Christian Rückert: Digitale Daten als Beweismittel im Strafverfahren

von Prof. Dr. Anja Schiemann

2023, Mohr Siebeck, ISBN: 978-3-16-162216-8, S. 834, Euro 164,00.

Schon in der Einleitung seiner umfangreichen Habilitationsschrift kritisiert *Rückert* nicht nur den Mangel an gesetzlichen Dateneingriffsbefugnissen sowie die mangelhafte Systematisierung der bestehenden Dateneingriffsbefugnisse, sondern auch die fehlenden Leitlinien und Auslegungskriterien für die Rechtsanwendung. Letzteres setzt sich die Untersuchung dann auch zum Ziel, nämlich möglichst allgemeingültige Leitlinien und Auslegungskriterien für strafprozessuale Dateneingriffe zur Beweisdatengewinnung herauszuarbeiten. Dabei hat *Rückert* den Anspruch, dass diese Leitlinien und Kriterien dem Gesetzgeber Hilfestellung bei der Schaffung neuer Normen und einer anzustrebenden Re-Systematisierung der strafprozessualen Dateneingriffsbefugnisse geben und darüber hinaus auch dem Rechtsanwender als Auslegungskriterien für die Anwendung der Befugnisnormen dienen.

Die Habilitationsschrift behandelt dabei drei Themengebiete. In den ersten fünf Kapiteln werden allgemeingültige Vorgaben und Leitlinien für die Schaffung und Anwendung strafprozessualer Dateneingriffsbefugnisse zur Beweisdatengewinnung aus dem Verfassungsrecht erarbeitet. In Kapitel 7 werden diese Vorgaben und Leitlinien den entsprechenden Anforderungen aus dem Europäischen Recht gegenübergestellt und in Kapitel 8 werden die Probleme rund um die Verwendung von Daten und Datenverarbeitungsergebnissen als Beweismittel im Strafverfahren behandelt.

Rückert kommt zunächst zu dem wenig überraschenden Ergebnis, dass die deutschen Grundrechte umfassenden Schutz für digitale Daten vor strafprozessualen Zugriffen gewähren. Geschützt werden die Vertraulichkeit von Datenübertragungen durch das Telekommunikationsgeheimnis, die Integrität und Vertraulichkeit von datenverarbeitenden Systemen durch das IT-System-Grundrecht und die Selbstbestimmung über personenbezogene Daten im Übrigen durch das Recht auf informationelle Selbstbestimmung. Dabei werden die Eingriffsbeschränkungen und verfahrensrechtlichen Sicherungen aus der Rechtsprechung zu einzelnen Grundrechten auf andere Grundrechte übertragen, so dass es keine Eingriffsbeschränkungen, die „exklusiv" nur für Eingriffe in ein bestimmtes Grundrecht vorgesehen sind, gäbe. Die Erforderlichkeit und Ausgestaltung bestimmter Eingriffsschwellen und Schutzmechanismen richte sich vielmehr hauptsächlich nach der Intensität des durch die strafprozessuale Eingriffsbefugnis gewährten Zugriffs auf Daten. Es komme also weder für die Bestimmung der konkreten Eingriffsintensität noch für die notwendigen, von Gesetzgeber und/oder Rechtsanwender zu beachtenden Eingriffsschwellen und die zu ergreifenden Schutzmechanismen für die Betroffenen darauf an, welches Grundrecht tangiert ist. Vielmehr gehe es darum, welche Eingriffstiefe der jeweilige Dateneingriff aufweise. Auch dabei sei nicht das betroffene Grundrecht entscheidend, sondern es komme auf abstrakte, auf alle Arten von Datenerhebungs- und -auswertungseingriffen anzuwendende Schwerekriterien an. Dabei überträgt nicht nur das *BVerfG,* sondern auch die ihm folgende h.M. in der Literatur die Schwerekriterien zur Eingriffstiefenbestimmung und die notwendigen Eingriffsschwellen und Schutzmechanismen in zunehmendem Maße zwischen den einzelnen Grundrechten, so dass der Einschlägigkeit der unterschiedlichen Grundrechte nur noch eine untergeordnete Rolle bei der Bestimmung der Eingriffstiefe und der Eingriffsschwellen zukomme.

