DGRI e. V. • Emmy-Noether-Straße 17 • D-76131 Karlsruhe

Prof. Dr. Dirk Heckmann
1. Vorsitzender

Universität Passau
Gottfried-Schäffer-Str. 20
94032 Passau

Tel.: (0851) 509-2291
Fax: (0851) 509-2292
E-Mail: heckmann@uni-passau.de

Passau, im Juni 2015

Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei
Hier: Stellungnahme der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI)

Sehr geehrte Damen und Herren,

I.

die DGRI ist eine der in Deutschland führenden unabhängigen wissenschaftlichen Vereinigungen auf dem Gebiet des IT-Rechts. Sie befasst sich mit Fragen an der Schnittstelle zwischen Informatik einerseits sowie Recht und Wirtschaft andererseits und fördert die Zusammenarbeit von Lehre, Forschung, Gesetzgebung und Praxis in allen Fragen der Informationstechnik. Zu ihren Mitgliedern zählen Wissenschaftler und Praktiker sowohl aus dem Gebiet der Rechtswissenschaft als auch der Technik. Mit ihnen sucht die Gesellschaft den ständigen Austausch von Wissen, Erfahrungen und Meinungen. Die DGRI begleitet mittels von der Gesellschaft veröffentlichter Stellungnahmen Gesetzgebungsvorhaben auf nationaler wie europäischer Ebene als neutrale Institution, die den Partikularinteressen einzelner Unternehmen oder Branchen nicht verpflichtet ist.
Die folgende Stellungnahme haben die Leiter des Fachausschusses Strafrecht, Prof. Dr. Susanne Beck, LL.M. und Rechtsanwalt Dirk Meinicke, LL.M., für die DGRI verfasst.

II.

Auf Initiative Hessens hat der Bundesrat im April 2014 den Entwurf eines Gesetzes zur Bestrafung der Datenhehlerei in den Bundestag eingebracht (BT-Drucks. 18/1288). Inzwischen liegt auch ein Referentenentwurf vor, als Teil des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Entwurf vom 15.05.2015). Der „Fachausschuss Strafrecht" der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI) hat sich mit der materiell-rechtlichen und prozess-rechtlichen Seite des Gesetzesentwurfs mit Blick auf die Datenhehlerei befasst. Dieser Straftatbestand hängt inhaltlich nicht zwingend mit der Einführung der Vorratsdatenspeicherung zusammen, wird von den Autoren als nicht unproblematisch angesehen und hier deshalb gesondert analysiert.

Stellungnahme der DGRI zum Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei (Drs. 18/1288)(RefE)

Illegal erlangte Daten werden häufig nicht direkt von demjenigen, der sie beschafft hat, zur Begehung von Straftaten verwendet. Vielmehr sind diejenigen, die die Begehung von Straftaten mit fremden Daten planen, oft gar nicht selbst in der Lage, sich diese Daten – z.B. durch Hacking oder Phishing – zu besorgen. Aus diesem Grund wird von einigen Institutionen – z.B. dem Justizministerium – an dieser Stelle eine zu schließende Strafbarkeitslücke vermutet. Diskutiert wird deshalb, die (Weiter)Verarbeitung von Daten und deren Weitergabe (etwa gegen Entgelt) gesondert unter Strafe zu stellen.[1] Der entsprechende, auf eine Initiative Hessens zurückgehende Gesetzesentwurf vom 30.04.2014[2] wurde dem Bundestag zugeleitet und soll demnächst, nun in Verbindung mit den Regelungen zur Verkehrsdatenspeicherung, in erster Lesung beraten werden. Sowohl materiell- als auch prozessrechtlich finden sich jedoch plausible Argumente gegen diesen Vorschlag, weshalb das Gesetzesvorhaben bezüglich des neuen Straftatbestands im Ergebnis nicht zu begrüßen ist.

A. Anmerkungen zum materiellen Recht

Es kann nämlich bereits bezweifelt werden, ob überhaupt eine Strafbarkeitslücke vorliegt, da die bestehenden Regelungen den relevanten Bereich recht weitgehend abdecken und viele der problematischen bzw. das Rechtsgut gefährdenden Handlungen bereits erfassen:

Nach den §§ 202a ff. StGB macht sich strafbar, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind,

[1] BT-Drucks. 18/1288, 2 f., 9-11; RefE., 2, 26-29; Justizminister Heiko Maas gegenüber Neue Presse am 08.08.2014, abrufbar unter: http://www.presseportal.de/pm/66865/2802923.
[2] BT-Drucks. 18/1288; Vgl. auch Bundestag, ID: 18-57888.

unter Überwindung der Zugangssicherung verschafft (§ 202a I StGB), unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus elektromagnetischer Abstrahlung einer Datenverarbeitungsanlage verschafft (§ 202b StGB) oder eine derartige Straftat vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht (§ 202c StGB).

