Massendaten in Strafsachen – Probleme und Lösungen

21. September um 15:00 Uhr bis 16:30 Uhr

Referenten:	Oberstaatsanwalt Markus Hartmann, Staatsanwaltschaft Köln
	Dr. Dominik Brodowski, Open Competence Center for Cyber Security, Goethe Universität Frankfurt
	Jörg Bartholomy, Microsoft Deutschland GmbH
Moderation:	Dieter Kesper, Oberstaatsanwalt als Hauptabteilungsleiter, Staatsanwaltschaft Köln
Protokoll:	Dipl. jur. Alexander Gratz

Die Menge der Daten auf bei Durchsuchungen sichergestellten Computern und Datenträgern wird angesichts größerer Offline- und Online-Speicher ebenfalls größer. Diese Daten müssen bislang von der Staatsanwaltschaft, der Polizei oder Sachverständigen beim Verdacht des Besitzes bzw. der Verbreitung kinderpornographischer Schriften größtenteils manuell und zeitintensiv ausgewertet werden. Aus diesem Grund stehen Auswerteergebnisse oft erst nach Jahren zur Verfügung. Die Strafverfolgungsbehörden fragen sich daher: Ist in diesem Bereich der Einsatz von künstlicher Intelligenz technisch machbar? Und darf diese eingesetzt werden?

Für diesbezügliche Grundsatzfragen ist in Nordrhein-Westfalen die **Zentrale Ansprechstelle Cybercrime – ZAC NRW** – zuständig. Diese bietet den Staatsanwaltschaften des Landes Aus- und Fortbildung sowie die Unterstützung bei grundsätzlichen IT-Fragen an.

Die bisher zur Verfügung stehenden Software-Lösungen beschränken sich darauf, die Hashwerte (digitale Fingerabdrücke) von Bildaufnahmen darauf zu überprüfen, ob diese Aufnahmen bereits den Strafverfolgungsbehörden bekannt sind. Eine automatisierte inhaltliche Bewertung beliebiger digitaler Bildaufnahmen ist noch nicht möglich.

Jörg Bartholomy von der **Microsoft Deutschland GmbH** wies auf die von der Firma Microsoft in diesen Bereichen betriebene Forschung und Entwicklung hin. Es wird an Lösungen zur automatischen Erkennung von Fotoinhalten, Gesichtern oder des Alter einer abgebildeten Person gearbeitet. Die Gesichter oder Objekte können mit einer Datenbank abgeglichen werden. Eine derartige Software kann zudem einen Alarm auslösen, wenn Menschen in einem bestimmten Bereich nicht erkannt werden, da sie einen Helm oder eine Maske tragen sowie beim Abstellen verdächtiger Gegenstände.

Dominik Brodowski von der **Goethe Universität Frankfurt** hat zu den sich stellenden Rechtsfragen referiert. Um eine Strafbarkeit der beteiligten Personen beim Umgang bzw. der automatisierten Auswertung von Datenträgern mit mutmaßlich kinder- und jugendpornographischem Inhalt zu vermeiden, darf die Tätigkeit nicht über den im Tatbestandsausschluss des § 184b Abs. 5 StGB definierten Rahmen hinausgehen. Die Übertragungswege der Daten zur Cloud sollten auf das Inland beschränkt werden. Sobald die Daten nicht mehr zur Strafverfolgung erforderlich sind, müssen sie unverzüglich gelöscht werden. Aus dem Datenschutzrecht folgt zudem eine Verpflichtung zur hinreichenden

Gewährleistung von IT-Sicherheit. Die Abwägung, ob das Restrisiko, dass Daten im Rahmen der Inanspruchnahme privater Cloudlösungen nach außen gelangen, eingegangen werden darf, ist eine politische Grundentscheidung.