendeckend Kassenabrechnungen in Zusammenhang mit mutmaßlichen Betrügereien im Gesundheitswesen automatisiert durchsucht wurden, diskutierte man noch Grundsatzfragen,[60] verlangte eine spezifische Rechtsgrundlage, erhob datenschutzrechtliche Bedenken und monierte, dass die hinter der Rasterung stehenden kriminalistischen Hypothesen auf eine Art Generalverdacht hinauslaufen würden, der noch dazu nicht auf statistisch stabilen Füßen stehe.[61] Da die Strafprozessordnung jedoch nicht vorgibt, wie ein solcher Anstoß zu Ermittlungen aussehen muss, fehlt letztlich eine gesetzliche Vorgabe, wie ein Tatverdacht begründender Erfahrungssatz intersubjektiv belegt werden muss,[62] der nicht auf menschliche Beobachtungen gründet.[63]

Klar scheint lediglich, dass es unzulässig ist, einen Tatverdacht ausschließlich mit der Zugehörigkeit zu einer (Risiko-)Gruppe zu begründen.[64] Aber es ist kaum zu rechtfertigen, weshalb die Polizei nicht zur Begründung eines Verdachts auf Data Mining soll zurückgreifen können.

Dem steht letztlich nur unser (heute noch geteiltes) Verständnis entgegen, dass nur ein von einem Menschen konkret gehegter Tatverdacht[65] Ermittlungsmaßnahmen rechtfertigt[66] und zugleich begrenzt.[67] Dieses Dogma ruht auf der Tradition des reformierten Strafprozesses mit seiner Vorstellung einer effizienten Einhegung staatlicher Strafverfolgung und der damit verbundenen Beschränkung von individuellen

---

[59] Wobei es hier dann natürlich auch zu kuriosen Korrelationen kommen kann, vgl. http://tylervigen.com/spurious-correlations.

[60] Vgl. dazu ausführlich: *Teyssen/Goetze*, NStZ 1986, 529 ff.

[61] *Teyssen/Goetze*, NStZ 1986, 532.

[62] Dazu u. a. *Deiters*, Legalitätsprinzip und Normgeltung, Tübingen 2006, S. 124.

[63] Vgl. *Weßlau*, FS Hilger, S. 65; *Freund*, Normative Probleme der „Tatsachenfeststellung", Heidelberg 1987, S. 15 f.

[64] *Fischer* (Fn. 58), S. 2; *Satzger*, FS Beulke, Heidelberg 2015, 1020.

[65] Vgl. dazu etwa BVerfG vom 23. 3. 1994 – 2 BvR 396/94; BFH: Urteil vom 9. 12. 2008 – VII R 47/07.

[66] Vgl. etwa BVerfG, Beschl. vom 13. 3. 2014 – 2 BvR 974/12, Rn. 17; LR/*Beulke*, § 152 Rn. 22; *Fischer/Maul*, NStZ 1992, 10; *Zabel*, ZIS 7/2014, 341.

[67] *Eisenberg*, Beweisrecht der StPO, Rn. 505 ff.; *Eckstein*, Ermittlungen zu Lasten Dritter, Tübingen 2013, S. 75 ff.; *Satzger*, FS Beulke, 1012.

Rechten.[68] Dass die Wirklichkeit bereits anders aussieht, lässt schon die semantische Komplexität der Definition des Tatverdachts vermuten,[69] die wohl eher verdeckt, was wesentlich ist: der Wunsch nach Zügelung der Macht der Menschen, denen die Strafverfolgung im Namen der Gemeinschaft anvertraut ist. Doch jede Eröffnung neuer technischer Möglichkeiten bringt die tradierte Begrenzung von Strafverfolgung unter Druck.[70] Die Erfahrungen mit dem Ausbau technischer Überwachungsmöglichkeiten machen wenig Hoffnung, dass die rechtliche Hürde des Tatverdachts noch als funktionierender Schutzwall zwischen *predictive policing* und operativer Verbrechensbekämpfung dienen könnte, sollte polizeiliches Data Mining in Deutschland tatsächlich Einzug halten. Der Tatverdacht ist maßgeblich auf menschliches Tätigwerden ausgerichtet.

