

05.11.2024

# Antrag

der Fraktion der CDU  
und der Fraktion BÜNDNIS 90/DIE GRÜNEN

## **Eine moderne Kriminalpolizei zur digitalen Kriminalitätsbekämpfung**

### **I. Ausgangslage**

Die nordrhein-westfälische Polizei ist in vielen Bereichen der digitalen Polizeiarbeit bereits gut aufgestellt. Ermittlerinnen und Ermittler der Direktionen Kriminalität und Verkehr können jetzt schon beispielsweise Onlinevernehmungen von ihrem Arbeitsplatz aus durchführen. Auch bildet die Polizei Cyberkriminalistinnen und -kriminalisten in einem Studiengang am Cyber Campus NRW aus, um auch der stetig wachsenden Anzahl an digitalen Tatorten begegnen zu können.

Die Landesregierung hat die nordrhein-westfälische Kriminalpolizei in den letzten Jahren bereits personell und technisch besser aufgestellt. Die Entwicklungen im digitalen Raum vollziehen sich jedoch rasant. Die Innovationskraft von Cyberkriminellen nimmt ständig zu. Hacker beschreiten immer neue Wege, um ganze Systeme lahmzulegen, persönliche Daten zu entwenden und Schadsoftware in großem Umfang zu verbreiten. Längst haben digitale Begehungsformen Einzug in die Alltagskriminalität gefunden, um im Schutze der Anonymität z.B. Betrug im Online-Handel zu begehen. Parallel dazu nimmt die Verbreitung von Hass und Hetze durch koordinierte Gruppen im Internet zu, wobei Frauen und marginalisierte Gruppen überproportional häufig und intensiv betroffen sind. Auch Islamistinnen und Islamisten sowie rechtsradikale Gruppierungen werben online um neue Anhängerinnen und Anhänger und finden ständig neue Formen der Radikalisierung. Daher hat sich die Landesregierung mit dem Maßnahmenpaket nach dem islamistischen Terroranschlag von Solingen darauf verständigt, dass sog. „virtueller Ermittler“ eingesetzt werden, die die sozialen Medien „digital bestreifen“, um Straftaten vorzubeugen und begangene Straftaten zu verfolgen.

Bei Ermittlungsverfahren im Zusammenhang mit den Abbildungen sexualisierter Gewalt werden häufig sehr umfangreiche Datenmengen sichergestellt, die kategorisiert und ausgewertet werden müssen. Insbesondere in Fällen einer noch bestehenden Gefährdungssituation ist es von besonderer Bedeutung, schnelle Ermittlungserfolge zu erreichen, um Opfern schnell helfen zu können. Die Verbreitung von Missbrauchsabbildungen erfolgt überwiegend über elektronische Kommunikationswege. Hier bestehende komplexe Netzwerke und Strukturen aufzudecken und alle abgebildeten Personen zu identifizieren, stellt die Polizei vor große Herausforderungen, denen sie nicht ohne moderne Technik und Künstliche Intelligenz (KI) gewachsen ist.

In sozialen Netzwerken schreiben meist männliche Täter gezielt minderjährige Mädchen an und versuchen, an private Bilder zu gelangen oder sogar persönliche Treffen zu forcieren. Der Schutz von Jugendlichen und Kindern ist hier nur mit hohem Personaleinsatz möglich. Mit technischer Unterstützung kann der Druck auf die Täter und Täterinnen maßgeblich erhöht werden. Deshalb wurden das LKA und die Kriminalhauptstellen technisch und personell bereits gestärkt. Zudem wurde die IT verbessert. Beispielsweise, indem virtuelle Auswerterechner („Forensik Desktop“) angeschafft wurden, wodurch zentral die wesentlichen Anwendungen zur Aufbereitung und Auswertung von IT-Daten vorgehalten werden. Die effektive und verhältnismäßige Rechtsdurchsetzung muss auch bei Straftaten, die mittels digitaler Technologie verübt werden, gewährleistet sein. Dies erfordert vor allem spezialisiertes Fachpersonal bei der Kriminalpolizei und muss mit präventiven Maßnahmen sowie umfassender Unterstützung und Beratung einhergehen.

