Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 G

bitkom

Stellungnahme

< April 2024>

Anhörung des Innenausschusses des Deutschen Bundestages zum Projekt „VeRA“ am 22.04.2024

Bitkom nimmt grundsätzlich keine Stellung zu den Angeboten einzelner Mitgliedsunternehmen, um hier Neutralität zu wahren.

Zentrale Herausforderung im Umgang mit großen Datenmengen

- Weltweit beträgt das Datenvolumen etwa 64,2 Zettabyte. 2025 werden es laut Europäischer Kommission bereits 175 Zettabyte sein. Das Verarbeiten großer Datenmengen ist bereits heute eine große Herausforderung für die Sicherheitsbehörden, da der Großteil davon unstrukturierte Daten sind. Allein in der Polizei Niedersachsen sind etwa 7,5 Petabyte Daten gespeichert. Diese Menge an Daten würde etwa 150 Millionen Aktenschränke füllen.

- Durch den weiteren Anstieg an Sensoren, mobilen Endgeräten (Smartphones, Tablets, etc.) sowie den Kapazitäten auf Speichermedien, wird diese Herausforderung weiter steigen. Hinzu kommt, dass sich Kriminalitätsphänomene immer weiter in den digitalen Raum verlagern und Sicherheitsbehörden stärker mit Daten in digitaler Form konfrontiert sind. (z.B. Daten aus Ermittlungen, Anzeigen, Kinderpornographie, Cybercrime usw.) Dies erfordert den Aufbau von weiteren Behördenkompetenzen, u. a. in der digitalen Forensik, Open Source Intelligence (OSINT) und der Analyse.

- Es stellen sich technische Fragen nach Speicherkapazitäten, Rechenkapazitäten sowie geeigneter Software zur Auswertung dieser Daten. Diese Herausforderungen können nur im Dreiklang aus Politik (Rahmensetzung), Behörden (Durchführung) und Wirtschaft (Digitale Kompetenzen und Ressourcen) konstruktiv und kooperativ gelöst werden.

- Eine Vernetzung von Analyse und Auswertung soll Schnelligkeit schaffen und Redundanzen verhindern und muss gleichzeitig mit einem aktiven Wissensmanagementsystem ausgestattet sein. Die eingesetzte Software muss daher große Datensätze strukturiert und nutzerfreundlich bearbeiten können. Dadurch entstehende Datenräume müssen auf gemeinsamen Standards (oder Werten, Technologien, Schnittstellen) basieren und die Transaktion von Daten erlauben und befördern. [1]

- Derzeit sind die Sicherheitsbehörden dazu nur eingeschränkt in der Lage. So sind die Behörden allein am Beispiel der Verfolgung aller Verdachtsfälle im Bereich Geldwäsche durch die Masse an Daten gelähmt, sodass eine Verfolgung nur rudimentär erfolgt, bzw. Erfolge bei der Polizei eher im geringfügigen Bereich liegen. Auch ist die Bearbeitung und Verfolgung eingehender digitaler Anzeigen kaum noch möglich, geschweige denn ein Feedback an die Anzeigenden. Die Folge ist ein zunehmender Verlust von Vertrauen der Bevölkerung in die Fähigkeiten der Sicherheitsbehörden. Die digitale Arbeitsfähigkeit staatlicher Einrichtungen sicherzustellen ist letztlich

Das für Sicherheitsbehörden auszuwertende Datenvolumen steigt stetig. Die meisten Daten sind dabei unstrukturiert. Die Fähigkeit zur vernetzten Analyse & Auswertung ist zentral für das Funktionieren des Staatsgefüges und derzeit nur eingeschränkt möglich.

[1] Herausforderungen der Polizei durch die digitale Transformation | Positionspapier 2023 | Bitkom e. V.

eine Voraussetzung für das Vertrauen der Bürgerinnen und Bürger in staatliche Institutionen.

- Ziel muss die Automatisierung von Verwaltungsprozessen sein, die eine medienbruchfreie Übermittlung von Daten innerhalb der Bundesländer, zwischen den Bundesländern und letztlich bis hin zum Bund ermöglicht. Diese Daten müssen analysiert und die Ergebnisse zeitnah der Justiz zur Einleitung möglicher Strafverfolgungsmaßnahmen bereitgestellt werden können.