Nach § 303a StGB wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Für die Vorbereitung gilt § 202c StGB entsprechend, vgl. § 303a Abs. 3 StGB. § 303b StGB sanktioniert bestimmte erhebliche Störungen einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, durch jeweils spezifisch beschriebene Handlungen.

§§ 106 ff. UrhG erklären unter anderem denjenigen für strafbar, der in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt (§ 106 UrhG), nach § 107 UrhG die Urheberbezeichnung unzulässig anbringt oder die Verwertungsbefugnisse der Inhaber verwandter Schutzrechte verletzt, § 108 UrhG. Wer diesbezüglich gewerblich handelt, erfüllt die Qualifikation des § 108a UrhG. Überdies sind die Umgehung technischer Schutzmaßnahmen und der Eingriff in zur Rechtewahrnehmung erforderliche Information strafbar, § 108b UrhG.

Schließlich ist gemäß §§ 44 BDSG strafbar, wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht. Das heißt konkret, wer

- unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
- unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,
- unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
- die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
- oder wer übermittelte Daten für andere als vorher bestimmte Zwecke nutzt, entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

- bestimmte Merkmale mit einer Einzelangabe zusammenführt oder bestimmte Mitteilungen über unrechtmäßige Übermittlungen oder Kenntnisnahmen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

Diese Darstellung der bereits existierenden, die Problematik doch recht weitgehend erfassenden Straftatbestände ist zudem im Zusammenhang mit den Beteiligungsregelungen (§§ 26 f. StGB) zu betrachten. In vielen Fällen werden Verhaltensweisen des späteren Datenverwenders als Anstiftung und Beihilfe zur illegalen Beschaffung von Daten also bereits heute strafrechtlich erfasst sein.[3]

Zwar gibt es wohl weiterhin einige wenige straflose Handlungen, die mit illegaler Datenbeschaffung in Verbindung stehen, etwa wenn tatsächlich jede Beteiligung an der Vortat fehlt und die Daten nicht unter das BDSG oder das UrhG fallen – an diesen Daten dürfte allerdings das Interesse gering sein. Zudem wird zugegebenermaßen die Verbindung zwischen Datenverwerter und Datenbeschaffer (also z.B. die Anstiftung) nicht in allen Fällen beweisbar sein.[4] Diese Aspekte bedeuten aber gerade nicht, dass diese Lücke strafrechtlich geschlossen werden müsse. Die Feststellung einer Lücke in der strafrechtlichen Erfassung denkbarer Handlungen ist nur notwendig, aber keineswegs hinreichend für den Erlass eines neuen Straftatbestands. Selbst wenn feststehen sollte, dass der Gesetzgeber an die nicht erfassten Handlungen bei Erlass des Gesetzes nicht gedacht hatte, heißt auch das nicht, dass andernfalls ein Strafgesetz erlassen worden wäre. Für den Erlass eines Strafgesetzes ist vielmehr erforderlich, dass das jeweilige Handeln konkret strafwürdig ist, dass eine hinreichend bestimmte und funktionale Strafnorm erlassen werden kann und es überdies plausibel ist, dass das Gesetz den sozialen Konflikt überhaupt nachhaltig auflösen kann. Das ist für die geplante Norm zu überprüfen.

Im Kontext mit illegal beschafften Daten gibt es, so der Gesetzgeber, „nach Angaben von Fachleuten […] einen millionenschweren Schwarzmarkt, auf dem beispielsweise gestohlene Konto- und Kreditkarteninfos verkauft werden.“[5] Die Zwischenhändler können derzeit nur nach nebenstrafrechtlichen Normen (§§ 43, 44 BDSG) belangt werden. Diese Normen erfassen nur ganz spezifische Fälle, ihre Strafdrohung ist vergleichsweise niedrig. Das spricht aus Sicht des Gesetzgebers dafür, die Datenhehlerei unter Strafe zu stellen, um den Handel mit Daten – und damit die illegale Beschaffung – weniger attraktiv erscheinen zu lassen. Dabei sei aber ebenfalls erforderlich, dass diese Norm gleichzeitig die Entlastung staatlicher Behörden garantiere; so soll

