Dr. Ralf Dietrich, Stuttgart

Die Rechtsschutzbegrenzung auf besonders gesicherte Daten des § 202 a StGB[1]

A. Hinführung

Das Ausspähen von Daten, auch Datenspionage genannt, oder das verwandte Hacking[2] sind *die* Delikte des Informationszeitalters. Doch sind nicht alle elektronischen Daten per se vor dieser Bedrohung strafrechtlich geschützt. Nur Daten, die bereits faktisch vor Zugang gesichert sind, wird gemäß § 202 a StGB[3] der Strafrechtsschutz gewährt. Passwortabfragen werden als beispielhafte Sicherungen genannt. Der Grund der Rechtsschutzbegrenzung ist sowohl von wissenschaftlich-theoretischem wie von praktischem Interesse, da er den Informationssphärenschutz in der digitalen Welt wesentlich konturiert sowie für Normauslegung und damit Rechtsanwendung von direkter Relevanz ist. Dieser Grund soll daher untersucht werden.

B. Anriss zur Bedeutung der Norm und ihrer Einschränkung

Diskretionsbedürfnisse, etwa an Privatsphäre[4] oder Betriebsgeheimnissen, und verschiedenste Informationsinteressen stehen sich schon von jeher gegenüber[5]. Elektronische Datensicherung und Datenspionage sind ihre modernen Erscheinungsformen[6] und § 202 a die zentrale Norm für deren strafrechtliche Einordnung. § 202 a erfasst in Form des Rechtsguts des formalen Geheimbereichs die eben genannten Diskretionsbedürfnisse und grenzt sie vom straffreien Informationsinteresse ab. Doch sein Verständnis hinkt aktuellen Entwicklungen hinterher[7] und findet trotz jüngerer Novellierung[8] unberechtigterweise wenig Beachtung.

Gründe lassen sich vermuten[9], insb. dass es in der Natur der Geheimnisdelikte liegt, dass sie im Dunkeln bleiben. Dies strebt schon der Täter an, oft aber auch das Opfer, sollte es die Tat überhaupt entdecken. Auch mag die Materie aufgrund ihres technischen Gepräges der juristischen Wertung schwer zugänglich erscheinen.

Die Rechtsschutzbegrenzung der Norm, erst technisch gesicherte Daten durch das Strafrecht zu erfassen, bedeutet zunächst Einschränkung des Strafrechtsschutzes für das Opfer und der Drohung für den Täter; weiter dass der Schutzbereich durch den Dateninhaber beeinflussbar ist; zudem dass derjenige rechtlich schutzlos bleibt, der technisch nicht schützen will oder kann, und schließlich dass der Strafverfolgungsapparat erst einschreitet, wenn ein gewisses Maß vorheriger Schutzaktivität stattfand. Diese Begrenzung formt die Privat- oder Geschäftsgeheimnissphäre im digitalen Zeitalter.

C. Analyse und Kritik der allgemeinen Ansicht

Nach ganz allgemeiner Ansicht liegt der Grund für die Schutzbereichseinschränkung auf besonders gesicherte Daten darin, dass sich in der Sicherung ein besonderes Geheimhaltungsbedürfnis des Dateninhabers dokumentiere[10]. Diese Ansicht sei hier Dokumentationstheorie genannt. Von Nuancierungen abgesehen, waren ihre Ausführungen selten weit oder stark vertiefend. Die gegebene Grundthese schien zu genügen. Ob sie (heute noch) genügt, soll überprüft werden.

Eine strafrechtliche Theorie dient einem Zweck: der Beantwortung der Frage, ob bestraft wird oder nicht. Daher sind an sie hohe Anforderungen zu stellen. Nicht nur muss das Ergebnis wertungsmäßig richtig sein. Es muss auch klar und sicher sein. *Nullum crimen, nulla poena sine lege stricta et certa*. An diesem Anspruch muss sie sich messen lassen. Daran sei vor der inhaltlichen Analyse erinnert. Zur nötigen Klarheit gehört, dass die Theorie in ihren Kriterien abschließend sein muss. Unbenannte Kriterien, Ausnahmen, Einschränkungen soll es zu Gunsten des Täters schon nicht geben, zu seinen Lasten darf es sie nicht geben. Die Theorie wäre vielleicht in sich schlüssig, doch ihr Nutzen, die sichere Rechtsanwendung, eingeschränkt. Der Ausspähwillige, oder neutraler formuliert, Auslesewillige (denn es gibt durchaus begrüßens-

1) Die Arbeit greift Thesen der Dissertation des *Verf.* auf, die am Lehrstuhl des Doktorvaters *Prof. Dr. H.-L. Günther* der Universität Tübingen entstanden und unter dem Titel „Das Erfordernis der besonderen Sicherung im StGB, § 202 a StGB" in der von *Prof. Dr. Dr. F.-C. Schroeder* und *Prof. Dr. A. Hoyer* herausgegebenen Reihe „Strafrechtliche Abhandlungen" 2009 bei Duncker&Humblot erschienen ist. Die Arbeit wurde mit dem *Reinhold-und-Maria-Teufel-Preis* ausgezeichnet.

2) Hacking zielt strenggenommen nur auf das sportlich motivierte „Knacken" einer Sicherung, nicht auf das Auslesen von Daten.

3) Paragraphenangaben beziehen sich in der Folge auf das StGB.

4) Zum Begriff „Privat", *Dietrich* (o. Fn 1), S. 171 ff. mwN.

5) *Dietrich* (o. Fn 1), Teil 1 Abschn. C, S. 103 ff. mwN.

6) Vgl. *Ernst* NJW 2009, 1320.

7) *Dietrich* (o. Fn 1), S. 27 ff.; zu Gedanken *de lege ferenda* ebda. S. 54 ff.

8) 41. StrÄndG; dazu *Ernst* DS 2007, 335 f.; *Schumann* NStZ 2007, 675 f.; *Gröseling/Höfinger* MMR 2007, 549 f., 626 f. Zur Normhistorie HK-GS-*Tag* § 202 a Rn 1.

9) Zu möglichen Gründen *Dietrich* (o. Fn 1), S. 20 ff.

10) Schon BT-Dr 10/5058, S. 29; stellvertretend S/S-*Eisele* § 202 a Rn 7.

werte Informationsinteressen), soll schon im Vorfeld wissen können, ob ihm das strafrechtliche Schwert als gesellschaftliche *ultima ratio* droht oder nicht. Auch der Dateninhaber ist faktisch Normadressat, er soll wissen, ob sein Interesse vom Strafrecht erfasst wird. Und letztlich muss der Richter wissen, ob das Ausspähen von Daten im konkreten Fall noch straffrei ist, weil der aufgefundene Sicherungsmechanismus den Kriterien des § 202 a nicht entspricht – oder ob er zur Strafe verurteilen muss. Wer eine Theorie zur Beantwortung der Frage der Strafbarkeit aufstellt und nach ihrer Anwendung zu keinem klaren Ergebnis kommt, hat die selbst gestellte Aufgabe nicht erfüllt. Wenn die Dokumentationstheorie zur Sicherung sagt, sie müsse ein besonderes Geheimhaltungsinteresse dokumentieren, dann behauptet sie zugleich, dass einer Sicherung genau eine solche Dokumentation valide entnommen werden kann.

I. Ermittlung impliziter Aussagen der allgemeinen Ansicht

Die Dokumentationstheorie impliziert zwingend dreierlei: Erstens, dass es auf die Dokumentation als solche des Geheimhaltungsinteresses überhaupt ankommt. Dies erscheint zunächst banal und ist doch hochrelevant.

