Dr. Simon Egbert
simon.egbert@uni-bielefeld.de

04.06.2021

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Ausschussdrucksache
19(4)863 A

Stellungnahme zum Antrag der FDP-Fraktion ‚Smart Police – Digitalisierung der deutschen Polizei anschieben' – Drucksache 19/27172 (02.03.2021)

Die Digitalisierung bietet selbstverständlich auch für die Polizei erhebliches Potenzial in Hinblick auf die Verbesserung ihrer Arbeit. Allerding sollte man nicht dem Trugschluss verfallen, dass digitale Technologien per se und gleichsam automatisch eine effektivere und/oder effizientere Polizeiarbeit ermöglichen. Vielmehr ist die erfolgreiche Implementierung von digitalen Technologien – nicht nur, aber vor allem bei der Polizei – überaus voraussetzungsvoll (vgl. Egbert/Leese 2021). Gleichzeitig ist die Einführung von digitalen Technologien stets mit Risiken verbunden, die im Rahmen jeglicher Pilotierungs- wie Implementierungsbemühungen reflektiert und konsequent in Rechnung gestellt werden müssen (vgl. Ferguson 2017).

Diesbezüglich gilt es zunächst auf ein grundsätzliches Faktum hinzuweisen: Digitalisierte Praktiken sind stets soziotechnische Praktiken, digitale Technologien immer und unumgänglich auch soziale Technologien. Dies impliziert u. a., dass algorithmische Analysen keineswegs per se neutrale oder objektive Ergebnisse liefern. Zu glauben, digitale Technologien könnten von sich aus für eine neutrale Risikobewertung sorgen, ist ohnehin naiv. Bei der Programmierung von Algorithmen und der Auswahl der zu analysierenden Daten sind vielfältige menschliche Entscheidungen zu treffen, die allesamt das Potenzial von Verzerrungen bergen (z. B. boyd/Crawford 2012: 666ff.; Kitchin 2017: 14f.).

Es stimmt selbstredend, dass ein Algorithmus stets strikt gemäß seiner Programmierung entscheidet und sich dabei nicht von Gefühlen, Vorteilen o.ä. leiten lässt – diese Entscheidungen kann er aber nur auf Basis einer Weltsicht treffen, die die ihm vorliegenden Daten ermöglichen. Liegen einer algorithmischen Analyse verzerrte Daten zu Grunde, kann kein neutrales Ergebnisse mehr am Ende der Analyse stehen (vgl. Abb. 1). Dieser Punkt ist bei Analysetechnologien, die mit polizeilichen Daten arbeiten, hochrelevant, ist doch seit Jahren, in nationalen wie internationalen Studien ebenso breit wie überzeugend belegt, bekannt, dass die Wahrscheinlichkeit für ethnische Minderheiten, in den Fokus der Polizei zu geraten, überproportional hoch ist (Glover 2009; Glaser 2014; Herrnkind 2014; Behr 2018). Darauf folgt, dass Personen betroffener Gruppen in polizeilichen Datenbanken überrepräsentiert sind, was ein Algorithmus für sich genommen aber nicht als Folge diskriminierender Polizeipraktiken zu erkennen vermag, sondern viel eher als Beleg interpretiert, dass derlei Personen ein höheres Kriminalitätsrisiko aufweisen – was zu diskriminierenden Verstärkerprozessen führen kann, da die

algorithmischen Risikoanalysen den polizeilichen Fokus auf bereits überpolizierte Bevölkerungsgruppen nochmals verstärken (z. B. O'Neil 2016).

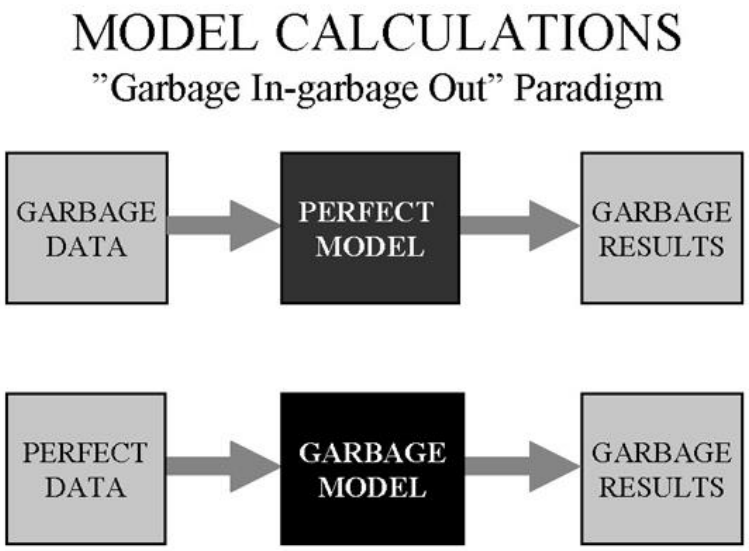

Abbildung 1: *Garbage in, Garbage out-Modell (Quelle: http://left.mn/2014/02/polymet-knew-now-knew/)*

