RUHR
UNIVERSITÄT
BOCHUM

RUB

RUHR-UNIVERSITÄT BOCHUM | 44780 Bochum | Germany

Juristische Fakultät

Juniorprofessur für Kriminologie, Strafrecht und Sicherheitsforschung im digitalen Zeitalter
Bochumer Fenster, Raum 7.22
Massenbergstraße 11, 44787 Bochum

JUN.-PROF. DR. SEBASTIAN GOLLA
Fon +49 (0)234 32-22280
sebastian.golla@rub.de
www.jura.rub.de/jpkrim

13. Mai 2021

Stellungnahme

zu dem Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Verbesserung des strafrechtlichen Schutzes gegen sogenannte Feindeslisten, BT-Drs. 19/28678

und

dem Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Überführung des § 42 des Bundesdatenschutzgesetzes in das Strafgesetzbuch zum verbesserten strafrechtlichen Schutz von persönlichen Daten, BT-Drs. 19/28777

Vorbemerkung: Die vorliegende Stellungnahme bezieht sich allein auf den Vorschlag der Einführung eines neuen Straftatbestandes des „Gefährdenden Verbreitens personenbezogener Daten“ (§ 126a StGB-E). Die in einem Änderungsantrag kurzfristig eingebrachten Vorschläge neuer Regelungen zur Strafbarkeit der Verbreitung und des Besitzes von Anleitungen zu sexuellem Missbrauch von Kindern (§ 176e StGB) sowie der verhetzenden Beleidigung (§ 192a StGB) konnten aus zeitlichen Gründen nicht berücksichtigt werden. Dass diese Vorschläge kein Gegenstand der schriftlichen Stellungnahme sind, lässt daher keinen Rückschluss auf ihre inhaltliche Einschätzung durch den Verfasser der Stellungnahme zu.

1. Die **Zielrichtung** des Gesetzesentwurfes ist nachvollziehbar. Die Verbreitung personenbezogener Daten politischer Gegner*innen kann geeignet sein, diese einzuschüchtern oder sogar zu Straftaten gegen diese führen. Dies kann auch das Klima des politischen Diskurses und der Meinungsbildung negativ beeinträchtigen.

Es erscheint allerdings nicht sinnvoll, diesen Risiken mit einem Straftatbestand zu begegnen, der auf den Schutz des **öffentlichen Friedens** zielt. Auch wenn Daten in geschlossenen Bereichen sozialer Medien oder in obskuren Kanälen, die der Öffentlichkeit nicht zugänglich sind, verbreitet werden, kann dies für die betroffenen Personen gefährlich werden. Handlungen in diesen Bereichen sind aber für sich genommen kaum geeignet, den öffentliche Frieden als „Bewusstsein der Bevölkerung, in Ruhe und Frieden zu leben“ (Schäfer, in MüKo-StGB, 3. Aufl. 2017, § 130 Rn. 22) nennenswert zu beeinträchtigen.

Es erschiene passender, Anpassungen im strafrechtlichen **Persönlichkeitsschutz** vorzunehmen, um den Gefahren, die von „Feindeslisten“ ausgehen, zu begegnen.

2. Die Ausgestaltung des Delikts als **Eignungsdelikt** ist zu weit und würde eine **Überkriminalisierung** mit sich bringen. § 126a StGB-E setzt voraus, dass die Verbreitung von personenbezogenen Daten geeignet ist, die betroffene oder eine ihr nahestehende Person der Gefahr eines gegen sie gerichteten Verbrechens oder einer gegen sie gerichteten sonstigen rechtswidrigen Tat gegen die sexuelle Selbstbestimmung, die körperliche Unversehrtheit, die persönliche Freiheit oder gegen eine Sache von bedeutendem Wert auszusetzen.

Wann die nötige konkrete Eignung zu einer Gefährdung besteht, ist **unklar**. Die Begründung des Entwurfes führt hierfür unter anderem den Kontext der Verbreitung (etwa auf extremistisch ausgerichteten Internetseiten), Bezüge zu Straftaten bei der Verbreitung und die Anonymität des Verbreitenden an. Rechtssicherheit geben diese Kriterien nicht. Der Schluss von der Anonymität des potentiellen Täters auf die Gefährlichkeit des Inhalts ist so allgemein nicht plausibel. Offen bleibt auch, nach welchen Kriterien die Verbreitung von Informationen in Medien mit Breitenwirkung geeignet sein kann, die Gefahr von Straftaten auszulösen.

Problematisch können auch Rückschlüsse von der tatsächlichen Begehung einer Straftat auf die Eignung einer vorigen Verbreitung von Daten für die Gefährdung des Opfers sein. Ist beispielsweise der Abdruck der Adresse einer Lokalpolitikerin im Telefonbuch geeignet, ihre Gesundheit zu gefährden, weil sich in einem konkreten Fall herausstellt, dass ein Angreifer die

Politikerin über die Gelben Seiten auffindbar gemacht hat? In sozialen Medien können außerdem spontane Kommunikationsdynamiken dazu führen, dass ein ursprünglich harmloser erscheinender Inhalt gefährlich wird.