Zweitens fordert der Wortlaut zwar Sicherung, aber diese Forderung wird mit der darin liegenden Dokumentation begründet. Wenn der Gesetzgeber und ihm folgend die allg. Ansicht letztlich auf Dokumentation abstellen, ist doch fraglich, warum sie diese nicht direkt normativ fassen, etwa „. . .*Daten, an denen ein besonderes Geheimhaltungsbedürfnis dokumentiert wurde* . . .“. Dies impliziert, dass die geforderte Dokumentation gerade in Form einer Sicherung vorliegen muss.

Drittens, und vor allem: Die Dokumentationstheorie besagt zur Sicherung, sie dokumentiere ein besonderes Geheimhaltungsinteresse. Da sie rechtspraktische Bedeutung haben will zur Beurteilung, ob ausgelesene Daten im Normsinn technisch gesichert und damit von § 202a erfasst wurden, behauptet sie zwingend zugleich, dass einer vorliegenden Sicherung genau eine solche Dokumentation valide entnommen werden kann.

Keine der impliziten Aussagen wurde explizit in der Literatur formuliert oder begründet. Entweder kann diese Begründungsabsenz daran liegen, dass diese Aussagen nicht bewusst erkannt wurden und daher kein Anlass ihrer Begründung gesehen wurde. Dann soll versucht werden, an die Stelle eines möglicherweise durchaus berechtigt gefühlten, unausgeprochenen Judizes eine analytische Begründung treten zu lassen. Oder kann diese Absenz daran liegen, dass die Begründungen als offensichtlich und weiterer Worte überflüssig angesehen werden?

Dem wäre schon für die erste These entgegenzuhalten, dass es etliche Rechtsgüter gibt, die auch ohne Dokumentation eines besonderen Interesses daran geschützt werden. So wird etwa das Eigentum geschützt, auch wenn es nicht vor Diebstahl gesichert wird. Auf die Geheimsphäre bezogen, könnte die Notwendigkeit der elektronischen Dokumentation dann gerechtfertigt sein, wenn auch schon in der analogen Welt eine Notwendigkeit einer Dokumentation bestünde und sich dort in sozialen Normen begründete, wenn also Dokumentation von jeher konstitutives Merkmal ist, damit Geheimhaltungsinteressen anerkannt werden. Zu untersuchen ist also erstens, ob es überhaupt zunächst dokumentierter Abgrenzungen zur sozialen Anerkennung der Privatsphäre bedarf.

Zur zweiten Frage, warum diese Dokumentation gerade in der Form der Sicherung vorzuliegen hat, ist zu untersuchen, ob auch dies entweder schon sozial hergebracht ist, und wenn nicht, ob etwa aufgrund spezifischer Beschränkungen in der digitalen Welt alleine die Sicherung als taugliche Dokumentationstechnik zur Verfügung steht.

Die ersten beiden Aussagen, dass und wie Geheimhaltungsbedürfnisse dokumentiert werden, können mittels einer sozialpsychologischen Untersuchung kritisch betrachtet werden. Der dritten Aussage, dass aus dem Vorliegen einer elektronischen Sicherung auf ein dahinterstehendes Geheimhaltungsbedürfnis geschlossen werden kann, ist sich danach in einem gesonderten Gedankengang zu nähern. Dieser soll jene Behauptung an der technischen Wirklichkeit, der sozialen Üblichkeit und der Gesetzessystematik messen.

II. Sozialpsychologische Kritik der Übertragung des Informationssphärenschutzes in die digitale Welt

Gesetzliche Normen sollen grds. kein aliud zu sozialen Normen sein, sondern sich vielmehr auf jenen gründen und sie rechtlich forcierend fortschreiben. Dies gilt auch für das Strafrecht[11]. Eine andere gesetzgeberische Intention ist auch für den Privatsphärenschutz weder bekannt noch erkennbar und auch für § 202 a nicht behauptet worden. Wenn dem so ist, dann ist kein Grund ersichtlich, bei der Fortschreibung nicht auf „Originalgetreue“ zu zielen. Anders herum müssen die Übertragungsergebnisse eine Fundierung in ihrem Ursprung haben. Abweichungen sind jedenfalls zu begründen. Zur Erkenntnis, ob das Fordern einer Sicherung eine solche Abweichung ist, sei hier der Blick auf den Ursprung der Fortschreibung gerichtet: die Privatheit.

Gefestigte sozialpsychologische Erkenntnisse zur Privatheit liegen vor. Sie sehen sie als „kreatürliches Grundbedürfnis“ nach Distanz, Einsamkeit und Für-sich-sein[12]. Dieses Bedürfnis wird letztlich durch Regulative des Informationsflusses realisiert[13]. Mittel zum Regulativzweck ist regelmäßig eine räumlich-territoriale Abgrenzung oder Marke. Diese kann aus physisch wirksamen Wehren (etwa Zäunen, Vorhängen) bestehen. Sie kann – und dies ist der häufigere Fall – aber auch rein symbolischer Art bleiben[14], wie etwa eine gezogene Linie oder ein Schild. Sie ist bevorzugt territorial[15], kann aber notfalls auch durch Stimmsenkung, Blickabwenden oder Ähnliches realisiert werden. Das Erfordernis der Dokumentation an sich ist also durchaus begründbar. Was die Art der Dokumentation anbelangt, so lässt sich eine räumliche Linie aber um elektronische Daten in einer „Datenwolke“, vor allem wenn man an das Internet denkt, kaum ziehen. Wo Daten loziert sind, ist in jener elektronischen Welt irrelevant und auch für den versierten Nutzer meist unbekannt. Die Fortschreibung in die elektronische Welt benötigt daher ein Substitut für die regelmäßig räumlichen Konturen der Privatheit. Eine Konturierung kann in elektronischen Sicherungen gesehen werden[16]. Dementsprechend wurde, diese

11) *Dietrich* (o. Fn 1), S. 165 ff. und schon *Bringewat* Grundbegriffe, Fn 40 f., S. 30 f.; *Jescheck/Weigend* StrafR AT, § 8, 2, S. 64; LK-*Jescheck* 11. Aufl., Einl. Rn 1 ff.; *Schmidhäuser* Sinn der Strafe, S. 26; *Maurach/Zipf* StrafR AT/1, § 7 Rn 1 ff.

12) *Schünemann* ZStW 90 (1978), 27; *Eibl-Eibelsfeldt* Verhaltensforschung, S. 306 ff.

13) *Dietrich* (o. Fn 1), S. 169 ff.; *Altman* Social behaviour, S. 18; vgl. auch *Van den Haag* On Privacy, S. 149; *Simmel* Privacy, S. 72; *Halmos* Solitude and Privacy, S. 102; *Margulis* Journal of Social Issues (JSI), 33/3 (1977), 5, 10; *Mogel* Umwelt, S. 58 f. und jünger: *Gifford* Environmental psychology, S. 171, 187 f.

14) *Dietrich* (o. Fn 1), S. 177 f.; *Mogel* Umwelt, S. 59; *Eibl-Eibelsfeldt* Humanethologie, S. 480. Vgl. auch *Fischer/Stephan* in *Kruse* Ökologische Psychologie, S. 166 ff.; *Sommer* Personal Space, S. 26 ff.; S. 45 ff.

15) *Dietrich* (o. Fn 1), S. 176 mwN.

16) Vgl. *Arzt/Weber/Hilgendorf* StrafR BT, 2009, § 8 Rn 50.