Zu diesem Zweck wurden eigene Kriminalinspektionen mit dem Schwerpunkt Cybercrime in den sechs § 4-Behörden eingerichtet. Die Kriminalinspektionen bündeln die Fachkompetenz der Kriminalpolizei, um Ermittlungen im Bereich Cybercrime effektiv voranzutreiben. Die Kriminalinspektionen und das Cyber-Crime-Competence-Center des LKA kooperieren eng mit Polizeibehörden auf Bundesebene sowie im Ausland, denn Cybercrime macht keinen Halt an nationalen Grenzen.

Die Kriminalinspektionen Cybercrime zeichnen sich durch ihre gut aufgestellten digitalen Interventionsteams aus. Diese reagieren schnell und effektiv auf akute Cyberbedrohungen und digitale Kriminalität und unterstützen fachkompetent Betroffene. Dabei unterstützen sie nicht nur Unternehmen und Organisationen bei der Bewältigung von IT-Sicherheitsvorfällen, sondern beraten auch bei der Verbesserung der IT-Sicherheit, um entsprechenden Angriffen langfristig besser vorzubeugen. Die Teams verfügen über mobile high end Labore, damit sie unmittelbar Hilfe vor Ort leisten können.

Die Einrichtung hochspezialisierter Fachteams allein reicht für eine effektive Bekämpfung von Cybercrime nicht aus. Vielmehr ist es unerlässlich diese Expertengruppen mit modernster technischer Ausrüstung auszustatten, um ihre Einsatzfähigkeit auf dem höchstmöglichen Niveau zu gewährleisten.

Dafür entwickelt die Polizei eigene innovative Apps, die den Alltag der Kriminalistinnen und Kriminalisten langfristig erleichtern. Die denkbaren Anwendungsfelder sind mannigfaltig. Beispielsweise sind Anwendungen im Bereich „digitale Vernehmung“, zur Aufnahme einer Strafanzeige, zur Identifizierung mittels eines Fingerabdrucks oder zur Durchführung einer Leichenschau denkbar.

Auch Anwendungen, die mit KI arbeiten, haben das Potential, die Arbeit der Kriminalpolizei langfristig erheblich zu erleichtern. Die Europäische Union hat mit dem AI-Act einen klaren Rechtsrahmen geschaffen. Der AI-Act verbietet KI-Systeme, die menschliches Verhalten manipulieren, um den freien Willen der Nutzerin oder des Nutzers zu umgehen, sowie Systeme, die ein „Social Scoring“ ermöglichen. Bei der Entwicklung und dem Einsatz von KI-Anwendungen durch die Polizei ist entscheidend, dass Transparenz, Nachvollziehbarkeit und Nichtdiskriminierung bei der Verarbeitung von Daten sichergestellt sind. Der Menschenrechtsschutz, die informationelle Selbstbestimmung sowie die informationstechnische Integrität und Sicherheit sind bei jedem Arbeitsschritt mitzudenken und bilden den Maßstab, an dem sich der Einsatz von KI stets messen lassen muss.

Unter Zugrundelegung dieser Maßstäbe lässt sich ein hohes Potential zum Einsatz von KI identifizieren. KI-Systeme können vielfältig eingesetzt werden, etwa zur Umwandlung von Worten in geschriebene Texte und umgekehrt, verbunden mit simultaner Übersetzung in

verschiedene Sprachen. Dabei können auch technische Übersetzungsmöglichkeiten für seltene Sprachen und Dialekte geschaffen werden, die bereits durch das Maßnahmenpaket der Landesregierung nach dem islamistischen Terroranschlag von Solingen in den Fokus gerückt wurden. Automatische Textqualifikation, Auswertung großer Textmengen und Objekterkennung kann unkompliziert durch KI erfolgen. Durch die Objekterkennung können beispielsweise verfassungsfeindliche und verbotene Symbole erkannt und mobilen Einsatzkräften auf ihren Handys für den Einsatz bei Versammlungen zur Verfügung gestellt werden. Menschenverachtende Organisationen bedienen sich einem sich stets weiterentwickelnden Repertoire an Symboliken, die dechiffriert werden müssen. Das kann KI mühelos bewerkstelligen. KI kann so Kriminalistinnen und Kriminalisten als Assistenz die tägliche Arbeit erheblich erleichtern und zur Bekämpfung von Kriminalität sach- und vor allem zeitgerecht beitragen. Wo Gesetze und Vorschriften menschlichen Ermessensspielraum vorsehen, darf dieser jedoch niemals von KI übernommen werden.