Dieses Problem verschärfend und bereits unter dem Schlagwort „tech-washing" diskutiert, können diese diskriminierenden Verstärkereffekte unbemerkt auftreten, indem sie nämlich von den Technologien selbst erzeugt werden. So kann die autonome Herstellung von Risikokorrelationen in großen Datenmengen durch selbstlernende und (weitestgehend) unüberwachte Algorithmen dazu führen, dass algorithmisch eigenständig diskriminierende Verbindungen, z. B. zwischen Hautfarbe und individuellem Kriminalitätsrisiko, konstruiert werden, wobei die nachträgliche Entdeckung und Eliminierung dieser Fehldeutungen überaus schwierig ist, da entsprechende Algorithmen immer auch als Black Box fungieren und oft – auch für die beteiligten Polizisten und Polizistinnen – uneinsehbar sind (Pasquale 2015).

Dies führt mich zu meinem nächsten Punk: Transparenz.

Die Zusammenarbeit mit Industriepartnern aus der Digitalwirtschaft birgt für die Polizei die grundsätzliche Gefahr, mit Instrumenten und Werkzeugen zu arbeiten, die tief in den organisationalen und praktischen Alltag von Polizistinnen und Polizisten eingreifen, gleichzeitig aber für jene auf Grund ihres proprietären Charakters weitestgehend intransparent bleiben. Dies muss so weit wie möglich verhindert werden, da ein kompetenter und kritischer Umgang mit derartigen Technologien sonst nicht möglich ist. Ein hinreichender Einblick in die Grundannahmen und -prinzipien der genutzten Technologien muss den Anwenderinnen und Anwendern innerhalb der Polizei zwingend gewährleistet sein.

Dies gilt ebenfalls für die Bürgerinnen und Bürger, denen gegenüber die Polizei begründungspflichtig ist. Trotz legitimer Geheimhaltungsinteressen muss auch die Bevölkerung eine hinreichend präzisen Einblick in die Arbeitsweise der polizeilich genutzten digitalen Technologien bekommen können. Dies gilt selbstredend ebenfalls und noch stärker für Richterinnen und Richter sowie für die Rechtsbeistände von angeklagten Personen, wenn in betreffenden Verfahren solcherart Technologien relevant sind. Auch und gerade im Falle digitalisierter Polizeipraktiken muss die Prüfung der Rechtmäßigkeit der erhobenen Vorwürfe umfassend möglich sein (z. B. Singelnstein 2018).

Ferner möchte ich auf die möglichen Folgen der polizeilichen Zusammenarbeit mit Industriepartnern aus der Digitalwirtschaft hinweisen.

Der Rechtstreit zwischen dem New York Police Department und der Firma Palantir (s. z. B. Price/Hockett 2017) hat gezeigt, dass sich Polizeibehörden zumindest potenziell in eine starke Abhängigkeit begeben, wenn sie ihre Erkenntnisse mit Hilfe kommerzieller Software generieren. Denn nachdem die New Yorker Polizei den Vertrag mit Palantir kündigen wollte, hat Palantir darauf bestanden, die mit ihrer Software gewonnenen Erkenntnisse nach Vertragsende dem Zugriff der New Yorker Polizistinnen und Polizisten zu entziehen.

In diesem Zusammenhang gilt es ebenfalls zu fragen, wie stark und übergreifend eine kommerzielle Software in die technische Infrastruktur von Polizeibehörden eindringen sollte, ohne dass etwaige Folgevertragsverhandlungen über Gebühr einseitig verlaufen, wenn nämlich die gesamte polizeiliche Datenhaltungs- und Kommunikationsinfrastruktur auf der betreffenden Software aufbaut und die Folgekosten eines Vertragendes für die Polizei exorbitant hoch wären.