Analogie bemühend, § 202 a auch als Tatbestand des elektronischen Hausfriedensbruchs bezeichnet[17]. Doch kennt die digitale Welt auch noch andere Möglichkeiten der Dokumentation: Es ist möglich, an Daten ein Geheimhaltungsinteresse zu dokumentieren, ohne sie zu sichern. Beispielsweise schlichte Bezeichnung im Dateinamen als „geheim", „privat" oder durch elektronische Attribuierung[18]. Die Dokumentation gerade in Form der Sicherung zu fordern, kann also nicht dadurch begründet werden, dass die elektronische Sicherung die einzige mögliche technische Art und Weise der Dokumentation wäre.

Die elektronische Sicherung als Entsprechung oder zwingende Fortführung hergebrachter Dokumentationstechniken zu sehen, ginge daher fehl. Sie ist zwar kein *aliud*, sie ist jedoch immerhin ein *plus*: Fordert man physische Sicherung, so fordert man erheblich mehr, als in der herkömmlichen Welt für eine Markierung nötig war. Dies grenzt andere Möglichkeiten aus und kupiert die bloß symbolische Abgrenzung. Die Einschränkung auf den technisch wirksam gesicherten elektronischen Bereich ist nicht dadurch gerechtfertigt, dass diese Einschränkung schon von jeher auch in herkömmlichen Bereichen bestünde. Eine Dokumentation ist dort notwendig – aber auch ausreichend. Die Einschränkung ist auch nicht dadurch gerechtfertigt, dass die Dokumentation nur in Form der Sicherung möglich wäre. Eine Forderung nach mehr und damit das Höherlegen der Schwelle zum Strafrechtsschutz muss damit nicht falsch sein. Sie braucht aber eine besondere und hier noch nicht gefundene Begründung.

III. Technische und soziale Kritik

Nochmals: Wenn die Dokumentationstheorie zur Sicherung sagt, sie müsse ein besonderes Geheimhaltungsinteresse dokumentieren, dann behauptet sie zugleich, dass einer Sicherung genau eine solche Dokumentation valide entnommen werden kann.

Dabei ist die Denkrichtung zu beachten und die These nicht zu verfälschen: Die These behauptet nicht, wer sensible Daten habe, der sichere sie regelmäßig. Dem sollte auch nicht widersprochen sein. Sondern sie behauptet, gesicherte Daten seien gesichert, weil der Inhaber sie wegen eines Geheimnisschutzbedürfnisses habe sichern wollen. Es sei überprüft, ob dieser Gedankengang tatsächlich zwingend und mit der im obigen Sinne für das Strafrecht nötigen Klarheit und Belastbarkeit zu seinem behaupteten Ergebnis führt. Dazu sei genau dieser Gang exemplarisch beschritten. Ausgangspunkt muss ein (sichernder) Mechanismus sein, mit dem die Daten versehen sind.

Vertreter der Dokumentationstheorie führen als Paradebeispiel regelmäßig an, die Passwortabfrage sei eine Sicherung in ihrem Sinne[19]. Zwar gibt es vorsichtigere Stellungnahmen, die besagen, das Passwort käme in Betracht, sei mögliches Beispiel und müsste bestimmte (meist unbenannte) Voraussetzungen erfüllen[20]. Andere schließen bestimmte Anwendungsfälle aus[21]. Zu welchem Anwendungsfall die Abfrage dient, kann von anderen als ihrem Nutzer aber oft erst nach ihrem Brechen beantwortet werden. Schon das Vorliegen der Sicherung muss aber nach oben genannten rechtlichen Anforderungen die nötigen Fragen beantworten. Ansonsten drohte die Dokumentationstheorie sich im Vagen zu verlieren und bliebe zur Rechtsanwendung von begrenztem Wert. Sie führte sich selbst ins Abseits. Nimmt man sie ernst, dann muss es konsequent auch möglich sein, bei Vorliegen einer Passwortabfrage ohne weitere Kenntnisse und ohne unbekannte Voraussetzungen zu beantworten, ob diese Abfrage nun eine Sicherung im Normsinne ist oder nicht. Einer in Aussagekraft und notwendiger Denkrichtung ernst gemeinten Dokumentationstheorie tut man kein Unrecht, wenn man behauptet: Wenn es ein Paradebeispiel gibt für die Behauptung, dass sich in Daten ein Geheimhaltungsinteresse zeigt, dann ist dies die Passwortabfrage. Daher sei dieses Beispiel gewählt.

Die herrschende Ansicht muss auf ihrem Weg vom Auffinden (hier im Beispiel) der Passwortabfrage zum erkannt geglaubten besonderen Geheimhaltungswillen des Inhabers vier verschiedene gedankliche Zwischenschritte unternehmen. Dabei führen die letzten zwei über das bereits gesetzlich Geforderte hinaus: Die Passwortabfrage muss zunächst eine Sicherung sein, weiter zielgerichtet gegen Zugang, motiviert aus Geheimhaltungszwecken und durch den Datenverfügungsberechtigten[22], den Dateninhaber, initiiert.

1. Sicherung

Die Passwortabfrage sichert zunächst Identifikation. Dabei heißt Identifikation nicht zwingend Kenntnis des echten Nutzernamens, seiner Adresse oder Ähnliches. Es reicht, wenn die Eingabe des Nutzernamens und damit verbundener Nutzmöglichkeiten durch das Passwort legitimiert werden. Was diese Identifikation wiederum schützt, darauf kommt es an.

2. Zielgerichtet gegen Zugang

Die Norm fordert Sicherung vor Zugang. Passwortabfragen begegnen wir nicht nur als Eintrittsschwelle zum privaten oder beruflich benutzten PC, sondern auch mehr und mehr im Internet. Onlineshops, -foren, -spiele etwa machen die Auswahl eines Nutzernamens nebst Passwort zur Nutzungsvoraussetzung. Nicht selten sind Nutzername, etwa „nutzer1", und ein zugehöriges Passwort die einzigen eingegebenen Daten. Zwar mag es etliche Fälle geben, in denen der Nutzer Daten zur Nutzung hinterlegen möchte und diese dann gerne per Passwortabfrage gesichert weiß. Doch es gibt ausreichende und zunehmende Fälle, in denen dies nicht der Fall ist. Im Gegenteil würden oft die Nutzer gerne auf solche Abfragen verzichten und einfach ohne persönliches Nutzerkonto im Shop kaufen, im Forum kommentieren oder online spielen. Oft werden die Nutzer, indem sonst eine Nutzung gar nicht oder nur eingeschränkt möglich ist, dazu gezwungen, sich einen Namen und Passwort zu geben, um die Dienste zu nutzen. Festzuhalten ist schon hier, dass der Nutzer oft keine Daten hinterlegt, die er mittels der Abfrage schützen könnte.

Ausschlaggebende Motivation für die aufgedrängte Passwortabfrage ist oft nicht die des Nutzers, sondern die des Betreibers. Um Daten des Letzteren kann es aber hier nicht gehen, darauf ist in Punkt 4 noch einzugehen. Der Betreiber bringt den Nutzer dazu, sich identifizieren zu

---

17) Stellvertretend *Bär* MMR 2005, 434, 436; *Ernst* NJW 2003, 3233, 3236. Zu Parallelen außerhalb Deutschlands *Wall* in *Wall* Cyberspace Crime, 2003, S. 113 ff.; *Dietrich* (o. Fn 1), S. 51 für weitere Nachw.