Die herausgearbeiteten verfassungsrechtlichen Vorgaben für strafprozessuale Dateneingriffe systematisiert der Verfasser dann in einem nächsten Schritt. Als absolute Eingriffsgrenzen seien die absoluten Erhebungs- und Verwertungsverbote sowie Löschpflichten hinsichtlich solcher Daten zu sehen, die Informationen über den sog. Kernbereich privater Lebensführung enthalten, das Verbot der Rundumüberwachung und das Verbot der Persönlichkeitsprofilbildung. Auch bei digitalen Daten kommt es nach der Auffassung von *Rückert* allein auf den inhaltlichen Kernbereichsbezug an.

Die weiteren Eingriffsschwellen und Schutzmechanismen, die vom *BVerfG* für die Ausgestaltung und Anwendung von strafprozessualen Dateneingriffsbefugnissen verlangt werden, könnten jeweils als spezielle Ausprägungen des Verhältnismäßigkeitsprinzips beschrieben werden. Während sich der Grundsatz des Vorrangs der offenen gegenüber der heimlichen Ermittlungsmaßnahme als Ausprägung der Erforderlichkeit und des sog. relativ mildesten Mittels beschreiben lasse, stellten die vom *BVerfG* geforderten Eingriffsschwellen und die notwendigen Schutzmechanismen jeweils Abwägungsgesichtspunkte bei der Abwägung der Grundrechtseingriffsintensität mit dem Strafverfolgungsanspruch des Staates auf Ebene der Verhältnismäßigkeit im engeren Sinne dar. Daher erscheint laut *Rückert* eine Systematisierung und Ausarbeitung von zwei entscheidenden Gesichtspunkten der Verhältnismäßigkeitsprüfung angezeigt. Denn bisher seien keine allgemeingültigen Kriterien erarbeitet worden, mit denen sich die Eingriffsintensität einer strafprozessualen Datenerhebung und Datenverarbeitung auf der einen und des Gewichts des staatlichen Strafverfolgungsanspruchs auf der anderen Seite transparent, nachvollziehbar und damit überprüfbar bestimmen lasse. Zudem fehle es an einer Systematisierung, wie die Eingriffsintensität mit der Notwendigkeit einzelner Eingriffsschwellen und Schutzmechanismen zusammenhängt. Daher macht es sich der Ver-

fasser im weiteren Verlauf seiner Arbeit zur Aufgabe, genau dies zu entwickeln.

Die Kriterien zur Messung bzw. Bestimmung der Eingriffsintensität eines strafprozessualen Dateneingriffs zur Beweisdatengewinnung wurden in Kapitel 3 entwickelt. Unter dem Oberbegriff der „Art der Daten" bestimmen laut Verfasser die Stärke des Personenbezugs, die Einordnung der Daten in die Sozial-, Privat- oder Intimsphäre die Wahrscheinlichkeit, mit der aus den Daten ein (partielles) Persönlichkeitsprofil erstellt werden kann sowie die Beantwortung der Frage, ob an den Daten ein besonderes, gesellschaftlich anerkanntes Vertraulichkeitsinteresse bestehe. Nur eine indizielle Rolle komme dagegen der Einordnung der Daten in die Kategorien der Inhalts-, Verkehrs-, Nutzungs-, Bestands- oder Zugangsdaten zu. Hinsichtlich der Menge der Daten komme es nicht auf die physikalische Menge, sondern auf die Informationsvielfalt und -dichte an, die sich aus den Daten gewinnen lasse. Beim Intensitätskriterium der Zugänglichkeit der Daten ließen sich drei Intensitätsstufen unterscheiden, nämlich öffentlich zugänglich, für einen begrenzten Empfängerkreis zugänglich und für keinen Drittzugriff bestimmt. Die Lesbarkeit der Daten habe eingriffsintensivierende Wirkung.

