

Der Knochenjäger im Web 2.0

Jeffery Deaver: The broken window: a Lincoln Rhyme novel. – New York: Simon & Schuster, 2008. 417 S. – ISBN 978-1-416-54997-0: 11,95 EUR. *543 S. – EST: The broken window <dt.>. – ISBN 978-3-7645-0296-6: 19,95 EUR.*

Jeffery Deaver: Der Täuscher. Übersetzt von Thomas Haufschild. – München: Blanvalet, 2009. – „There was, of course, no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Po-

lice plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time.“ – *George Orwell, 1984*

Vor etlichen Jahren bereits erschien der erste Roman einer Reihe mit dem querschnittgelähmten Kommissar namens Lincoln Rhyme und dessen Assistentin Amelia Sachs: „Der Knochenjäger“ (engl.: „The bone collector“), bekannt geworden durch die Verfilmung mit Denzel Washington und Angelina Jolie.

Einige Jahre und Romane weiter:

Rhyme, ein wegen seiner Akribie und zuverlässigen Arbeitsweise weit über die Grenzen der Vereinigten Staaten hinaus geachteter Ermittler, wird von seinen US-amerikanischen Kollegen auch gefürchtet: zu schnell kippt sein Umgangston ins Ruppige, wenn er ungeduldig wird. Zwar ist er ans Bett gefesselt, kann sich vom Halswirbel abwärts nicht mehr bewegen, doch ein Zeigefinger gehorcht ihm noch, und die ganze Technik um ihn herum, Telefon, Computer, etc. hört auf seine mündlichen Befehle. Außerdem hat er die schöne rothaarige Polizistin Amelia Sachs, die für ihn die Tatorte abläuft, die Verdächtigen verhört und den Verbrechern mit höchstem körperlichem Einsatz hinterherjagen kann. Die beiden sind schon länger ein Paar und auch in der Ermittlungsarbeit ein eingespieltes Team.

Rhymes Stärke ist nicht nur das übliche Sammeln von Beweismitteln, Fingerabdrücken und DNA an Tatorten, vielmehr interessiert ihn Sand, Erde, Staub, der nicht an den Tatort gehört und vom Täter herrühren könnte. Er hat eine immense Datenbank angelegt, besitzt die notwendigen Apparaturen in seinem Haus, die diese Art von Spuren untersuchen bzw. in seine chemischen Bestandteile zerlegen können, um so den Herkunftsort des Täters einzukreisen.

Nun wird zufällig sein Cousin, dem er seit der Kindheit brüderlich-herzlich verbunden ist, eines Raubmordes angeklagt, was dieser vehement abstreitet, obwohl alle Beweise wasserdicht sind und gegen ihn sprechen. Rhyme besorgt sich – da er ja befangen ist – auf nicht ganz legalem Weg die Unterlagen. Er kann sich nicht vorstellen, dass sein Cousin, ein vergeistigter Akademiker, ein solches Verbrechen begangen haben könnte. Also sucht er nach ähnlichen Fällen, in denen die Angeklagten als unbescholten galten und ebenfalls verzweifelt ihre Unschuld beteuerten.

Es gibt sie tatsächlich in New York und Umgebung und schnell stellt er einige Gemeinsamkeiten fest: Die Beweise zeigen sich für seine sensible Spürnase als zu deutlich hinterlegt und sie finden sich zudem meist an leicht zugänglichen Orten, z. B. in der Garage oder im Garten. Da hat sich jemand Zugang zu sehr vielen persönlichen Da-

ten verschafft, sowohl vom Opfer als auch vom vermeintlichen Täter und konnte so Spuren beispielsweise des gleichen Rasierschaumes, der gleichen Schuhmarke und -größe und vieles mehr am Tatort hinterlassen, die direkt mit dem Täter in Zusammenhang gebracht werden konnten. Und: Es gab immer einen anonymen Anrufer, der einen Vorfall meldete und ein weggehendes Auto beschrieb. So soll die Polizei zum vermeintlichen Täter finden, aber nicht zu schnell. Bis sie anhand der unvollständigen Nummer erst die infrage kommenden Halter ausfindig gemacht hat, kann der wahre Täter in der Zwischenzeit noch einige Beweismittel vom Tatort beim angeblichen Täter deponieren: etwas Blut des Opfers, ein paar Haare usw.

Die Frage ist nun, wie kann eine einzelne Person in so kurzer Zeit an so viele Informationen herankommen, seine Opfer so gut einkreisen?

Ein Fall von unglaublich klingendem Identitätsklau wird aufgerollt und ebenso schnell wird eine mögliche Quelle ausgemacht, eine Firma namens SSD (Security Systems Data), die sich dem „data mining“ verschrieben hat. Damit ist die systematische Anwendung von Methoden gemeint, die meist statistisch-mathematisch begründet sind, und die auf einen großen Datenbestand mit dem Ziel der Mustererkennung angewandt werden. „Data Mining bedeutet Extrahieren von impliziten, noch unbekanntem Informationen aus Rohdaten. Dazu sollten Computer in die Lage versetzt werden, Datenbanken automatisch nach Gesetzmäßigkeiten und Mustern zu durchsuchen und einen Abstraktionsprozess durchzuführen, der als Ergebnis aussagekräftige Informationen liefert.“ (Institut für Informatik, Univ. Duisburg)