18) Ordner-, Dateiname und E-Mail-Betreff können bspw. den Begriff „privat" anführen. Letzteres wird in Unternehmen, etwa der Daimler AG, ausdrücklich geregelt. Dateien können durch Attribute „versteckt" werden. Weiteres bei *Dietrich* (o. Fn 1), S. 296.

19) Stellvertretend nur *Schmachtenberg* DUD 1998, 402 und BSI, IT-Grundschutzhandbuch, 2009, M 4.1.

20) *Otto* Grundkurs StrafR BT, § 34 VIII, Rn 66 ff.; *Rengier* StrafR BT/II, § 31 IV. S. 251; *Wessels/Hettinger* StrafR BT/1, Rn 559. Vgl. a. *Maurach/Schroeder/Maiwald* StrafR BT/1, § 29 V 4; Als Beispiel nennen es etwa *Haft* StrafR BT/II, I. IV; *Kindhäuser* StrafR BT I, § 30 Rn 8; *Eisele* StrafR BT I, Rn 700.

21) *Fischer* § 202 a Rn 8 a; *Satzger/Schmidtt/Widmaier-Bosch* § 202 a Rn 5.

22) Zu Rechtsgut und -träger *Dietrich* (o. Fn 1), S. 26 ff., 60 ff.; *Kühl* § 202 a Rn 1; *Maurach/Schroeder/Maiwald* (o. Fn 20), Rn 100 – jew. mwN.

lassen. Das ist für ihn kommerziell interessant, vor allem, wenn jener regelmäßig das Angebot nutzt, um betreiberseitig nicht nur die Nutzung zu steuern, sondern vor allem um konkretes und abstraktes Käuferverhalten, Klickraten auf Seiten und Verweildauern zu erkennen (sog. Datamining). Die meist kostenlosen Angebote dienen letztlich dem Anlocken des Besuchers, dem etwa möglichst nutzer- und zielgruppengerecht Werbung eingeblendet wird. Letzteres setzt Kenntnis über den Besucher voraus. Nicht umsonst werden den Eignern von facebook, StudiVZ, twitter etc. Millionen- und Milliardenbeträge geboten.

Für unsere Frage muss es hier um Sicherung gegen Zugang zu Daten gehen. In den genannten Anwendungen sichern sich die Betreiber aber den Zugang zu Daten, nämlich Daten des Nutzerverhaltens. Diese werden so erst greifbar, zuordenbar und damit auswertbar. Wenn man so will, werden sie so erst generiert. In diesen verbreiteten Fällen kann man dann aber nicht mehr davon sprechen, dass die Identifikation per Passwortabfrage der Sicherung vor Zugang zu ja gar nicht hinterlegten Daten dient.

3. Geheimhaltungszweck – Finalität

Der Sicherungszweck braucht nicht alleiniger Zweck zu sein, er darf aber auch nicht nur nebensächlich sein, so die Vertreter der Dokumentationstheorie[23]. Auf oben genannte Nutzungen, etwa Onlineforen und -spiele zurückkommend, ist mit einer Passwortvergabe oft keine weitere Eingabe von Daten verbunden. Oft stellen die Nutzer bspw. nur ein Nutzerprofil ein, etwa die Art und Weise, wie sie angesprochen werden möchten. Dies sind oft Daten, die nicht geheim sein müssen – und auch oft komplett von anderen Nutzern einsehbar sind. Das Passwort dient dem Nutzer alleine dazu, dass nur er seine Einstellungen ändern kann. Das Passwort regelt zwar einen „Zugang" zu Daten, aber nicht bezüglich des Auslesens von Daten, sondern bezüglich der Veränderung von Daten. Jenes wurde von § 303 a erfasst.

Dann dient aber das Passwort nicht – und in diesen Fällen auch nicht beiläufig – der Geheimhaltung von Informationen. Es sichert anderes, beispielsweise, dass andere nicht fremde Konten sabotierend manipulieren oder sich nicht ein anderer als der vielleicht im Forum mittlerweile anerkannte und geschätzte „nutzer1" einwählt, sich als dieser ausgibt und untauglich kommentiert. Ein echtes Geheimhaltungsinteresse des Nutzers oder des Betreibers ist hier nicht erkenntlich. Das einzig Geheime ist die Kombination aus Nutzername und Passwort. Die Kombination ist Mittel, nicht Ziel einer Sicherung.

Hinter einer Passwortabfrage mag oft ein Geheimhaltungswille stehen. Zwingend ist dies aber nicht. Es gibt etliche Ausnahmen – hier sei nur ein kleines Beispiel aus vielen herausgegriffen, bei denen mittels der Identifikation alternativ andere (und nicht nur zusätzliche) als Geheimhaltungsinteressen verfolgt werden.

Wen dies noch nicht überzeugt, dem sei ein anderes Argument genannt und sich vom Beispiel des Passworts lösend ein klassisches Sicherungsmittel dargelegt: das Haustürschloss. Nehmen wir an, im Haus befinde sich ein selbst ungesicherter Computer. Wie soll dem Schloss anzusehen sein, dass es jedenfalls auch zur Geheimhaltung der Daten des Dateninhabers diene? Zwar ist das Hausschloss als Sicherung anzuerkennen und schützt faktisch auch vor Zugang zu den Daten. Das Haus zu verschließen mag faktisch mannigfaltige Gründe haben, Schutz vor Diebstahl, Sabotage, Ruhestörung etc. Doch das Geheimhaltungsbedürfnis an Daten tritt möglicherweise im Motivbündel bis zur Unkenntlichkeit zurück oder ist schlicht nicht vorhanden. Zu postulieren, ein Geheimhaltungsbedürfnis „sei stets da", wäre schlichte, unbelegte Behauptung. Diese Problematik erkennt die Literatur[24] und versucht sich mit verschiedenen Lösungsansätzen, ohne jedoch Anlass zu sehen, die Dokumentationstheorie als solche zu diskutieren. So versucht sie, mit räumlichen Analogien zu arbeiten[25]. Räumlich-territoriale Begriffe sind jedoch in der digitalen Welt schwer anzuwenden, vor allem wenn man eine taugliche Anwendung für das „raumlose" Internet benötigt. Sie laufen Gefahr, eine bloße ausfüllungsbedürfige sprachliche Metapher zu bleiben. Andere Stimmen führen das Kriterium der Computerspezifität ein[26]. Es bleibt jedoch fraglich, woran sich diese bemisst. Das Hausschloss hat jedenfalls keinen erkennbareren Bezug zum im Haus befindlichen Computer als zu jedem anderen Gegenstand, einschließlich des Biomülls, an dem man kaum ein besonderes Interesse dokumentiert sehen möchte. Wie das Sicherungsmittel ausgestaltet ist, ob das Haus mittels klassischem Schloss oder „computertechnisch" mittels biometrischem Irisscan bzw. Magnetkartenleser gesichert ist, sollte ebenfalls keinen Unterschied machen. Die angebotenen Abgrenzungskriterien führen nur bedingt weiter. Es lässt sich schließen, dass ein Hausschloss das Interesse am Hausfrieden dokumentiert. Aber es dokumentiert nicht zwangsläufig einen auch nur stets hinzutretenden besonderen Geheimhaltungswillen an im Haus befindlichen Daten.

Es kann daher weder bei jüngeren Erscheinungsbildern, wie Passwortabfragen im Internet, noch bei „klassischer" Sicherungstechnik dem Mittel ein ganz bestimmter Zweck, namentlich ein Geheimhaltungszweck, angesehen werden. Es gibt zu viele plausible Alternativzwecke.