3. Verwendungs- und Verwertungsregeln

Vielversprechender für die Einrichtung eines effektiven Schutzwalls zwischen Prävention und Repression scheinen daher Verwendungs- und Verwertungsverbote, die den Informationsfluss eindämmen.[71] Denn, wie Edda Weßlau einmal bemerkte, „wenn gar kein Datentransfer stattfindet, so wird [die beschuldigte Person als solche ...] nicht beeinträchtigt“[72] – allerdings dafür die Wahrheitssuche im Strafverfahren.

Gelangen für die Sachverhaltsklärung in einem Strafverfahren relevante Informationen nicht zur Kenntnis der zuständigen Instanzen, bedarf das einer besonderen Rechtfertigung, etwa des Schutzes von Grund- und Menschenrechten.[73] Bei der Entscheidung über das Eingreifen eines Beweisverwertungsverbots müssen regelmäßig widerstreitende Interessen gegeneinander abgewogen werden, etwa das Allgemeininteresse an der Aufklärung des Sachverhalts gegen Persönlichkeitsrechte einzelner und deren Recht auf informationelle Selbstbestimmung.

Welchen konkreten Schutz gerade das letztgenannte Recht im Rahmen einer strafprozessualen Beweisführung entfalten könnte, ist fraglich. Sinn des Beweisverfah-

---

[68] Ausführlich dazu: *Zabel* ZIS 7/2014, 340. Illustrativ dafür, unter welchen (extremen) Umständen dieses Erbe praktische Konsequenzen zeitigt: *AG Saalfeld*, Beschl. vom 3.7.2001, 157/01 (abgedruckt in: NJW 2001, 3642).

[69] Vgl. dazu etwa *Satzger*, FS Beulke, 1012 ff.

[70] *Weßlau* (Fn. 1), S. 243 ff.; vgl. auch *Wohlers*, GA 2014, 680.

[71] Zum Verhältnis von Verwendungsregeln und Verwertungsverboten *Dencker*, FS Meyer-Gossner, München 2001, 237 ff.; *Singelstein*, ZStW 120 (2008), 854 (865 ff.).

[72] *Weßlau*, FS Hilger, S. 66.

[73] Vgl. etwa BGH Urteil vom 9.9.2003 – 1 StR 356/03 = NStZ-RR 2004, 19; BGH Urteil vom 17.3.1983 – 4 StR 640/82 = BGHSt 31 308; *Gless*, Internationales Strafrecht, 1. Aufl., Basel 2011, § 136 Rn. 3; *Eisenberg*, Beweisrecht der StPO, 7. Aufl., München 2011, Rn. 330; *Jahn*, Beweiserhebungs- und Beweisverwertungsverbote im Spannungsfeld zwischen den Garantien des Rechtsstaates und der effektiven Bekämpfung von Kriminalität und Terrorismus, Gutachten C für den 67. DJT 2008, C 38 ff.; *Puppe*, GA 1978, 305.

rens ist es ja, alle relevanten Informationen ans Tageslicht zu befördern. Beschuldigte und Zeugen können diesem Anliegen traditionell nur wenige Verweigerungsrechte entgegensetzen.[74] Setzte man nun dem Aufklärungsauftrag ein starkes Individualrecht entgegen, nach dem grundsätzlich jeder selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen kann,[75] dann würden sich die Gewichte im Strafprozess erheblich verschieben. Gleichzeitig kann im Konfliktfall nicht immer die staatliche Aufklärung dem Persönlichkeitsschutz vorgehen, denn Datenschutz wird nicht ganz obsolet, weil man sich im Strafprozess befindet. Das Dilemma wird an der Verwendungsregelung für Informationen aus einer Rasterfahndung deutlich.

Nach § 98a StPO[76] dürfen bei zureichenden tatsächlichen Anhaltspunkten für bestimmte Straftaten von erheblicher Bedeutung Daten automatisch abgeglichen werden, wenn andernfalls eine Aufklärung erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Die Verfahrensregelung äußert sich nicht dazu, wie mit dem Transfer zwischen polizeilicher und strafrechtlicher Rasterfahndung[77] umzugehen ist. Vielmehr wird allgemein auf § 477 II StPO zurückgegriffen. Danach dürfen die „auf Grund einer entsprechenden Maßnahme nach anderen Gesetzen erlangten personenbezogenen Daten zu Beweiszwecken im Strafverfahren *nur* zur Aufklärung solcher Straftaten verwendet werden",[78] zu deren Aufklärung eine solche Maßnahme nach der StPO hätte angeordnet werden dürfen. Was sich wie eine Einschränkung anhört, kommt praktisch einem datenschutzrechtlichen Dammbruch gleich.[79] Denn für Katalogtaten, deren Aufklärung andernfalls „erheblich weniger erfolgversprechend oder wesentlich erschwert wäre", existiert kein Schutzwall zwischen präventiver und repressiver Rasterung.