Hinsichtlich des Intensitätsfaktors der Heimlichkeit einer Maßnahme wurden vier Eingriffsstufen mit steigender Intensität definiert: der offene Eingriff mit aktueller Kenntnis des Betroffenen, der offene Eingriff ohne aktuelle Kenntnis des Betroffenen, ein bewusst heimlicher Eingriff und bewusst heimlicher Eingriff ohne Hinzuziehung eines Intermediärs. Beim Kriterium der Streubreite unterscheidet der Verfasser dagegen drei Stufen. Am niedrigsten sei die Intensität bei der Beschränkung auf Daten einzelner Tatverdächtiger, höher bei einer unbeabsichtigten Miterhebung der Daten nicht Tatverdächtiger und am höchsten bei Maßnahmen, die gezielt die Daten vieler, auch nicht tatverdächtiger Personen erfassen. Für automatisierte Maßnahmen arbeitete der Verfasser als entscheidende Oberkriterien zur Eingriffstiefenbestimmung die Richtigkeitswahrscheinlichkeit und die Nachvollziehbarkeit der verwendeten Methoden heraus.

Bei den Kriterien der Dauer der Maßnahme, der Sicherheit der Daten in staatlicher Obhut und der Veränderung an bestehenden Datensätzen durch die Eingriffsmaßnahme lägen sog. Je-desto-Beziehungen vor. Je länger die Maßnahme, desto intensiver der Eingriff, je systemrelevanter, je weniger rückgängig machbar und je größer die Veränderung, desto schwerwiegender der Eingriff. Je schlechter die IT-Sicherheit der Daten in staatlicher Obhut, desto schwerer wiege der Verarbeitungseingriff. Außerdem beeinflusse die Kenntnis bzw. Unkenntnis der Strafverfolgungsbehörden hinsichtlich des Vorliegens bestimmter Eingriffsschwerekriterien die Intensität. Abstufen lasse sich die Schwere hier danach, ob die Unkenntnis auf Fahrlässigkeit beruhe oder Kriterien bewusst nicht berücksichtigt werden.

Sodann werden unter dem Oberbegriff der Anlassbezogenheit aus Sicht des Betroffenen weitere Schwereabstufungen definiert. Am wenigsten schwer wiege hier der Eingriff, wenn der Anlass hierfür in einem rechtswidrigen, steuerbaren Verhalten des Betroffenen liege. Ein höheres Gewicht liege vor, wenn als Anlass ein rechtmäßiges, aber steuerbares Verhalten genügt, noch höher sei das Eingriffsgewicht, wenn nicht steuerbares Verhalten zugrunde läge. Am intensivsten sei der Eingriff dann, wenn er völlig anlasslos, d.h. ohne Anknüpfungspunkt im Verhalten des Betroffenen erfolge.

Schließlich werde die Eingriffstiefe davon bestimmt, welche Folgen der Eingriff für den Betroffenen außerhalb der bloßen Verarbeitung seiner persönlichen Daten habe. Hier unterscheidet *Rückert* nach zwei Schwerestufen, nämlich der Stigmatisierung des Betroffenen sowie private und berufliche Nachteile für den konkret Betroffenen und eine allgemeine Diskriminierung der Personengruppe, der der Betroffene angehört. Im Übrigen werde die Eingriffstiefe ebenfalls von mehreren Je-desto-Beziehungen bestimmt. Der Eingriff wiege umso schwerer, je schwerer die Straftat ist, wegen derer die Ermittlungsmaßnahme durchgeführt wird, je geringer die Richtigkeitsgewähr des Ergebnisses, auf das die stigmatisierende Maßnahme gestützt wird und je mehr verschiedene Behörden und Personen innerhalb der Behörden Kenntnis haben.