4. Initiation durch den Datenverfügungsberechtigten[27], den Dateninhaber

Geht man davon aus, die Passwortabfrage sichere aus einem Geheimhaltungsbedürfnis heraus, so muss sie vom Dateninhaber initiiert oder ihm zumindest zurechenbar sein. Wie oben schon angedeutet, müssen in Fällen der aufgedrängten Identifikation die Interessen des aufdrängenden Betreibers außen vor bleiben. Auch kann nicht argumentiert werden, die Abfrage sichere den Zugang zu den mittels ihrer generierten Nutzerdaten. Diese werden nicht durch die Passwortabfrage gesichert, sonst könnte der Nutzer an sie durch Eingabe seines Passwortes herankommen. Das kann er aber nicht. Vielmehr wird der Betreiber die ermittelten Nutzerdaten (mittels eigener Sicherungstechniken) vor dem Zugriff anderer, inkl. des betroffenen Nutzers, schützen.

Nicht widersprochen werden soll, wenn man in von anderen, etwa vom Computerhersteller, installierten Passwortabfragen eine vorauseilende Ermöglichung der Realisierung der Nutzerinteressen sehen möchte. Wenn der Nutzer diese verwendet und seine Daten dahinter daher schützt, ist ihm dies zuzurechnen. Doch gibt es genügend Fälle, Beispiele sind genannt, in denen diese Zurechnung irrig wäre und sich an der oft gegenläufigen Motivation von Abfrageninitiator und -verwender stieße. Damit kann

23) Vgl. *Fischer* § 202 a Rn 9; MüKo-*Graf* § 202 a Rn 31; *Hilgendorf* JuS 1996, 702; LK-*Hilgendorf* 12. Aufl., § 202 a Rn 30; SK-*Hoyer* § 202 a Rn 9; *Jessen* Sicherung i. S. v. § 202 a, S. 78; *Krutisch* Computerdaten, S. 105; *Leicht* iur 1987, 45, 46 f.; *Lenckner/Schittenhelm* § 202 a Rn 7; LK-*Schünemann* 11. Aufl., § 202 a Rn 15; *Schulze/Heiming* Computerdaten, S. 66; anschaulich *P. Schmid* Computerhacken, S. 73 mwN.

24) *Dietrich* (o. Fn 1), S. 233.

25) *Hilgendorf* JuS 1996, 702 ff.; *Jessen* (o. Fn 23), S. 120.

26) LPK-*Kindhäuser* § 202 a Rn 4; *Arzt/Weber* StrafR BT, § 8 Rn 58 S. 216.

27) Vgl. o. Fn 22.

nicht zwingend aus dem Vorhandensein einer Sicherung ein besonderer, genau benennbarer Wille ihres Verwenders geschlossen werden.

5. Zwischenschluss

Es gibt etliche Fälle der Nutzung von Passwortabfragen, bei denen man nicht sagen kann, dass der Nutzer diese wegen eines Geheimhaltungsbedürfnisses nutze. Im Gegenteil wird ihm oft die Passwortnutzung aufgedrängt, um ihn zu identifizieren und erst Daten über ihn zu generieren.

Soweit ist damit zur allg. Ansicht zu schließen, dass die Dokumentationstheorie nicht nur keine Stütze in den von jeher etablierten Konturen der Geltendmachung des Privatbereichs findet, denn hier stellt sie zu hohe Hürden auf. Sie lässt sich auch in ihrem neuen und speziellen Anwendungsfeld, den elektronischen Sicherungen, nicht begründen. Aus dem bloßen Vorhandensein einer Sicherung, etwa der Passwortabfrage oder dem Haustürschloss, kann nicht gefolgert werden, dass jemand ein besonderes Bedürfnis an der Geheimhaltung bestimmter oder aller Daten habe. Dabei lässt sich die Kritik über die genannten Beispielsfälle hinaus erstrecken, sowohl was beispielhafte Techniken wie Passwortabfrage und Türschloss anbelangt, als auch was Verwendungskontexte, etwa Onlineforen, anbelangt. Eine Untersuchung unterschiedlicher weiterer klassischer Schutztechniken und -kontexte hat Entsprechendes ergeben[28].

IV. Systematische Kritik

Besondere Sicherungen und vergleichbare Techniken als strafrechtliches Kriterium finden sich auch an anderen Stellen des StGB; etwa bei §§ 123 I, 202 I u. II, 202 b, 243 I 2 Nr. 1 u. 2 und 244[29]. Dies wirft die Frage auf, ob das Kriterium jener Techniken normativ vergleichbar wie die Sicherung des § 202 a begründet wird: also dokumentationstheoretisch. Wenn ja, so wäre vor allem zu fragen, ob die hiesige Kritik auch auf jene Normen zu übertragen ist. Falls keine dokumentationstheoretische Begründung angeführt wird, so ist schon bemerkenswert, dass trotz ähnlicher Normtechniken unterschiedliche normative Begründungen angeführt werden. Möglicherweise ist eine solche andere Begründung auch bei § 202 a tragfähig. Es sei hier nur ein kurzer vergleichender Blick vor allem auf folgende Aspekte jener Normen geworfen: vorab Rechtsgut und normative Wirkung des vergleichbaren technischen Merkmals; dann Begründung dessen normativer Relevanz einerseits und damit vergleichend andererseits die faktische Wirkung in technischer, sozialer und verkehrsanschaulicher Hinsicht.

Vergleich mit §§ 202 I, II, 202 b, 123 I und 243 I 2 Nr. 1, 2

a) § 202 b StGB

Bevor auf Normen eingegangen wird, die wie § 202 a eine Sicherung voraussetzen, soll der ihm nächste § 202 b angeführt sein, gerade weil er ihm eng verwandt ist und (dennoch) auf eine Sicherung verzichtet. Der jüngst eingeführte § 202 b erfasst Daten im Übertragungsstadium und damit ein dem § 202 a korrespondierendes Rechtsgut, verzichtet aber auf die formale Umgrenzung. Er schützt fließende Daten per se vor „Anzapfen" und nicht erst, wenn sie faktisch geschützt sind. Mit der Dokumentationstheorie lässt sich dieser Unterschied zu § 202 a kaum begründen. Die Übertragung ist kaum Substitut der Sicherung. Oder wollte man davon ausgehen, dass der Dateninhaber durch das Übertragen sein besonderes Interesse ausdrücke oder es dort selbstverständlich sei – jedoch bei Daten „im Stillstand" eine Dokumentation unabdingar ist? Wohl kaum. Allenfalls könnte vertreten werden, dass es für den Täter regelmäßig schwieriger ist und er mehr Energie aufwenden muss, fließende als (ungesicherte) gespeicherte Daten zu erhalten. Möglicherweise nimmt der Gesetzgeber an, ein solcher besonderer Aufwand für den Täter ließe die Sicherung normativ obsolet werden. Dies hieße aber, die Dokumentationstheorie zu verlassen[30]. § 202 b stützt also nicht die Dokumentationstheorie.