Der Strafprozess lässt hier die Zweckbindung und damit das Grundrecht auf informationelle Selbstbestimmung letztlich leerlaufen.[80] Aus datenschutzrechtlicher Sicht ist eine weitere Verwendung und Verwertung von den durch Rasterfahndung generierten Daten nur zulässig, wenn sie dem ursprünglich vorgesehenen Zweck,

---

[74] *Gleß*, FS Paeffgen, Berlin 2015, S. 712; *Krauß*, FS Gallas, Berlin u.a. 1973, S. 365 ff.

[75] BVerfGE 65, 1.

[76] Dazu ausführlich LR/*Menges*, § 98 Rn. 2 ff.; *Siebrecht*, Rasterfahndung. Eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, Berlin 1997, 27 ff.

[77] Differenzierung zwischen zufälligen Funden, die der Klärung des Tatverdachts dienen, zu dessen Klärung der strafprozessuale Eingriff angeordnet war (dann Verwertung zulässig), und zufälligen Funden, die auf eine andere Straftat hinweisen (dann Verwertung unzulässig) vgl. *Singelnstein*, ZStW 120 (2008) 859.

[78] Hervorhebung durch Verf.

[79] Die ursprünglich vorgesehene Beschränkung wurde im Vermittlungsverfahren gestrichen, vgl. dazu: BT-Drucks. 14/2595, S. 26 f.; BT-Drucks. 14/3525, S. 2 f.; zu datenschutzrechtlichen Erwägungen in die Beweisverbotslehre: *Dencker*, FS Meyer-Gossner, S. 237 ff.; *Kutscha*, ZRP 1999, 156; *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaften und Nachrichtendiensten, Heidelberg 2002, S. 263 ff.

[80] Vgl. auch *Singelnstein*, ZStW 120 (2008) 860 ff.

der Klärung der für die Fahndung formulierten Frage dienen.[81] Aus dieser Sicht müsste die Verwendung einer Erkenntnis jenseits des Tatvorwurfs, zu dessen Klärung der automatisierte Datenabgleich durchgeführt wurde, als Zweckänderung und damit als neu zu rechtfertigender Eingriff anzusehen sein.[82] Doch eine solche Orientierung am Grundrecht auf informationelle Selbstbestimmung wird von vielen als Fremdkörper in einem primär auf Wahrheitsfindung orientierten Strafverfahren empfunden. Deshalb sieht die herrschende Meinung die – über einen hypothetischen Ersatzeingriff eingegrenzte – Datenumwidmung als zulässig an.[83]

Hier offenbart sich ein Problem, das bei einem Einsatz breit gestreuter Eingriffe in das Recht auf informationelle Selbstbestimmung im Strafverfahren durch automatisierten Datenabgleich weiter an Brisanz gewinnen dürfte: Ein datenschutzrechtlich begründetes Beweisverwertungsverbot fügt sich zwar nur schwer in ein vom Amtsaufklärungsgrundsatz geprägtes Strafverfahren ein, aber wenn man alle Erkenntnisse, die man beispielsweise bei Personalisierung einer Kriminalitätswetterkarte erlangen könnte, auch benutzen dürfte, dann lohnt sich genau die Verdachtsausforschung, die es zu vermeiden gilt. Hier muss man neue Ansätze für Beweisverbote fruchtbar machen. In der Schweiz etwa gilt ein Verbot der „Fishing expeditions"[84], das ein ausforschendes Suchen nach Beweismitteln im trüben Wasser[85] mit Hinweis auf die fehlende Verhältnismäßigkeit verbietet.[86]

4. Verfahrensrechte der Betroffenen

Zu überlegen bliebe noch, wie man Verfahrensrechte betroffener Personen adäquat vor Nachteilen schützen kann, wenn man den Weg eines strikten Verwendungs- und Verwertungsverbots nicht gehen wollte. Diese Frage stellt sich, weil sich aus Data Mining Informationsasymmetrien ergeben können. Denn die betroffene Person wird weder bei der Auswahl bzw. Generierung des betreffenden Datenpools noch bei der Programmierung der Software-Agenten noch in anderer Weise an der Informationssammlung beteiligt. Selbst derjenige, dem bewusst ist, dass er digitale Spuren

---

[81] *Weßlau*, FS Hilger, S. 58, 66; BT-Drs. 16/5864, S. 64, 66.