Digitalisierung bietet immer auch digitale Schnittstellen für die Anbindung von technischen Einrichtungen zum Abbau von Barrieren. Dies betrifft beispielsweise Programme für Menschen mit Behinderung, die auf technische Unterstützung zur Erfassung oder Erstellung von Texten angewiesen sind. Der Einsatz von KI kann auch Sprachbarrieren verringern, indem sowohl das gesprochene als auch das geschriebene Wort übersetzt werden kann. Dieser erleichtert die Zugänge zur nordrhein-westfälischen Polizei für Menschen, die nicht über deutsche Sprachkenntnisse verfügen.

Zudem wappnet sich Nordrhein-Westfalen für eine digitale Zukunft. Eine Reihe von Forschungsprojekten untersucht das Potential neuer digitaler Anwendungen für die polizeiliche Arbeit. Das Ziel ist, gesellschaftlich verantwortungsvolle und gleichzeitig effiziente soziotechnische KI-Systeme zu entwerfen.

Der Weg der nordrhein-westfälischen Kriminalpolizei zu einer bundesweit führenden Rolle muss weiter forciert werden. Sie kann damit Vorbild bei der Digitalisierung der Sicherheitsbehörden unter Wahrung eines hohen Standards an Bürgerrechten werden.

## **II. Beschlussfassung**

Der Landtag stellt fest:

- Die Kriminalpolizei stellt sich den Herausforderungen der digitalen Transformation.
- Eine wirksame Bekämpfung der digitalen Kriminalität verlangt nach exzellentem Fachpersonal, moderner Ausstattung, präventiven Maßnahmen sowie einer umfassenden Unterstützung und Beratung der Betroffenen.
- Die Kriminalinspektionen mit dem Schwerpunkt Cybercrime sind ein Erfolgskonzept.
- Cybercrime kennt keine Landesgrenzen. Eine Länder- und Bundesgrenzen überschreitende Kooperation mit Ermittlerinnen und Ermittlern im Bereich Cybercrime ist deshalb Kernelement einer effektiven Bekämpfung.
- Transparenz, Nachvollziehbarkeit und Nichtdiskriminierung bei der Verarbeitung von Daten sind bei der Entwicklung und Anwendung von KI sicherzustellen.
- Daten- und Menschenrechtsschutz, die informationelle Selbstbestimmung, sowie die informationstechnische Integrität und Sicherheit sind der Maßstab, an dem sich Entwicklung und Anwendung von Systemen Künstlicher Intelligenz messen lassen muss.

Der Landtag beauftragt die Landesregierung im Rahmen vorhandener Mittel,

- die digitalen Kompetenzen der Ermittlerinnen und Ermittler in allen Kriminalitätsphänomenen weiter auszubauen.
- hochqualifizierte Fachkräfte im Spektrum der digitalen Entwicklung durch Personalentwicklungsmöglichkeiten an die Polizei zu binden.
- eine personelle Vollbesetzung der digitalen Interventionsteams anzustreben und voranzutreiben.
- die Projekte zu den Themen Speech-to-Text, automatische Textklassifikation, Objekterkennung und Auswertung großer Datenmengen weiter zu fördern.
- die Entwicklung der kriminalfachlichen App „digitale Vernehmung“ weiterzuführen und zu prüfen, ob weitere kriminalfachliche Apps, wie z.B. zur Durchführung der Fast-ID (Identifizierung mittels Fingerabdrucks) sowie zur Durchführung einer Leichenschau, entwickelt werden können.
- Transparenz, Nachvollziehbarkeit und Nichtdiskriminierung stets bei der Verarbeitung von Daten sicherzustellen.
- Forschungsprojekte, die NRW dabei helfen, digitale Entwicklungen vorzudenken, auch im engen Austausch mit den Hochschulen und Universitäten sowie internationalen Partnern, weiter zu unterstützen und voranzutreiben.

Thorsten Schick  
Matthias Kerkhoff  
Gregor Golland  
Dr. Christos Katzidis  
Angela Erwin

und Fraktion

Wibke Brems  
Verena Schäffer  
Mehrddad Mostofizadeh  
Dr. Julia Höller  
Dorothea Deppermann

und Fraktion