b) § 202 I, II

§ 202 schützt nach der h. M. das Verfügungsrecht darüber, wer den Inhalt eines Schreibens zur Kenntnis nehmen darf[31]. Wie bei § 202 a ist die Sicherung Strafbarkeitsbedingung, die hier in zwei Formen vorliegen kann: (Briefumschlag-)Verschluss und verschlossenes Behältnis. Deren Vorhandensein reicht, während bei § 202 a ein Zweck inhärent sein muss: Sicherung *vor Zugang*. Verschiedene Begründungen der normativen Voraussetzung und zugleich Forderung an einen konkreten potentiellen Mechanismus werden angeführt, beispielsweise dass dieser Verschluss den Geheimhaltungswillen des Verfügungsberechtigten kenntlich macht – also wie bei § 202 a. Darüber hinaus wird aber auch ausgeführt, dem Täter sei regelmäßig gewahr, dass er sich über ein Hindernis hinwegsetze[32]. Einigkeit besteht nach der hM, dass ein fast nur noch symbolhaftes Hindernis ausreicht[33]. Die physische Wirkung ist nahezu vernachlässigbar. Das ist anders als bei § 202 a. Es sei stellvertretend für § 202 der zugeklebte Briefumschlag angeführt. Das Öffnen ist kinderleicht, die physische Hürde denkbar minimal und selbst das unauffällige Öffnen (mittels Wasserdampf) und Wiederverschließen sind leicht möglich. Es wird aber verstanden und verkehrsanschaulich anerkannt, dass der Verschluss nicht gebrochen und zugeklebte Briefe nicht gelesen werden dürfen. Dieser Appell dagegen ist bei Postkarten oder nur eingesteckten Umschlägen erheblich geringer, ja nahezu verschwindend. Die Klarheit des symbolischen Appells resultiert dann nicht in erster Linie aus der physischen Hürde, sondern aus leicht realisierbaren und plausiblen Handlungsalternativen zum Verschließen, d. h. dass „umgekehrt" das Briefumschlagverkleben kaum andere Gründe als Geheimhaltungsinteressen hat. Daher wohnt auch physisch minimalen Hürden eine erhebliche Aussagekraft inne. Andere Gründe verwässern diese Aussage nicht. So dient der Briefumschlag kaum als Schutz gegen Sabotage, Manipulation oder Entwendung. Wie gezeigt wurde, verhält sich dies beim Passwortschutz anders.

Bei § 202 werden verschiedene Begründungen angeführt, weshalb es auf den Schutz ankomme. Soweit der dokumentationstheoretische Begründungsmodus angeführt wird, entsprechen sich normative Voraussetzungsbegründung, normative Forderung an den jeweiligen Mechanismus und faktisch-technische wie verkehrsan-

28) Vgl. *Dietrich* (o. Fn 1), zu Firewalls (S. 269 ff.), Antivirenprogrammen (S. 272 ff.), sog. Kopierschutz (S. 277 ff.), weiteren auch nicht-elektronischen Maßnahmen (S. 280 ff.), Steganographie (S. 287 ff.) und Kryptographie (S. 287 ff., S. 303 ff.).

29) Die hiesigen Linien zu § 123 und § 243 lassen sich auf § 244 übertragen. Aus Platzgründen sei auf *Dietrich* (o. Fn 1), S. 261 ff. verwiesen.

30) Bei der Datenübertragung ist Verschlüsselung das Mittel der Wahl. Die sog. Kryptopolitik des Gesetzgebers ist ambivalent. Er will einerseits zu Schutz ermutigen, andererseits muss er seine strafprozessualen und polizeilichen Abhörmöglichkeiten erhalten. Vgl. *Engel-Flechsig* in *Moritz/Dreier* Rechts-Hdb. zum E-Commerce, Kap. F, Rn 183.

31) Vgl. *Dietrich* (o. Fn 1), S. 238 mwN.

32) LK-*Schünemann* 12. Aufl., § 202 Rn 15.

33) LK-*Schünemann* (o. Fn 32), Rn 13; S/S-*Eisele* § 202 Rn 7; *Lackner/Kühl* § 202 Rn 2; *Wessels/Hettinger* (o. Fn 20), Rn 550; SK-*Hoyer* § 202 Rn 11.

schauliche Wirkung des Mechanismus. Dies liegt bei § 202 a, wie gezeigt wurde, anders. Das Passwort mag als digitale Entsprechung des verklebten Briefumschlages angesehen werden. Es ist sie aber leider nicht.

Eine geringe Übereinstimmung findet sich im Ergebnis für die Variante des verschlossenen Behältnisses. An dieser Stelle soll auf die korrespondierenden Ausführungen zu § 243 verwiesen werden[34]. Es sei allerdings erwähnt, dass die h. M. die Dokumentationstheorie zum verschlossenen Behältnis bei § 202 nur ergänzend anführt.

c) § 123 I

Zu § 123 wird ein Kanon verschiedener Rechtsgüter diskutiert. Überzeugend ist, dass verschiedene Interessen an Alleine-gelassen-werden, Ruhe, physischem Schutz und Geheimhaltung zu einem einheitlichen, territorial gefassten Abwehrrecht kombiniert werden.

Historisch wachsen dabei physischen Schutzkomponenten moderne Geheimhaltungs- und Freiheitsinteressen mehr und mehr zu. Die Norm erfasst damit jedenfalls heute auch einen besonderen Teil der Privatsphäre[35]. Ihre formal sichernde Umgrenzung ist Strafrechtsschutzvoraussetzung. Damit ist die Norm insoweit inhaltlich und in ihrer formalen Fassung mit § 202 a vergleichbar.

Die rechtliche Forderung einer Befriedung oder anderer Wehr lässt sich dabei wie bei § 202 a nicht schon aus der Verkehrsanschauung begründen. Denn zur sozialen Anerkennung benötigt der Hausfrieden keine besondere physische Sicherung, wie die sozialpsychologische Forschung zeigt (s. o.). Dennoch sollen rein symbolische Wehre rechtlich nicht reichen[36]. Der geschützte Bereich muss grundsätzlich befriedet oder bewehrt sein[37]. Diese Forderung wird aber prinzipiell anders als die entsprechende des § 202 a begründet. Nach der umfassenden Analyse *Amelungs* liege ihr Grund darin, dass der Täter nicht nur symbolische, sondern darüber hinaus physisch wirksame Barrieren missachte[38]. Und darauf komme es an: Die Schutzniveausteigerung lässt sich, weiter *Amelung* folgend, rechtfertigen, indem nicht bloß eine Dokumentation eines besonderen Interesses gefordert oder gefolgert werden soll, selbst wenn sie sozial anerkannt sei. Sondern indem ein erkennbares Interesse auch noch mit physischer Gewalt, mit besonderer Energie überwunden und damit besonders missachtet wird. Der Unterschied im Meinungsstand zu § 202 a ist dabei erheblich, auch wenn dies auf den ersten Blick nicht so scheinen mag: Bei § 202 a wird der Blick auf das potentielle Opfer gelenkt. Gefordert wird (die Dokumentation) *von ihm*. Im Mittelpunkt des § 123 steht aber der Täter. Zugleich wird begründet weshalb: *Er* handele in besonderer, gesteigerter Weise.

d) § 243 I 2 Nr. 1 und 2

Anders als bei den vorgenannten Normen ist ein besonderer Mechanismus nicht Strafvoraussetzung, denn schon die Wegnahme ungeschützten Eigentums ist strafbar. Er kann aber den Strafrahmen erhöhen. Es werden mannigfaltige Gründe für die Strafrahmenerhöhung bei der Nr. 1 der Norm (umschlossener Raum) und der Nr. 2 (verschlossenes Behältnis oder andere Schutzvorrichtung) angeführt[39]. Um den Rahmen nicht zu sprengen, sei der *BGH* zusammenfassend zitiert, in dessen Ausführungen sich die wesentlichen Strömungen wiederfinden: Der Täter missachte den vom Gewahrsamsinhaber zum Ausdruck gebrachten Besitzwillen, den gesetzgeberischen Willen, die vom umschlossenen Raum erfassten Gegenstände in erhöhtem Maße als schutzwürdig anzusehen, und den erhöhten Rechtsfrieden des Ortes. Er überwinde zudem die entgegenstehenden Hindernisse durch besondere Gewalt oder List und zeige damit eine stärkere verbrecherische Energie, die ihn gefährlicher und eher strafwürdig erscheinen lasse[40]. Weiter werde der Hausfrieden verletzt[41]. Bemerkenswert sind neben den Begründungsmodi selbst deren Vielfalt, ihre Kombination, und dass es keine echte Auseinandersetzung um sie gibt. Vergleichbar verhält es sich bei der respektiven Nr. 2, dort wird die Dokumentationstheorie allenfalls ergänzend angeführt[42].