[82] *Singelnstein*, ZStW 120 (2008) 856; *Weßlau*, ZStW 113 (2001) 681; *Wolter*, FS Rudolphi, Neuwied 2004, S. 735 ff.

[83] Dazu etwa *Singelnstein*, ZStW 120 (2008) 856.

[84] BGE 137 I 218 (221 f.); 103 Ia 206 (211); *Gutz*, Beschwerde ans Bundesgericht gegen Entscheide des Bundesverwaltungsgerichts auf dem Gebiet der internationalen Rechtshilfe in Strafsachen (Art. 84 BGG). Die materielle Abgrenzung von Amts- und Rechtshilfe am aktuellen Beispiel der strafprozessual unzulässigen amerikanischen „fishing expeditions" („Gruppenanfragen"), Archiv für schweizerisches Abgaberecht 80, 713.

[85] *Donatsch/Heimgartner/Meyer/Simonek*, Internationale Rechtshilfe, Zürich 2015, 93.

[86] Vgl. dazu etwa BGE 106 Ib 260 (264). Dazu *Donatsch/Heimgartner/Meyer/Simonek*, (Fn. 5), 92 ff.; *Popp*, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel 2000, § 14, Rn. 400 ff. mit Verweis auf Art. 5 II Bundesverfassung und Art. 4, Art. 30 IV, Art. 40 II und Art. 63 I Internationales RSG.

schafft, also jedem, dem die (Vorrats-)Datenregistrierung bekannt ist, weiß trotzdem nicht, wozu die Daten benutzt werden. Es ist nicht bekannt, mit welchen anderen Daten ein durch Benutzung eines Mobiltelefons oder eines GPS-Systems erstelltes Bewegungsprofil in einem automatisierten Datenabgleich verknüpft und gegen einen verwendet werden könnten. Selbst wenn Hinweise auf allen Mobiltelefonen warnen würden: „Achtung! Wenn Sie dieses Telefon mit sich tragen oder jemanden anrufen, dann können die registrierten Verbindungsdaten im Falle einer Strafermittlung gegen Sie verwendet werden!" würde damit einer möglichen Aushöhlung strafprozessualer Garantien nicht komplett vorgebeugt. Oftmals ergibt sie sich erst, wenn man die durch polizeiliches Data Mining generierten Muster für die Strafverfolgung personalisiert.

Wann die Einschränkung von Verfahrensrechten bei einer Umwidmung von *predictive policing* vom Präventionsinstrument zum Instrument für die Strafverfolgungsbehörden tatsächlich zu einem Verwendungs- und Verwertungsverbot führen müsste, lässt sich kaum abstrakt beurteilen. Maßgeblich wäre wohl das Zusammenspiel der unterschiedlichen Risiken für eine faire Strafverfolgung. So könnte neben dem Recht auf rechtliches Gehör der Grundsatz *nemo tenetur se ipsum accusare*[87] verletzt sein. Denn Data Mining rekonstruiert individuelle Gewohnheiten, die ein Beschuldigter vielleicht nie preisgegeben hätte und die ihn möglicherweise einer Risikogruppe zuordnen. Er müsste sich dann gegen einen Verdacht verteidigen, dessen Zustandekommen von Datenkorrelationen abhängt, die er nicht unbedingt nachvollziehen kann, und der sich dann auf eine vermeintlich durch Fakten begründete Wahrscheinlichkeit stützt, die er entkräften muss. Es braucht nur wenig Phantasie, um sich vorzustellen, dass die Passagiere eines Linienbusses, die auf der Grundlage der aufaddierten und mit anderen Daten abgeglichenen „Kriminalitätswetterkarten" in Verdacht geraten könnten, nicht im Nachhinein eine überzeugende Alibi-Liste für ihre Bewegungen der letzten Monate geben können oder wollen. Vergleichbares gilt für Besucher eines Museums, Käufer eines bestimmten Getränks oder Hilfesuchende in einer Suppenküche. Verböte sich eine rückwärtsgerichtete Mustersuche vielleicht bereits deshalb, weil dadurch das Recht zu schweigen und die Unschuldsvermutung ausgehöhlt werden? Denn wenn sich ein einzelner gegen eine automatisiert erstellte Wahrscheinlichkeitshypothese und aus selektiv gerasterten Informationen verteidigen muss, kann Schweigen gefährlich werden.[88]