- Eine solche Software muss aber nicht nur die Nutzung des Potentials der Datenanalyse für die Polizeiarbeit ausschöpfen, sie muss auch den Erfordernissen des Daten- und Grundrechteschutzes sowie der Informationssicherheit gerecht werden. Der verantwortungsvolle, sichere und rechtmäßige Umgang mit Daten durch Sicherheitsbehörden und eine zeitgemäße gesetzliche Regelung sind die Schlüssel für Innovationen und Vertrauen in eine moderne Polizeiarbeit. Weiterhin sind Souveränitätsaspekte zu berücksichtigen.

Software im Bereich der Sicherheitsbehörden muss grundsätzlich den Erfordernissen des Daten- und Grundrechteschutzes sowie der Informationssicherheit gerecht werden.

Bedeutung digitale Souveränität

- Digitale Souveränität bedeutet nicht Autarkie, sondern unabhängige digitale Selbstbestimmung: Es geht darum, die Wahl zu haben etwa zwischen eigenen Lösungen (z.B. eigenständige Lösungen der Behörden) und denen vertrauensvoller (auch internationaler) Partnerinnen und Partner (marktverfügbar oder als beauftragte Entwicklung).

- Digitale Souveränität ist die Möglichkeit zur digitalen Handlungs- und Gestaltungsfreiheit. Das bedeutet Mitgestaltungs- und Innovationsspielräume zu erhalten. Die Fähigkeit international auf Augenhöhe Schlüsseltechnologien, Geschäftsmodelle und Ökosysteme mitzugestalten, sowohl durch Forschung als auch durch Entwicklung, in der Mitgestaltung internationaler Standards und als Kunde und Partner.[2]

- Aus sicherheitspolitischer Perspektive muss in besonders kritischen Bereichen immer eine Risikoabwägung stattfinden. So ist eine vollständige Neuentwicklung von bereits auf dem (globalen) Markt verfügbaren Lösungen zwar sehr kosten- und zeitintensiv, kann aber nach Abwägung aller Chancen und Risiken einen Mehrwert haben, wenn es um Kernkomponenten im Bereich der nationalen Sicherheit geht. Andererseits lassen sich solche komplexen Systeme immer weniger in Eigenentwicklungen aufbauen oder gar betreiben. Gerade hinsichtlich geeigneter Software sollten neben der Digitalwirtschaft auch innovative Forschungsinstitutionen einbezogen werden, um Zugang zu zukunftsfähigen Lösungen zu erhalten.

- Europa und Deutschland müssen dort technologische Kernkompetenzen weiter ausbauen, wo Expertise, Marktanteile und Innovationskraft vorhanden sind, bzw. in der Zukunft entwickelt werden können. Das umfasst die Fähigkeit, die weltweit bereits bestehenden und neu entstehenden Technologien auf ihre Vertrauenswürdigkeit hin zu bewerten und in die eigenen Produkte, Prozesse, Organisationen und in die Gesellschaft zu integrieren, um dadurch Wertschöpfung zu erzielen und die Wachstums- und Wettbewerbsfähigkeit der deutschen und europäischen Wirtschaft in Kernfeldern abzusichern und auszubauen. Schlüsseltechnologien müssen daher systematisch betrachtet und entwickelt werden, so dass rechtzeitig eigene Kompetenzen in besonders wichtigen Bereichen aufgebaut werden können. Dazu gehört auch der Aufbau und Erhalt eines entsprechenden Anbieterökosystems in Europa in Bereichen, die als Schlüsseltechnologie identifiziert wurden.

Digitale Souveränität bedeutet nicht Autarkie, sondern unabhängige digitale Selbstbestimmung. Dies umfasst die Fähigkeit zwischen vertrauensvollen Partnern zu wählen.

[2] Vgl. auch Bitkom 2020.

