

Herbstkonferenz

10. November 2023 in Berlin



Beschluss

TOP II.9

Strafbarkeitslücke bei der heimlichen Überwachung mittels Bluetooth-Trackern und anderen Eingriffen in das Recht auf informationelle Selbstbestimmung durch Privatpersonen schließen

Berichterstattung: Hamburg und Bayern, Saarland, Mecklenburg-Vorpommern

1. Die Justizministerinnen und Justizminister haben sich mit dem strafrechtlichen Schutz vor unbefugter Erhebung und Verarbeitung personenbezogener Daten durch Privatpersonen befasst.
2. Sie stellen fest, dass die fortschreitende Digitalisierung insoweit Gefahren für die Persönlichkeitsrechte des Einzelnen verstärkt hat. Insbesondere seit der Einführung der Technologie von neuartigen Bluetooth-Trackern (sog. Air/SmartTags) zur Erleichterung der Suche nach leicht verlegbaren Gegenständen sind zunehmend auch missbräuchliche und kriminelle Nutzungen dieser Tracker – vor allem zur Ortung und Überwachung von Personen – zu verzeichnen.
3. Die Justizministerinnen und Justizminister sind sich darin einig, dass gegen solche erheblichen Eingriffe in das Recht auf informationelle Selbstbestimmung zur Gewährleistung eines konsequenten Opferschutzes auch mit den Mitteln des Strafrechts vorgegangen werden muss. Allerdings wird gerade das Phänomen des unbemerkten Einsatzes technischer Mittel zu Zwecken der Überwachung weder durch die bestehenden Straftatbestände des Strafgesetzbuchs noch durch solche des Nebenstrafrechts, etwa § 42 Bundesdatenschutzgesetz (BDSG), ausreichend strafrechtlich erfasst.

4. Die Justizministerinnen und Justizminister bitten daher den Bundesminister der Justiz, gegebenenfalls unter Einbindung der Bundesministerin des Innern und für Heimat, den konkreten strafgesetzgeberischen Handlungsbedarf zu prüfen und einen entsprechenden Regelungsvorschlag zu unterbreiten, um die aufgezeigte Strafbarkeitslücke zu schließen. Dabei sollte sich die Prüfung auch darauf erstrecken, ob und wie eine Modifikation und Überführung von § 42 BDSG in das Strafgesetzbuch zu Verbesserungen beim Schutz personenbezogener Daten vor Missbrauch führen kann.