Nachdem der Verfasser die Kriterien herausgearbeitet hat, wird eine relative ordinale Ordnung der Intensitätskriterien für strafprozessuale Dateneingriffe erstellt. Diese werden in Tabellenform zusammengestellt (S. 315 ff. sowie S. 751 ff.), so dass das „maximal erreichbare Maß an Rationalisierung" erreicht werde (S. 749). Aus den Erkenntnissen werden dann in Kapitel 5 die abstrakt und konkret zu erreichenden Eingriffsschwellen für strafprozessuale Dateneingriffe und zu ergreifende Schutzmechanismen abgeleitet. Ziel ist die Entwicklung eines „Baukastensystems" (S. 399) der aus dem Verhältnismäßigkeitsprinzip, den Kriterien zur Bestimmung der Eingriffsintensität und des Gewichts des staatlichen Strafverfolgungsanspruchs abzuleitenden Schutzmechanismen und Eingriffsschwellen. Dabei wurden die Eingriffsschwellen und Schutzmechanismen in unterschiedliche Kategorien eingeteilt. Zu den unabhängig von der Eingriffsintensität geltenden Schutzmechanismen zählen Grundsätze der Normenklarheit und -bestimmtheit, der Zweckbindung und -änderung inklusive der Pflicht zur Kennzeichnung und das Verbot der Rundumüberwachung, Gewährleistung der IT-Sicherheit für vom Staat gespeicherte und verarbeitete Daten, die Vermeidung bzw. Rückgängigmachung von Veränderungen an IT-Systemen der Bürger durch staatliche Eingriffe, die Pflicht zur Löschung bzw. Sperrung von personenbezogenen Daten, wenn diese nicht mehr zur Strafverfolgung oder anderen legitimen staatlichen Zwecken benötigt werden sowie die Pflicht zur Berichtigung unrichtiger personenbezogener Daten.

Daneben wurden Schutzmechanismen identifiziert, die in Abhängigkeit von spezifischen Eingriffskriterien gelten.

Hierzu wurde wieder übersichtlich in Tabellenform die Abhängigkeit der Schutzmechanismen von Eingriffsschwerekriterien zusammengestellt (S. 761). Die übrigen Schutzmechanismen und Eingriffsschwellen hängen dann in ihrer Anwendbarkeit von der Gesamtintensität des strafprozessualen Dateneingriffs ab. Auf Seiten der Eingriffsschwellen sind dies Anforderungen an die Qualität der verfolgten Straftat, Mindestanforderungen an die Stärke des Tatverdachts, Beschränkungen des Kreises der zulässigen Maßnahmenadressaten und Vorgaben hinsichtlich der Auffindewahrscheinlichkeit. Zu den Schutzmechanismen gehören Beschränkungen der Dauer der Maßnahme, Vorgaben für die Form der Anordnung der Maßnahme und Subsidiaritätsklauseln als vertypte Erforderlichkeitsschranken.

Im Anschluss überprüft der Verfasser die erarbeiteten Eingriffsschwellen und Schutzmechanismen darauf, ob diese durch den Gesetzgeber für den Bereich der strafprozessualen Dateneingriffe zur Gewinnung von Beweisdaten bereits hinreichend umgesetzt wurden. Auch diese gesetzlichen Regelungen werden in Tabellenform zusammengefasst (S. 763). Soweit es keine explizite gesetzliche Regelung gab, wurde überprüft, ob durch Auslegung gewinnbare Eingriffsschwellen- und Schutzmechanismusregelungen vorhanden sind. Hier wurden §§ 64 und 71 BDSG identifiziert.

Schließlich wird festgestellt, dass es einige Eingriffsschwellen und Schutzmechanismen gibt, für die keine oder nur unzureichende gesetzliche Regelungen existieren. Hier unterbreitet der Verfasser Änderungs- und Regelungsvorschläge, die in den Schlussbetrachtungen ebenfalls noch einmal in Tabellenform zusammengetragen werden (S. 764 ff.). Letztlich wird hervorgehoben, dass einige der Eingriffsschwellen und Schutzmechanismen auch ohne eine entsprechende gesetzliche Regelung unmittelbar kraft Verfassungsrechts gelten. Dies sei für die verfassungsrechtlichen Schranken-Schranken der gerechtfertigten Grundrechtseinschränkung wie dem Grundsatz der Normenklarheit und Bestimmtheit ebenso anzunehmen wie für den Schutz des Kernbereichs und die Verbote der Persönlichkeitsprofilbildung und die Rundumüberwachung. Schließlich ergäbe sich die zwingende Anwendung einiger Eingriffsschwellen und Schutzmechanismen unmittelbar aus dem Verhältnismäßigkeitsgrundsatz. Dies gelte etwa für die Pflicht zur Durchführung der Dateneingriffe in möglichst unauffälliger Weise zur Vermeidung beruflicher und privater Stigmatisierung der Betroffenen, die absoluten Grenzen der Dauer der Maßnahme und die Subsidiarität von heimlichen gegenüber offenen Dateneingriffen.