[3] Vgl. für den Ankauf von Steuerdaten *Benkert*, in: Lüderssen/Volk/Wahle (Hrsg.), Festschrift für Wolf Schiller, 2014, 33 f.
[4] BT-Drucks. 18/1288, 11; RefE., 27.
[5] http://www.fnp.de/nachrichten/transfer_alt/Datenhehlerei-soll-strafbar-werden;art1463,326277.

der Ankauf illegal erworbener Steuerdaten weiterhin möglich sein. Als Vorschlag eines entsprechenden Gesetzes wird derzeit diskutiert[6]:

§ 202d StGB „Datenhehlerei“

(1) Wer Daten im Sinne von § 202a Abs. 2, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

[…] (3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie

2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

Wie erwähnt führt der Gesetzgeber für die Notwendigkeit des Tatbestands der Datenhehlerei das Schutzbedürfnis des Dateninhabers an, da seiner Ansicht nach durch die Norm die Attraktivität der illegalen Beschaffung verringert wird. Auch stünde eine Straflosigkeit derartigen Verhaltens in Widerspruch mit der Strafbarkeit der Hehlerei nach § 259 StGB. Das letztere Argument ist jedoch bereits insofern unplausibel, als die klassische Hehlerei von Sachen die Perpetuierung des Eigentumsverlusts bedeutet – bei Daten, die gerade nicht materialisiert sind und nicht nur einmal in der Wirklichkeit existieren und nur vom Gewahrsamsinhaber verwendbar sind, ist der Weiterverkauf dagegen nicht im selben Maß rechtsgutsverletzend wie bei Sachen (auch wenn das generelle Interesse des Verfügungsberechtigten daran, dass seine Daten nicht weiterverbreitet werden, nicht zu bestreiten ist, wird es eben nicht auf dieselbe Weise verletzt wie das Eigentum durch Hehlereitaten). Deshalb lässt sich die Notwendigkeit der Norm jedenfalls nicht mit einer Parallelität zu § 259 StGB begründen. Eine Vertiefung der Rechtsgutsverletzung kann zwar in der weiteren Kenntnisnahme durch Dritte – also den Täter der Datenhehlerei – liegen, wobei aber zu beachten ist, dass der sich die Daten Verschaffende nicht unter Umgehung besonderer Sicherungsvorkehrungen o.ä. handelt, was daran zweifeln lässt, dass seine Tat mit Blick auf die Verwerflichkeit der ersten Tat entspricht und tatsächlich einer eigenständigen Regelung im StGB – über die Regelungen des BDSG und UrhG hinaus - bedarf.

[6] BT-Drucks. 18/1288, 7 f., hier aktualisiert entsprechend der Fassung im Referentenentwurf (S. 20).

Fraglich ist, ob das Argument der Attraktivitätsmilderung des Datenerwerbs valide ist. Die Verschaffung der Daten sind ja an sich bereits strafbar, der Ersttäter begeht also bereits eine illegale Handlung und geht dabei davon aus, dass er dafür nicht belangt wird – sonst würde er schon von dieser Ersttat Abstand nehmen. Diese Handlung ist eigentlich selbst schon durch einen entsprechenden Straftatbestand „unattraktiv", wird aber in diesen Fällen trotzdem vorgenommen. Es ist nicht davon auszugehen, dass die Möglichkeit der Weiterverwertung der Daten – sei es durch eigenes, weiteres illegales Handeln oder durch Verkauf – durch das Gesetz derart eingeschränkt wird, dass die Unattraktivität der Ersttat im Vergleich zu der ohnehin schon bestehenden Gefahr der Strafverfolgung so ansteigt, dass der Ersttäter nun gerade deshalb sein Handeln überdenkt. Auch begeht er von den von der Norm erfassten Taten die Ersttat ja ohne vorherige Kontaktaufnahme mit einem möglichen Abnehmer (da sonst Anstiftung oder Beihilfe vorläge); er handelt also jedenfalls nicht aufgrund der Aussicht auf einen gesicherten Gewinn durch den Weiterverkauf der Daten, sondern – wenn materiell motiviert – auf Basis einer vagen Hoffnung, einen solchen Gewinn erreichen zu können. Dass sich diese verringert, ist zu bezweifeln. Das Argument ist also jedenfalls nicht so überzeugend, dass es als einzige Begründung die Einführung eines neuen Straftatbestands rechtfertigen könnte.