Der Chef von SSD, Andrew Sterling, eine Mischung aus Bill Gates und Steve Jobs, sammelt Daten von amerikanischen Bürgern und verkauft seine Erkenntnisse gewinnbringend an Kunden, die in erster Linie an Käuferprofilen interessiert sind. Andrew stellt bei jeder Gelegenheit die Vorzüge seiner Analysen heraus: sinnvolle Weihnachtsgeschenke, wenn man die Wünsche des zu Beschenkenden zuverlässig erkennen kann, Krankheiten könnten frühzeitig entdeckt werden, die Kreditwürdigkeit einzelner Personen kann durch Analysen und den daraus resultierenden Vorhersagen am Ende doch positiv beantwortet werden, auch wenn die Bank dieses im ersten Moment vielleicht ablehnt, und so vieles mehr!

Von Datenschützern argwöhnisch beäugt, und um den Ruf der Firma besorgt, führt er den ermittelnden Polizisten seine ausgeklügelten Sicherheitssysteme vor, die Daten werden in vielen verschiedenen Abteilungen unabhängig voneinander gespeichert, nur einem kleinen Kreis

von Mitarbeitern ist es möglich, auf alle Daten zuzugreifen. Damit wird der Täterkreis deutlich eingegrenzt. Ein zurate gezogener ehemaliger Mitarbeiter der Firma entwirft ein ganz anderes Bild: nicht das eines fürsorglichen Chefs, den alle Mitarbeiter lieben, sondern das eines undurchschaubaren, machthungrigen, mit allen Mitteln die Konkurrenten ausschaltenden Emporkömmelings.

Aber auch seine engsten Mitarbeiter sind nicht ohne – teils arrogante, teils verhuschte Computerexperten, die ganz selten ein anderes Alibi für den Sonntagnachmittag bieten können, als alleine am Rechner gegessen zu haben.

Man liest die Krimis von Deaver mit Genuss: er baut alle diese informationstechnischen und kriminalistischen Erkenntnisse geschickt in die Handlung ein, ohne belehrend zu wirken. Und ehe man sich versieht, kann man schon wie ein Experte über die neuesten Methoden der Spurensicherung sprechen bzw. die Vor- und Nachteile der personenbezogenen Datenspeicherung erörtern, ebenso die sorglose Preisgabe von persönlichen Daten, ja sogar Fotos, verurteilen – eine Sorglosigkeit, deren Folgen der Nutzer von sozialen Plattformen sich selbst zuzuschreiben hat.

Er fährt dabei zweigleisig: einerseits setzt er ein Computer-Kid, einen bei der Polizei beschäftigten Hacker, auf die Firma an, der versucht, in das System einzudringen, um mehr über deren Methoden und die Beschäftigten zu erfahren. Gleichzeitig wird aber konventionelle Polizeiarbeit geleistet: Befragung von Verdächtigen mit den üblichen psychologischen Techniken, Überprüfung von Alibis, Sicherung von Beweismitteln, die vom eigentlichen Täter herrühren könnten (Stichwort: Staub!). Und nicht zuletzt kommt der Instinkt des Ermittlers ins Spiel, der von keiner noch so ausgetüftelten Maschine ersetzt werden kann.

Der Täter selbst fühlt sich langsam eingekreist, immer mal wieder wird ein kurzer Teil der Handlung aus seiner Perspektive vorangetrieben, um

einen Einblick in seine Psyche zu bekommen, ohne dass seine Identität preisgegeben wird. Man hat als Leser den Eindruck, dem Täter immer näher zu kommen, und wird am Schluss doch überrascht davon, wer er nun tatsächlich ist.

Erschreckend sind die im Laufe der Handlung deutlich werdenden Ausmaße, die das Sammeln von personenbezogenen Daten annehmen kann: sie sind durchgehend realistisch gezeichnet, die technischen Möglichkeiten sind alle vorhanden. Noch erschreckender wirkt die Schilderung der Auswirkungen, die ein möglicher Missbrauch bewirken könnte, als der in die Enge getriebene Täter schließlich auch die Ermittler in sein Netz verwickelt. Denn: werden Informationen zuungunsten Einzelner manipuliert, so ist das nicht einfach nachzuweisen und zurückzufolgen, schließlich glaubt man den Unterlagen aus dem Computer im Zweifelsfall eher als der ihre Unschuld betuernde Person. In den USA noch viel stärker als hier diskutiert wurde z. B. die Beschränkung der Bürgerrechte durch den umstrittenen „patriot act“, die online-Durchsuchungen und Überwachungen aller Art erlaubte, die allesamt mit dem Anschlag auf das World Trade Center und der Terrorismusbekämpfung begründet werden. Um den Einzelnen zu schützen, müsse dieser eben so viel wie möglich von sich preisgeben, um seine Unverdächtigkeit zu belegen.

„The privacy and dignity of our citizens [are] being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen – a society in which government may intrude into the secret regions of a [person’s] life.“ – *Supreme Court Justice William O. Douglas*

Gespensisch, wie George Orwells Visionen aus „1984“ in der Gegenwart von 2008 angekommen sind.

*Birgit Fernengel –
(Die Neue Sammlung München, Bibliothek)*