Damit liegt in den Begründungsmodi der Nrn. 1 und 2 ein wesentlicher Unterschied zu § 202 a: Die Dokumentationstheorie ist bei Ersteren nur eine mehrerer angebotener Begründungen und nicht die wesentlichste. Und das, obwohl bei jenen Normen die Dokumentationstheorie jedenfalls teilweise besser passte. Denn zumindest werden die Techniken des § 243 Abs. 1 S. 2 Nr. 1 und 2 eher als Sicherung vor Wegnahme des Eigentümers erkannt und respektiert, und Überschreitungen gelten als deviant. Dennoch ist die behauptete Dokumentation durch das Opfer nur eine Begründung von vielen. Und auch hier fällt auf, dass vor allem besondere Anforderungen an den Täter gesehen werden und sie dadurch begründet werden, dass er erhöhte Energie aufbringen müsse, um diese Sicherungen zu überwinden.

e) Zwischenschluss

Das dem § 202 a aufs engste verwandte Rechtsgut des § 202 b bedarf keiner Dokumentation einer besonderen Sicherung. Weiter wird bei Norminhalt und Abgrenzungstechnik mit § 202 a vergleichbaren Normen das Erfordernis des Abgrenzungsmechanismus unterschiedlich begründet. Dies gilt selbst dann, wenn sich dort die Dokumentationstheorie gar besser anwenden ließe als bei § 202 a. Als anderer Grund wird insbesondere bei § 123, aber auch anderen Normen angeführt, dass zur Privatbereichsverletzung hinzutrete, dass der Täter eine gesetzte Schwelle mit besonderer Energie überwinde und dass er hierdurch seine besondere Gefährlichkeit zeige.

D. Suche alternativer Begründungen

Die hergebrachte Begründung zu § 202 a findet also wenig Stütze. Denn sie kann sich weder auf den hergebrachten Umgang mit der Privatsphäre stützen, noch steht sie mit erheblichen Erscheinungsformen moderner Technik und ihrer Anwendung im Einklang. Zudem erfährt sie keine ausreichende rechtssystematische Flankierung. Daher sei sich auf die Suche nach anderen Begründungen begeben. Findet sich keine Alternativbegründung, so müsste *de lege ferenda* ein Reformvorschlag unterbreitet werden. Denkbar wäre, vergleichbar der Schwesternorm des § 202 b, auf die Schutzanforderung zu verzichten. Findet sich eine Alternativbegründung, so kann der Normtext „beim Alten“ bleiben. Die neu gefundene Begründung aber wäre zukünftig *de lege lata* der Auslegung zu Grunde zu legen.

I. Viktimodogmatik

Neben der Dokumentationstheorie werden bei § 202 a vereinzelt viktimodogmatische Begründungen angedeu-

34) Ausf. *Dietrich* (o. Fn 1), S. 238 ff.
35) *Amelung* NJW 1986, 2075, 2080; grdl. *ders.* ZStW 98 (1986), 355, 403 ff.
36) Zur Ausdehnung auf ungeschützte Angrenzungsflächen S/S-*Lenckner/Sternberg-Lieben* § 123 Rn 6 mwN.
37) S/S-*Lenckner/Sternberg-Lieben* (o. Fn 36).
38) *Amelung* ZStW 98 (1986), 355, 403 ff.
39) *Dietrich* (o. Fn 1), S. 253 bis 256.
40) *BGHSt* 1, 158, 164 f.
41) *BGHSt* 15, 134.
42) *Dietrich* (o. Fn 1), S. 256 mwN.

tet[43]. Die Viktimodogmatik besagt verkürzt, dass das scharfe Schwert und der administrative Apparat des Strafrechts nicht denjenigen schützen solle, der es versäumt, sich selbst mit eigenen vorhandenen und zumutbaren Mitteln zu schützen[44]. Diese These will vor allem *Schünemann* auf § 202 a übertragen wissen[45]. Einem solchen Transfer lassen sich schon die der Viktimodogmatik grundsätzlich entgegengehaltenen Gründe erwidern[46]. Für § 202 a ist keine Ausnahme zu machen. Im Gegenteil, die Argumente wider die Viktimodogmatik gelten hier „par excellence". Gerade der Schutzlose braucht besonderen staatlichen Schutz. Dies gilt auch und vor allem vor dem Hintergrund der immer komplexer werdenden elektronischen Welt. Sie droht ohnehin, Teile der Gesellschaft abzuhängen. Dies soll nicht noch verstärkt und technisch weniger Versierten auch noch der Strafrechtsschutz entzogen werden. Richtig ist im Gegenteil, besonders Schwache verstärkt zu schützen[47], beispielsweise dem sich mutwillig schutzlos Trinkenden den erhöhten Strafrechtsschutz des § 243 I 2 Nr. 6 zuteilwerden zu lassen, was selbst Vertreter der Viktimodogmatik befürworten[48]. Es steht dazu systematisch im Widerspruch und ist auch in sich falsch, dem weniger kundigen Bürger nötigen Schutz zu entziehen[49]. Viktimodogmatik und Dokumentationstheorie, die ja beide eine Handlung vom potentiellen Opfer fordern, rücken dieses damit in den Mittelpunkt. Es ist sicher begrüßenswert, dem Opfer in vieler Hinsicht mehr Aufmerksamkeit zu widmen. Deutsches Strafrecht ist aber als Schuldstrafrecht in erster Linie als Täterstrafrecht konzipiert. Rechtsdogmatische Durchbrechungen drohen, wie sich zeigt, dem Opfer „Steine statt Brot" zu geben.

II. Erhöhung des Erfolgsunrechts

Statt der bisherigen Ansätze kann vielleicht die Besinnung auf die Grundlinien des Strafrechts Abhilfe schaffen. So rechtfertigen anerkanntermaßen eine vertiefte Rechtsgutsverletzung und damit erhöhtes Erfolgsunrecht die Begründung oder Erhöhung von Strafe. Ein erhöhtes Erfolgsunrecht wäre etwa gegeben, wenn weitere Rechtsgüter verletzt wären. Für den Vergleich der Verletzung eines gesicherten mit der eines ungesicherten Raumes ist festzuhalten, dass die Sicherung nicht das Rechtsgut originär erschafft. Wie bei § 123 besteht die persönliche Sphäre auch ohne Sicherung. Sie ist kein eigenes Rechtsgut, da sie kein Selbstzweck ist. Damit scheidet die erfolgssteigernde Variante des Verletzens weiterer Rechtsgüter aus. Erfolgssteigernd wäre auch, wenn das Rechtsgut von erhöhtem Wert wäre (statt ins Persönliche wird ins Intime eingedrungen), wenn es tiefer (zur Auslese hinzutretend Verbreitung der Informationen), breiter (Aufnahme von mehr Information) oder längerdauernd verletzt wäre. Doch auch für diese Fälle spielt die Sicherung keine Rolle. Daran ändert auch die Novelle des § 202 a nichts, der nun auch das bloße Eindringen, das Hacking erfassen soll. Das Ausspähen gesicherter Daten birgt damit kein erhöhtes Erfolgsunrecht im Vergleich zum Ausspähen ungesicherter[50]. Diese Begründung scheidet aus.