Nicht nur, dass die Argumente für den neuen Tatbestand nicht weit tragen – es finden sich zudem auch einige Argumente, die gegen seine Einführung sprechen:[7] Zum einen ist die Handlung selbst – mangels konkreter weiterer Gefährdung der Verfügungsmacht über die Daten (diese bleibt vom Weiterverkauf unbeeinträchtigt, da Daten kein nur ein einziges Mal tatsächlich existierendes Gut sind) – nicht derart verwerflich, dass sie eine Bestrafung erfordert. Auch die bloße Überwindung von Beweisschwierigkeiten reicht jedenfalls nicht als Begründung für die Strafwürdigkeit der Datenhehlerei; es wäre höchst problematisch, eine Ausweitung der Strafbarkeit nur deshalb vorzunehmen, weil man bereits bestehende Strafbarkeiten in der Praxis nicht nachweisen oder angemessen verfolgen kann. Zudem wäre auch die Datenhehlerei selbst wahrscheinlich häufig schwer beweisbar, vor allem die zusätzliche Bereicherungs- oder Schädigungsabsicht.

Das Verbot erscheint zudem nicht geeignet und erforderlich, um das Problem des Handels mit Daten zu lösen – so ist insgesamt das Strafrecht im Internet wenig erfolgversprechend, da die Akteure nur wenig Angst vor Strafverfolgung haben, die Strafnormen also kaum Abschreckungswirkung erzielen; das gilt gerade in Kontexten, in denen die konkrete Handlung für den Dateninhaber nicht erkennbar ist und deshalb nur die Taten zur Verfolgung gelangen, die vom Staat selbst ermittelt werden. Auch liegt die geringe Hemmschwelle vor der Begehung einer Straftat an der fehlenden Sozialkontrolle – der Täter agiert hier meist zumindest real alleine und unbeobachtet. Diese Überlegungen lassen sich nur entkräften, wenn im Einzelfall gute Gründe dafür erkennbar sind, dass eine Strafnorm tatsächlich geeignet ist, das Verhalten des Akteurs zu

[7] Vgl. *Golla/von zur Mühlen* JZ 2014, 668 ff.

beeinflussen. Das ist hier nicht der Fall: Da sowohl Erwerb als auch Bezahlung der Daten ausschließlich online möglich sein werden, spricht mehr für eine schwache Resonanz auf strafrechtliche Verbote – auch, da sich wie in den meisten Fällen derartiger Taten die Problematik der Anwendbarkeit deutschen Strafrechts bzw. der Verfolgbarkeit der nicht auf deutschem Boden begangenen Straftaten stellt. Nicht zuletzt würden sich viele derzeitige Beweisprobleme wohl auch bei der Verfolgung dieses Straftatbestands ergeben.

Neben den durch den Gesetzgeber nicht ausgeräumten Zweifeln an der Eignung ist auch nicht erkennbar, warum gerade Strafrecht das mildeste Mittel zur Bewältigung dieses Sozialkonflikts sein sollte – da es sich um die ultima ratio des Staates handelt, muss dies jeweils besonders begründet werden. Des Weiteren lässt sich ein solches Verbot kaum hinreichend genau beschreiben – weshalb auch auf die eher vage Formulierung „sonst zugänglich macht“ zurückgegriffen wird, dies ist jedoch mit Blick auf das Bestimmtheitsgebot problematisch. Schließlich wird die Entlastung staatlicher Behörden nach Abs. 2 kritisiert. So ist fraglich, warum Journalisten oder auch andere bestimmte Interna Veröffentlichende (Blogger, Whistle-Blower) vom Gesetzgeber nicht in derselben Weise privilegiert werden sollen, gibt es doch insofern verfassungsrechtlich geschützte Interessen (Informationsfreiheit), die zumindest die Begründung der Schlechterstellung erschweren.[8] Das Problem wurde zwar durch die aktuelle Fassung etwas entschärft, aber wiederum zumindest nicht eindeutig mit Blick auf Blogger oder Whistle-Blower – die Ungleichbehandlung der staatlichen Institutionen ist jedenfalls weiterhin nicht ohne Weiteres begründbar.

Es ist deshalb festzustellen: Auch wenn grundsätzlich nachvollziehbar ist, dass es an der Einschränkung des von der geplanten Norm umschriebenen Verhaltens ein gewisses Interesse gibt, sprechen doch bessere Argumente für den Verzicht auf den Straftatbestand der „Datenhehlerei“, da er inhaltlich nicht geeignet und überdies nicht erforderlich ist, dieses Verhalten einzuschränken, problematische prozessuale Folgen hätte (dazu sogleich) und durch diese Mängel das Strafrecht insgesamt geschwächt wird: Jede neue symbolische Strafnorm stellt eine Schwächung des Kernstrafrechts dar!