Fakt ist, dass durch die zunehmende Datafizierung der Polizei externe Akteure tief in den operativen Alltag der Polizei vordringen, womit zahlreiche Risiken verbunden sind. Dazu zählt insbesondere, dass gesichert werden muss, dass Unbefugte keinen Zugriff auf sensible polizeiliche Daten haben. Ebenso muss gesichert sein, dass so wenig Daten wie möglich aus den Polizeibehörden herausgeben werden.

Nun zu meinem letzten Punkt: Überwachung.

Internationale Studien haben bereits festgestellt, dass digitalisierte Polizeipraktiken das Potenzial haben, Überwachungspotenziale der Polizei zu vervielfältigen. So schildert Brayne (2021) in Bezug auf die Nutzung von Palantir-Software des Los Angeles Police Department das Phänomen der „dragnet surveillance“ (dt.: Schleppnetz-Überwachung), welches eines substantielle Ausweitung des überwachenden Blickes impliziert, da durch die auf Verbindungsanalysen

(„link analyses“) spezialisierte Palantir-Software auch solcherart Personen in den Fokus der Polizei rücken, die bis dato noch keinen Kontakt zur Polizei hatten – weil sie mit verdächtigen Personen in Kontakt stehen (vgl. Abb. 2). Eine solche Spielart von Kontaktschuld (auch „guilt by association“ genannt) darf keinesfalls Gegenstand polizeilicher Analysetätigkeiten werden.