Es erscheint jedoch fraglich, ob polizeiliches Data Mining den *nemo tenetur*-Grundsatz oder auch die Unschuldsvermutung per se in einem Maße beeinträchtigt, das ein Verwendungs- oder Verwertungsverbot nach sich ziehen muss. Denn die Verarbeitung persönlicher Daten kollidiert nicht ohne weiteres mit dem Grundsatz *nemo tenetur se ipsum accusare,* nur weil den Einzelnen betreffende persönliche Daten ohne seine persönliche Mitwirkung mit anderen Daten verknüpft werden.[89] Solange

[87] *Weßlau*, ZStW 110 (1998).

[88] Vgl. *Weßlau*, FS Hilger, S. 62 und 65 sowie 66 ff.

[89] SK-StPO/*Wohlers*, 4. Aufl. 2010, § 98a Rn. 7.

der Einzelne nicht gezwungen wird, sich selbst zu belasten, käme man in der durch Data Mining vorbereiteten Vernehmungssituation nur dann zu einer Einschränkung von *nemo tenetur,* wenn man jede Einschränkung der Willensfreiheit in einer Vernehmungssituation als grundsätzlich erheblich ansieht, etwa weil die geheime staatliche Informationssammlung den Einzelnen zwingt, eine bereits durch eine umfangreiche Beweissammlung validierte Sachverhaltshypothese zu entkräften.[90]

IV. Fazit

Da nicht auszuschliessen ist, dass *predictive policing* in der Zukunft als Präventionsinstrument eingesetzt werden wird, sind mögliche Implikationen für die Strafverfolgung zu bedenken, bevor vollendete Tatsachen geschaffen werden. Edda Weßlaus beharrliche Arbeit an den Schnittstellen von Prävention und Repression unter den Vorzeichen zunehmender Technologisierung hat die Notwendigkeit aufgezeigt, möglichst früh die aus strafprozessualer Sicht notwendigen Forderungen für die Ausgestaltung der rechtlichen Rahmenbedingungen zu formulieren, damit im Ernstfall ein funktionierender Schutzwall zwischen Prävention und Repression existiert.[91]

Manche mögen eine Nutzung von *predictive policing* für repressive Zwecke als unwahrscheinliches Schreckensszenario ansehen. Doch der vorsichtige Vorstoß von Bundes- und Landesbehörden[92] und die allgemeine Tendenz, menschliche Entscheidungen durch automatisch generierte Daten zu untermauern,[93] lassen den künftigen Einsatz von polizeilichem Data Mining in der einen oder anderen Form erwarten.[94]

Ob die dafür notwendigen breit gestreuten Eingriffe in das Recht auf informationelle Selbstbestimmung[95] dann nur die Situation derjenigen verändert, die als Verdächtigte den Strafverfolgungsbehörden gegenüber stehen, oder das Leben aller,[96] bleibt abzuwarten. Gegen einen flächendeckenden Einsatz von polizeilichem Data Mining in Deutschland spricht die hierzulande kritische Haltung gegenüber automatisiertem Datenabgleich. Gleichwohl sollte man nicht vergessen, dass die deutsche Rechtspolitik nicht mehr alleine die Richtung vorgeben kann. Die Einbindung in

[90] LR/*Gleß*, § 136a Rn. 15.

[91] Vgl. *Weßlau* (Fn. 1), S. 22, 90, 204 ff.

[92] Vgl. etwa BT- Drs. 17/8544 sowie BT-Drs. 18/3703.

[93] Dieses Phänomen ist etwa auch in Zusammenhang mit der Sicherungsverwahrung zu beobachten, vgl. *Boetticher/Dittmann/Nedopil/Nowara/Wolf*, NStZ 2009, 478 ff.

[94] Im Bereich der Strafen und Maßnahmen hat diese Revolution bereits stattgefunden, vgl. dazu etwa: *Schuman*, 18 New Criminal Law Review (2016). S. 214 ff. für die USA; *Gerth/Rossegger/Singh/Endrass*, Assessing the risk of severe intimate partner violence: Validating the DyRiAS in Switzerland. 1 Archives of Forensic Psychology (2015) no 2/15.