III. Erhöhung des Handlungsunwerts

Es wurden Stimmen zitiert, nach denen der Täter, der fremde gesicherte Daten auslese, rücksichtsloser handele als der, der ungesicherte auslese. Dies normativ zu greifen suchend lässt sich festhalten, dass nicht auf den Taterfolg (auslesen), sondern die Begehungsweise (rücksichtslos) abgezielt wird. Sehen könnte man damit bei gleichbleibendem Erfolgsunwert (verstanden als Verstoß gegen eine Bewertungsnorm) einen verstärkten Verstoß gegen eine Bestimmungsnorm und damit erhöhten Handlungsunwert und erhöhten Intentionsunwert[51]. Das ginge zunächst in die richtige Richtung. Es ließe sich aber entgegenhalten, dass, verkürzt gesagt, der Intentionsunwert des Eindringens in einen fremden gesicherten im Vergleich zu dem in einen fremden ungesicherten Raum nicht zwingend erhöht ist. Der Täter stellt sich vielmehr gerade demjenigen gleich, der einen ungesicherten Raum betritt. Denn er negiert gerade die Sicherung und damit den Unterschied[52].

IV. Fundamente des Strafens – Strafzwecklehre

Auf der Suche nach der Begründung, weshalb das Eine (Ausspähen gesicherter Daten) bestraft wird und das Andere (Ausspähen ungesicherter Daten) nicht bestraft wird, könnte man eine besondere, modernistische, computerspezifische Lösung fordern. Vielleicht aber hilft eine nochmalige Besinnung darauf, weshalb von der hiesigen Materie abgesehen überhaupt das Eine bestraft wird und das Andere nicht. Dies beantwortet die Strafzwecklehre[53]. Anerkannt ist heute neben anderen Zwecken die Spezialprävention. Aus ihr folgt, dass auf den Gefährlicheren überhaupt oder mehr noch einzuwirken ist als auf den Ungefährlicheren.

Auf die hiesige Materie übertragen: Wenn derjenige, der für ihn nicht bestimmte gesicherte Daten ausliest, erheblich gefährlicher ist, als derjenige, der ungesicherte ausliest, dann hätten wir hier ein Begründungsfundament. Bildet man Fallgruppen, so zeigt sich: Am ungefährlichsten ist der, der fremde Zuordnungsbereiche respektiert und dem die Mittel fehlen, gesicherte Bereiche zu betreten. Davon hebt sich derjenige ab, der den fremden Zuordnungsbereich erkennt („… *Daten, die nicht für ihn bestimmt* …") und ihn dennoch betritt. Er verstößt gegen eine soziale Norm, bringt entsprechende psychische Energie zum Sozialnormbruch auf und ist aufgrund dieses Willens gefährlicher. Doch könnte ihn ein faktischer Schutz zurückhalten, wenn ein solcher bestünde. Es ist jedenfalls nicht gezeigt, dass er ihn brechen könnte und würde. Derjenige wiederum, der Schutztechniken faktisch überwinden kann, ist aufgrund seines Könnens gefährlicher für geschützte Objekte als derjenige, der dies nicht kann. Doch ihn mag ein Normappell und sein Gewissen zurückhalten. Erst derjenige, der – wie es § 202 a normiert – einen erkennbaren fremden Bereich betritt und dies trotz Sicherung, verwirklicht beide Gefahrpotentiale: Das Können und das Wollen. Dies findet sich auf gleicher Linie wie *Amelungs* oben angerissene Ausführungen zu § 123. Man könnte dieses „Mehr" auch als besondere kriminelle Energie bezeichnen. Solchem kann weder mit Appellen noch mit Schutzwehren beigekommen werden. Um auf

43) Vgl. etwa LK-*Schünemann* (o. Fn 23), Rn 14; *LK-Hilgendorf* (o. Fn 23), Rn 29. Zur Viktimodogmatik bei § 202 a ausf. *Dietrich* (o. Fn 1), S. 321-357.

44) S/S-*Lenckner/Eisele* vor § 13 Rn 70 b mwN.

45) LK-*Schünemann* (o. Fn 23), Rn 14.

46) Grdl. *Günther* in FS Lenckner, S. 67 ff.; vgl. S/S-*Lenckner/Eisele* (o. Fn 44).

47) Vgl. zur Deliktsgruppe „Ausnutzung von Schwächelagen" *Kindhäuser* BT II, § 42 Rn 1, S. 328; ausf. *Brandl* Spielleidenschaft und StrafR, 2003, S. 16 ff.

48) *Blei* StrafR BT, § 54, 6; *ders.* Zur Viktimodogmatik in StrafR BT, § 61 IV.

49) *Dietrich* (o. Fn 1), S. 354 f.

50) *Dietrich* (o. Fn 1), S. 36 ff.

51) Zu Handlungs- und Erfolgsunrecht vgl. *Jescheck/Weigend* (o. Fn 11), § 24 II mwN; *Dietrich* (o. Fn 1), S. 366 mwN.

52) Zum Handlungsunrecht bei § 202 a *Dietrich* (o. Fn 1), S. 365 ff.

53) Überblick bei *Kühl* Sanktionensystem, S. 141 ff.; *Roxin* StrafR, AT/1, § 3.

ihn einzuwirken, bedarf es der *ultima ratio*: der Strafe. Es ist gesetzgeberisch legitim und gut begründbar, erst ihn zu bestrafen. Damit lässt sich das Erfordernis der besonderen Sicherung bei § 202 a mit spezialpräventiven Strafzwecken begründen.

E. Schluss

Die allgemeine opferfokussierte Ansicht, die Begründung des Sicherungserfordernisses darin zu sehen, dass der Rechtsinhaber hier ein besonderes Geheimhaltungsinteresse gezeigt habe, ist keine Fortzeichnung hergebrachter Konturen der Privatsphäre in die digitale Welt. Sie wird der heutigen Technik und gelebten Realität nicht gerecht. Sie passt sich nicht in die Begründung anderer Sicherungserfordernisse ein. Dagegen ist es ein tragfähiger Ansatz, auf Basis der Strafwecklehre den Täter als gefährlicher als andere und zugleich die Schwelle der Strafwürdigkeit überschreitend anzusehen, der gezeigtermaßen sowohl fähig wie willens ist, gesetzte Datensicherungen zu überwinden. Diese Begründung steht in Passung mit den technischen Gegebenheiten, der heute sozial gelebten Wirklichkeit, der Gesetzessystematik[54] und durch Besinnung auf Täter und Strafwecklehre zugleich mit den Grundlinien des Strafrechts. Die Neufundierung sollte zugleich zu einem besseren Verständnis des elektronischen Geheimbereichs und zu fundierterer praktischer Rechtsanwendung führen[55].

54) Zur Technik und Systematik *Dietrich* (o. Fn 1), S. 372 ff., 377 ff.
55) Ausgewählte praktische Folgen *Dietrich* (o. Fn 1), S. 383 ff.