Zwar lassen sich derartige Probleme in der Praxis der Strafverfolgung möglicherweise über das Vorsatzerfordernis korrigieren, dennoch können aus einem derart weiten Tatbestand erhebliche **Einschüchterungseffekte** folgen. Diese „chilling effects" könnten etwa für die öffentliche Meinungsbildung relevante Publikationen verhindern, obwohl nach § 126a Abs. 3 i.V.m. § 86 Abs. 3 StGB ein Tatbestandsausschluss für die Berichterstattung über Vorgänge des Zeitgeschehens gilt. Der Verweis auf § 86 Abs. 3 StGB dokumentiert zwar Bemühungen, ein Korrektiv für den weiten Tatbestand einzufügen. Er erfasst allerdings nicht sämtliche relevante Tätigkeiten, wie etwa von Laienjournalist*innen und Blogger*innen.

Einschüchterungseffekte, die aus dem sehr weiten Tatbestand für die Allgemeinheit folgen können, wiegen dann besonders schwer, wenn die Verfolgung der eigentlich bedrohlichen Verhaltensweisen praktisch kaum gelingt. Dann stehen geringen Erträgen der Verschärfung des Strafrechts hohe Freiheitsrisiken entgegen. Mit Blick auf den konkreten Vorschlag ist zumindest kritisch zu hinterfragen, ob die Verbreitung von „Feindeslisten", die etwa in geschlossenen Kanälen sozialer Medien erfolgt, in der Praxis tatsächlich zu einer nennenswerten Zahl strafrechtlicher Verurteilungen führen wird. Die negativen Effekte der Einführung des Tatbestandes scheinen seinen positiven Auswirkungen im Ergebnis zu überwiegen.

3. Der vorgeschlagene Straftatbestand verfolgt damit im Ergebnis zwar ein nachvollziehbares Ziel, ist aber **in seiner Ausgestaltung grundsätzlich verfehlt**. Ein strafrechtlicher Schutz vor der Verbreitung von Feindeslisten existiert zudem schon in § 42 Abs. 2 Nr. 2 BDSG, der die Verbreitung von Daten mit Schädigungsabsicht unter Strafe stellt. Eine Schädigungsabsicht ist auch dann anzunehmen, wenn Täter*innen ihre Opfer einschüchtern wollen (LG Aachen, Urteil vom 18.02.2011 – 71 Ns-504 Js). Selbst wenn der Nachweis des subjektiven Elements in manchen Fällen schwierig sein mag, ist diese Form der Regelung gegenüber der unklaren Anknüpfung an die Eignung zur Gefährdung einer Person vorzugswürdig.

Das **Datenschutzstrafrecht**, das das Bundesdatenschutzgesetz regelt, wird in der Praxis allerdings kaum wahrgenommen und angewandt. Gründe für das Schattendasein des

Datenschutzstrafrechts sind unter anderem die Unbestimmtheit der Regelungen, das Antragserfordernis und der Standort außerhalb des StGB.

Betrachtet man die vielfältigen Risiken, die vom Missbrauch personenbezogener Daten in der digitalisierten Welt ausgehen, wird das der Materie nicht gerecht. Es wäre sinnvoll, das Datenschutzstrafrecht **in das StGB zu integrieren** und seine Regelungen mit Blick auf bestimmte Risiken zu schärfen. Zu diesen Risiken gehört neben der Verbreitung von Feindeslisten das so genannte Doxing oder auch die Verarbeitung von Daten zur Erstellung von „Fakes“, um fremde Identitäten vorzutäuschen.

Es wäre daher zu begrüßen, einen Straftatbestand zur missbräuchlichen Verarbeitung – einschließlich der Verbreitung – personenbezogener Daten zu schaffen und diesen im 15. Abschnitt des Besonderen Teils (§§ 201 ff. StGB) zu integrieren. § 42 BDSG (und ggf. auch § 33 KUG) könnten dann gestrichen werden. Der in BT-Drs. 19/28777 hierzu unterbreitete Vorschlag sollte allerdings eine tatbestandliche Schärfung erfahren. Auch die Terminologie und der Umfang der Verweise auf das Datenschutzrecht sollten mit Rücksicht auf die Bestimmtheit angepasst bzw. reduziert werden.

Schließlich ist zu bedenken, dass das Strafrecht beim Schutz vor der Verbreitung von Feindeslisten und ihren Folgen **nicht das einzig Instrument** ist, das Abhilfe schaffen kann. Insbesondere Maßnahmen zum Schutze und der Beratung von Opfern derartiger Praktiken sind zu bedenken. Auch in der Regulierung von sozialen Medien könnte die Problematik Niederschlag finden, indem etwa Dienste wie Telegram zumindest bzgl. ihrer allgemein zugänglichen Bereiche verpflichtet werden, Schutzvorkehrungen gegen die Verbreitung von personenbezogenen Daten Dritter zu treffen.

Jun.-Prof. Dr. Sebastian Golla