B. Anmerkungen zum Prozessrecht

Auch aus strafprozessualer Sicht begegnet die beabsichtigte Neuregelung durchgreifenden Bedenken. Insbesondere fehlt es nach wie vor an geeigneten Ermittlungsbefugnissen, um – vor allem in transnationalen Sachverhalten – im Bereich von Datennetzen den rechtsstaats- und gesetzeskonformen Zugriff auf potentiell beweiserhebliche Informationen zu gewährleisten. Mit diesen Problemen wären auch Ermittlungen wegen Verstößen gegen die beabsichtigte

[8] Beck-Newsdienst, ZD-Aktuell 2012, 03007; Beck Fachdienst Strafrecht, FD-StrafR 2014, 357851.

Neuregelung des § 202d StGB konfrontiert. Denn die derzeit geltende Strafprozessordnung ist nicht geeignet, den Anforderungen an Ermittlungen im IT-Bereich in grundrechtskonformer Weise Rechnung zu tragen.[9] Unproblematisch ist der Zugriff allein dann, wenn die Ermittlungsbehörden Hardware in etwaig zu durchsuchenden Räumlichkeiten vorfinden, die dann ohne Frage Gegenstand einer Beschlagnahme nach den §§ 94 ff. StPO sein kann. Diese Ausgangslage entspricht jedoch nur selten der Realität. Denn potentiell inkriminierte bzw. beweiserhebliche Daten finden sich nicht selten auf externen Speichermedien. Das gilt vor allem in Zeiten der zunehmenden Nutzung von „Cloud Computing", also der dezentralen Speicherung im Wege einer bedarfsorientierten und online verfügbaren Nutzung von Soft- und Hardwarekapazitäten. Die Beschuldigten benötigen in solchen Fällen nicht einmal zwingend eigene Hardware, sondern benutzen nicht selten öffentlich zugängliche Rechner in Internetcafés oder Call-Shops. Die in der Strafprozessordnung vorgesehenen Ermittlungsmaßnahmen geraten in diesen Fällen oft an ihre Grenzen – daran ändert auch die geplante Pflicht zur Vorratsdatenspeicherung nichts. Das gilt insbesondere dann, wenn es sich um Sachverhalte mit transnationalem Bezug handelt.[10] Der Gesetzgeber betont selbst, dass die vermeintlichen Täter einer „Datenhehlerei" oft vom Ausland aus agieren.[11] Der Gesetzgeber würde hier demnach eine Strafnorm schaffen, zu deren effektiver (und zugleich rechtsstaatskonformer!) Durchsetzung ihm die Mittel bislang fehlen. Er ist demnach gehalten, zunächst die strafprozessualen Eingriffsnornen in grundrechts- und verfassungskonformer Weise an die Umstände moderner Telekommunikations- und IT-Nutzung anzupassen, bevor er – ohnehin nur vermeintliche – Strafbarkeitslücken materiell zu schließen versucht.

C. Zusammenfassende Stellungnahme

Sowohl in materieller als auch in prozessualer Hinsicht sprechen die besseren Argumente gegen den Erlass des neuen Strafgesetzes zur Datenhehlerei. So existiert schon keine zu schließende Strafbarkeitslücke bzw. kein Strafbedürfnis. Die Norm hätte überdies aufgrund der Probleme, die subjektiven Elemente (Bereicherungs- oder Schädigungsabsicht) nachzuweisen, wohl primär symbolischen Gehalt bzw. würde der Eröffnung strafprozessualer Maßnahmen zur Verfolgung eigentlich anderer Taten dienen – das darf aber gerade keine Begründung für die doch stark freiheitseinschränkende Ausweitung materiellen Strafrechts sein. Überdies fehlen bisher die Mittel zur effektiven Durchsetzung dieser (und anderer in diesem Kontext bereits existierender) Straftatbestände. Insgesamt ist deshalb die geplante Schaffung eines neuen § 202d StGB abzulehnen.

---

[9] Vgl. zu einer Beschreibung und Kritik einzelner Problemfelder *Meinicke* DSRITB 2012, 773 ff.
[10] Überblick zu den dabei aufkommenden Fragen bei *Bär* ZIS 2011, 53 ff.
[11] BT-Drucks. 18/1288, 1; RefE., 28.

Deutsche Gesellschaft für Recht und Informatik e.V.

Für ergänzende Erläuterungen steht Ihnen die Gesellschaft gerne zur Verfügung.

Mit freundlichen Grüßen, zugleich im Namen der Fachausschussleiter Prof. Dr. Susanne Beck, LL.M. und Rechtsanwalt Dirk Meinicke, LL.M.

Prof. Dr. Dirk Heckmann
1. Vorsitzender der DGRI