[95] Zur Gefahr des „eingeschüchterten Grundrechtsgebrauchs": SK-StPO/*Weßlau*, Vor § 474 Rn. 4; *Limbach*, AnwBl 2002, 454; *Mager* (Fn. 51), S. 53 ff.

[96] BVerfGE 65, 1, 42 f.

die europäische Zusammenarbeit in den Bereichen Justiz und Inneres legt den großen Rahmen fest.[97] Ob eine gesamteuropäische Abwägung von Sicherheit und Freiheit anders ausfällt, als wenn eine solche alleine in Deutschland vorgenommen würde, ist offen – die Meinungen sind breit gestreut. In der deutschen Rechtsprechung votieren seit langem dezidierte Stimmen dafür, dass nicht alles, was Sicherheitserhöhung verspricht, auch eingesetzt werden muss.[98] Die jüngere Rechtsprechung des EuGH[99] und kritische Bewertungen aus anderen EU-Staaten[100] weisen in jüngerer Zeit in eine ähnliche Richtung. Doch stehen wir wohl erst am Beginn einer Debatte, die höchst kontrovers geführt werden dürfte – während der automatisierte Datenabgleich immer neue Einsatzmöglichkeiten verspricht und die Rechtsetzung sich nicht mit gleicher Dynamik entwickeln dürfte.

Edda Weßlau mahnte bereits vor wenigen Jahren in der Auseinandersetzung um den Transfer polizeilich erlangter Daten in das Strafverfahren: „Nur eine Rechtspolitik, die wesentlich konsequenter mit dem Prinzip der Zweckbindung von Daten ernst machen würde, könnte dem Streit wieder eine reale, grundrechtsrelevante Dimension verleihen".[101] In der Zwischenzeit steht angesichts der digitalen Umwälzung vieler Bereiche bereits die Forderung nach „Bürgerrechten in Netzversion" im Raum: Sie sollen jenseits der tradierten Grundrechte (etwa auf Persönlichkeitsrecht, Privatsphäre oder Datenschutz) im digitalen Miteinander funktional eine adäquate Zügelung der Staatsmacht sichern.[102] Bei einem Ausbau digitalisierter Polizeiarbeit wird es nicht lange dauern, bis auch die Strafrechtswissenschaft ihre Rechtsinstitute in Netzform übersetzen muss, damit der Strafprozess weiterhin seine doppelte Aufgabe erfüllen kann: einerseits Rechtsgrundlagen und Instrumentarium bereitzustellen, damit Schuldige einer Straftat überführt werden können, und andererseits bestmögliche Vorsorge dafür zu treffen, dass Unschuldige nicht verurteilt werden und in die Freiheit aller möglichst wenig eingegriffen wird.[103]

---

[97] Was sich unter anderem in dem Tauziehen um einen Beschluss der EU-Staaten zur Speicherung von Fluggastdatensätzen (sog. Passenger Name Records, PNR) in innereuropäischen Flügen mit dem Ziel der Verhütung und Verfolgung terroristischer Straftaten und anderer schwerer Kriminalität gezeigt hat. Zum Gesetzesvorhaben siehe http://www.consilium.europa.eu/de/press/press-releases/2015/12/04-eu-passenger-name-record-directive/; zur Gesamtsituation: *Mantelero/Vaciago*, Cri 2013, 168 f.

[98] Vgl. dazu etwa das eindrückliche Minderheitsvotum der Richterinnen *Jäger* und *Hohmann-Dennhart* zur Entscheidung des BVerfG betreffend die Zulässigkeit von Abhörmaßnahmen in Wohnräumen (BVerfGE 100, 382 [391]).

[99] EuGH vom 8.4.2014, verb. Rs C-293/12 und C-594/12 (Digital Rights Ireland), Rn. 26 ff.; EuGH vom 6.10.2015, Rs C-362/14 („Schrems") Rn. 39 ff.

[100] House of Lords, Surveillance. Citizens and the State, London 2009, S. 26–29.

[101] *Weßlau*, FS Hilger, S. 58.

[102] *Dotzler*, Vom Unbehagen im Netz, NZZ vom 3.2.2016, S. 39.

[103] Vgl. *Roxin*, Einführung zur StPO, 49. Aufl. 2013, S. IX.

II. Strafrecht und Kriminalpolitik

III. Grundlagen

IV. Persönliches