Die Notwendigkeit der einzelnen Eingriffsschwellen und Schutzmechanismen hänge dabei bis auf wenige absolut geltende Ausnahmen vom Ausgang der vorzunehmenden Verhältnismäßigkeitsprüfung ab. Eingriffsschwellen dienten dabei der Erhöhung des Gewichts des Strafverfolgungsanspruchs, die Schutzmechanismen der Absenkung der Eingriffsintensität. In einigen Fällen sei dabei die Ergreifung von Schutzmaßnahmen und das Prüfen von Eingriffsschwellen aufgrund des dem Erforderlichkeitsgrundsatz innewohnenden Prinzips des relativ mildesten Mittels zwingend. Ebenso müssten Schutzmaßnahmen ergriffen werden, wenn diese nicht zu einem Effektivitätsverlust der Dateneingriffsmaßnahme führten. Im Übrigen dienten die Eingriffsschwellen und Schutzmechanismen zur Feinregulierung und damit zur Gewährleistung der Verhältnismäßigkeit der strafprozessualen Dateneingriffsbefugnisse und der konkret vorgenommenen Dateneingriffe. *Rückert* regt an, dass sich Gesetzgeber und Rechtsanwender in diesem Fall aus den von ihm vorgeschlagenen Maßnahmen wie in einer Art strafprozessualem „Baukastensystem“ bedienen, um die Verhältnismäßigkeit zu wahren (S. 767). Insofern werde dadurch zu einer Rationalisierung und besseren Nachvollziehbarkeit und Überprüfbarkeit von Verhältnismäßigkeitsentscheidungen beigetragen.

Der Verfasser stellt aber auch klar, dass die Schaffung neuer Eingriffsbefugnisse der schnellen technologischen Entwicklung zwangsläufig hinterherhinken würde. Daher behelfe sich die Praxis mit einer kreativen Auslegung. Hier werden Grenzen der erweiternden Auslegung von Ermittlungsbefugnissen zur Ermöglichung neuartiger strafprozessualer Dateneingriffe aufgezeigt sowie Möglichkeiten und Grenzen der Schaffung technikoffener Eingriffsgrundlagen beschrieben.

Kapitel 7 beleuchtet dann die europarechtlichen Vorgaben für die Schaffung und Auslegung strafprozessualer Dateneingriffsbefugnisse, bevor in Kapitel 8 zentrale Probleme der Verwendung von Daten und Datenanalysen als Beweismittel in der Hauptverhandlung beschrieben werden. Leserfreundlich werden die gewonnenen Erkenntnisse in den Schlussbetrachtungen des Kapitels 9 zusammengefasst.

Es kann nicht Aufgabe einer Rezension sein, inhaltlich eine so umfangreiche Habilitationsschrift wie diese auch nur annähernd wiederzugeben. Aber es ist, so hoffe ich, deutlich geworden, dass diese Arbeit nicht nur sehr dezidiert die bestehenden Grundlagen und Eingriffsbefugnisse sowie Auslegungsgesichtspunkte zur Erhebung und Verwertung digitaler Beweismitteldaten aufzeigt, sondern auch den Finger in die Wunde der mehr als unzureichenden Rechtsgrundlagen legt und dann nicht weniger bietet, als allgemeingültige Leitlinien und Auslegungskriterien für Rechtsanwender und Gesetzgeber an die Hand zu geben. Insofern wird das Anfangs gegebene Versprechen des Verfassers eingelöst, so dass es, auch durch die anschaulichen Tabellen ein Leichtes ist, sich im Dickicht des unübersichtlichen Gestrüpps an Vorschriften zurechtzufinden. Möge hinzukommen, dass das von *Rückert* identifizierte Regelungsdefizit vom Gesetzgeber aufgegriffen und in Rechtsform gegossen wird. Eine Systematisierung und Neujustierung der Vorschriften der Dateneingriffsbefugnisse ist längst überfällig.