

TOP 10:

Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei - Antrag des Landes Hessen -

Drucksache: 70/14

I. Zum Inhalt des Gesetzentwurfes

Mit der Gesetzesinitiative sollen Strafbarkeitslücken in Fällen des Handels mit rechtswidrig erlangten Daten durch die Einführung eines neuen Straftatbestands der Datenhehlerei (§ 202d StGB-E) geschlossen werden. Von der Regelung sollen nur die Daten, an deren Nichtweiterverwendung ein schutzwürdiges Interesse besteht und die nicht aus allgemein zugänglichen Quellen entnommen werden können, erfasst werden. Handlungen, die ausschließlich der Erfüllung gesetzlicher Pflichten durch Amtsträger oder deren Beauftragte dienen, werden nicht vom Tatbestand der Datenhehlerei erfasst (§ 202d Absatz 5 StGB-E).

Mit dem Gesetzentwurf soll der Strafrahmen für das unbefugte Ausspähen (§ 202a StGB) und Abfangen (§ 202b StGB) von Daten, also für die einschlägigen Delikte bei Angriffen gegen die Integrität, Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme und Daten, im Falle des Handelns mit Bereicherungs- oder Schädigungsabsicht mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bewehrt werden. Fälle des gewerbs- oder bandenmäßigen Handelns (Organisierte Kriminalität) sollen ausschließlich mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren bestraft werden. Der Versuch entsprechender Handlungen soll bereits strafbar sein.

Bei diesen Verletzungen des persönlichen Lebens- und Geheimbereichs durch Ausspähen von Daten (§ 202a Absatz 4 StGB-E), Abfangen von Daten (§ 202b Absatz 3 StGB-E) oder Datenhehlerei (§ 202d Absatz 3 StGB-E) in Fällen des gewerbs- oder bandenmäßigen Handelns (Organisierte Kriminalität) soll durch Änderungen der Strafprozessordnung auch eine wirkungsvolle Strafverfolgung ermöglicht werden. Die Bekämpfung der organisierten Cyberkriminalität könne nur dann wirksam erfolgen, wenn eine angemessene Sanktionierung aufgrund einschlägiger Tatbestände möglich ist und den Strafverfolgungsbehörden die zur wirkungsvollen Strafverfolgung notwendigen Mittel zur Verfügung gestellt werden. Durch eine Ergänzung des Strafgesetzbuches soll ausdrücklich klargestellt werden, dass Amtsträger oder deren Beauftragte beim Ankauf von Datenmaterial zur ausschließlichen Verwendung in einem Besteuerungsverfahren,

einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren nicht mit Strafe bedroht werden dürfen.

Den Strafverfolgungsbehörden sollen als notwendige Ermittlungsmaßnahmen ohne Wissen der Betroffenen die Überwachung und Aufzeichnung der Telekommunikation (§ 100a StPO) und das Abhören und Aufzeichnen des in einer Wohnung nichtöffentlich gesprochenen Wortes mit technischen Mitteln (§ 100c StPO) zur Verfügung stehen.

Zum Hintergrund wird in der Vorlage Folgendes angeführt:

Im Bereich der Informationstechnologie nimmt der Handel mit rechtswidrig erlangten digitalen Identitäten (z. B. Kreditkartendaten oder Zugangsdaten zu Onlinebanking, E-Mail-Diensten oder sozialen Netzwerken) immer mehr zu. Mit Schadsoftware werden über das Internet in großem Umfang Daten ausgespäht oder anderweitig rechtswidrig erhoben und auf Servern gespeichert. Die Täter, die sich solche Daten verschaffen, nehmen häufig selbst keine unmittelbaren Vermögensverfügungen mit den ausgespähten oder entwendeten Daten vor, sondern die widerrechtlich erlangten Daten aller Art werden über Webportale und Foren intensiv gehandelt. Entsprechende Angriffe werden häufig von internationalen, arbeitsteilig strukturierten Gruppen verübt, die in speziellen - meist nicht öffentlich zugänglichen - Diskussionsforen und Chat-Diensten eine breite Palette von Diensten anbieten und damit hohe Gewinne erzielen. Die Angriffe erfolgen zwar regelmäßig aus finanziellem Interesse, in manchen Fällen aber auch aus politischen Gründen mit zum Teil terroristischem Hintergrund. Der Gefahr dieses massenhaften Datenmissbrauchs kann bisher nicht ausreichend wirksam begegnet werden, weil die mit Bereicherungs- oder Schädigungsabsicht vorgenommene Weitergabe der rechtswidrig erlangten Daten selbst bisher nur in Teilbereichen von den bestehenden Strafnormen erfasst ist.

Das Bundesverfassungsgericht hat mit dem "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" (vgl. BVerfGE 120, 274 ff. - Urteil vom 27. Februar 2008) den besonderen strafrechtlichen Schutzbedarf in diesem Bereich verdeutlicht.

II. Zum Gang der Beratungen

Es handelt sich um einen Gesetzentwurf, den der Bundesrat bereits in der 17. Wahlperiode beim Deutschen Bundestag eingebracht hatte - vgl. BR-Drucksache 284/13 (Beschluss) -, der jedoch mit Ablauf der 17. Wahlperiode der Diskontinuität unterfallen ist.

Das Land Hessen hat die erneute Einbringung des Gesetzentwurfes beantragt und um sofortige Sachentscheidung in der Plenarsitzung am 14. März 2014 gebeten.