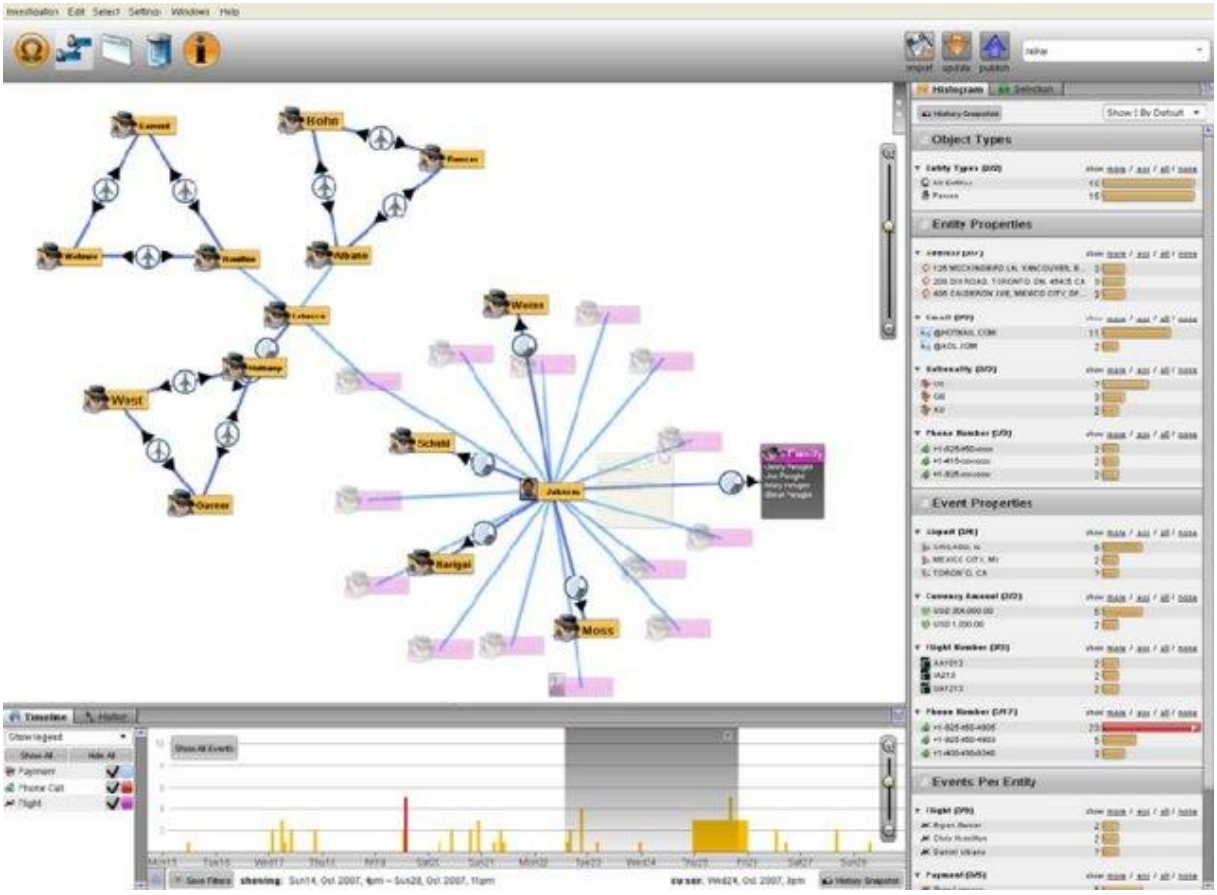

Abbildung 2: *Palantir Gotham-Screenshot (Quelle: https://www.researchgate.net/profile/Brian-Ulicny/publication/230818105/figure/fig2/AS:340539108020226@1458202258875/Palantir-Screenshot-from-Palantir-Tech-Blog-The-graph-is-linked-to-the-histogram-view_W640.jpg)*

Neue Datenanalysealgorithmen in den Händen der Polizei haben ebenso das Potenzial, die Überwachung von bereits polizeibekannten Personen zu intensivieren, indem beispielsweise automatische Alarme aktiviert werden können (z. B. durch sogenanntes „geofencing“, mit dem sich Areale vordefinieren lassen, bei dessen Betreten von ausgewählten Personen automatisch eine Alarmmeldung ausgelöst wird).

Und nicht zuletzt bergen avancierte Datenanalysealgorithmen die Gefahr, einen starken institutionellen Anreiz pro Datensammlung zu erzeugen, da sie umso besser funktionieren, je zahlreicher und heterogener die Daten sind, auf die sie zugreifen können. Datenanalyseplattformen wie Palantirs Gotham können ihr volles analytisches Potential beispielsweise nur dann

ausschöpfen, wenn sie auf viele verschiedenen Datentöpfe gleichzeitig zugreifen können (vgl. Egbert 2020).

Entsprechenden Dynamiken muss früh genug Einhalt geboten werden, um weitreichende Rechtsverletzungen zu unterbinden.

Literatur

Behr, Rafael (2018) Rassismus und Diskriminierung im Polizeidienst. *SIAK-Journal* 13: 57-66.

boyd, danah; Crawford, Kate (2012): Critical Questions for Big Data. *Information, Communication & Society* 15(5): 662-679.

Brayne, Sarah (2021): *Predict and Surveil. Data, Discretion, and the Future of Policing*. New York: Oxford University Press.

Egbert, Simon (2020): Datafizierte Polizeiarbeit – (Wissens-)Praktische Implikationen und rechtliche Herausforderungen. In: Hunold, Daniela; Ruch, Andreas (Hrsg.): *Polizeiarbeit zwischen Praxishandeln und Rechtsordnung. Empirische Polizeiforschungen zur polizeipraktischen Ausgestaltung des Rechts*. Wiesbaden: Springer VS, S. 77-100.

Egbert, Simon; Leese, Matthias (2021): *Criminal Futures. Predictive Policing and Everyday Police Work*. London/New York: Routledge.

Ferguson, Andrew Guthrie (2017): *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.

Glaser, Jack (2014): *Suspect Race. Causes and Consequences of Racial Profiling*. Oxford: Oxford University Press.

Glover, Karen S. (2009): *Racial Profiling. Research, Racism, Resistance*. Lanham et al.: Rowman & Littlefield.

Herrnkind, Martin (2014) „Filzen Sie die üblichen Verdächtigen!“ oder: Racial Profiling in Deutschland. *Polizei & Wissenschaft* 15 (3): 35-58.

Kitchin, Rob (2017): Thinking critically about and researching algorithms. *Information, Communication & Society* 20(1): 14-29.

O’Neil, Cathy (2016): *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy*. London: Penguin Books.

Pasquale, Frank (2015): *The Black Box Society. The Secret Algorithms that Control Money and Information*. Cambridge/London: Harvard University Press.

Price, Michael; Hockett, Emily (2017): *Palantir Contract Dispute Exposes NYPD’s Lack of Transparency*, 20. Juli 2017. https://www.brennancenter.org/our-work/analysis-opinion/palantir-contract-dispute-exposes-nypds-lack-transparency [abgerufen am 04.06.2021].

Singelnstein, Tobias (2018): Predictive Policing. Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention. *Neue Zeitschrift für Strafrecht* 1/2018: 1-9.