Lösungsansätze bei großen Datenmengen

- **Monetäre Herausforderungen meistern:** Die öffentliche Haushaltslage ist angespannt. Notwendige Investitionen sind dadurch schwieriger durchzuführen. Gleichwohl steht der Haushalt gestiegenen Anforderungen gegenüber, u. a. an die Öffentliche Sicherheit und an den Schutz kritischer Infrastrukturen. Digitale Lösungen müssen daher verstärkt Interoperabilität, auf Basis offener Standards, gewährleisten.

- **Personelle Voraussetzungen und Qualifikationen von Behördenpersonal:** Gleichzeitig ändert sich das Aufgabenprofil der Beschäftigten der Sicherheitsbehörden. Sie werden zusätzlich zu ihren Tätigkeiten, zukünftig u. a. stärker mit dem Auswerten großer Datenmengen konfrontiert sein. Die Ausbildung muss daher in diesem Bereich angepasst werden. Es sollten auch andere Möglichkeiten in Betracht gezogen werden: Der Quereinstieg (entsprechend ausgebildeter Personen) oder das Einkaufen von externer Fachexpertise sind Möglichkeiten, diesen Herausforderungen zu begegnen.

- **Management der Sicherheitsbehörden-Landschaft**
  Die föderale Struktur in der Bundesrepublik macht die Koordinierung von Aktivitäten der Sicherheitsbehörden nicht leicht. Gerade, weil insbesondere die Polizeiarbeit in die Zuständigkeit der Länder fällt. Nicht alle Daten stehen allen Beteiligten in Bund und Ländern immer zur Verfügung, sodass bei übergreifenden Kriminalitätsphänomenen zum Teil nicht die richtigen Analysen durchgeführt- und Schlussfolgerungen in Ermittlungsprozessen gezogen werden können. Das gilt sowohl im nationalen Raum (über Grenzen der Bundesländer), als auch im internationalen Raum (über Ländergrenzen). **Eine zentrale Analyse unter den gegebenen Sicherheitsaspekten, könnte einen großen Mehrwert für die Sicherheitsbehörden enthalten. Gleichzeitig könnten Infrastrukturen dadurch effizienter genutzt werden. Bislang ist eine zentrale, länderübergreifende Datenverarbeitung nur eingeschränkt möglich.**

  Dabei ist die Anpassungsfähigkeit und Erweiterbarkeit von IT-Lösungen, unter Einbeziehung der Nutzenden, wichtig. So lassen sich Abhängigkeiten zu einzelnen Anbietern vermeiden.

Eine übergreifende Analysefähigkeit kann großen Mehrwert für die Sicherheitsbehörden bieten.

IT-Lösungen sollten anpassbar und erweiterbar sein, um nicht in Abhängigkeiten zu einzelnen Anbietern zu geraten.

Dabei ist die Orientierung an den Bedürfnissen der Nutzenden essentiell.

Optionen für die Sicherheitsbehörden zum Erhalt relevanter Fähigkeiten

a) Die Erstellung von Eigenlösungen durch die Sicherheitsbehörden

- Grundsätzlich können die Behörden selbst am besten beurteilen, welche Lösungen sie benötigen. Die Erstellung eigener Lösungen kann jedoch dauerhaft erhebliche Personal-, Material- und finanzielle Ressourcen binden und kann unter Umständen deutlich teurer als die Beschaffung marktverfügbarer Lösungen sein, ohne gleichzeitig in Sachen Erprobung und Updates wettbewerbsfähig zu sein.

- Hinzu kommt, dass sich die technologischen Innovationszyklen immer schneller vollziehen. Dies bedingt eine permanente Betreuung technischer und rechtlicher Aspekte, um rechtssichere Lösungen zu erstellen. Dies bedeutet eine starke Bindung von Fachpersonal, welches perspektivisch immer schwerer zu finden sein wird.

- Zu bedenken ist, dass Software nie „zu 100 % fertig“ ist. Sie muss dauerhaft weiterentwickelt und betreut werden, in enger Abstimmung mit relevanten Stakeholdern wie Endnutzenden, Datenschutz- und Informationssicherheitsbeauftragten usw. Personal und Haushaltsmittel müssen also von der Planung über die initiale Entwicklungsphase bis hinein in den Betrieb und die Wartung der Software in auskömmlicher Weise zur Verfügung stehen.

b) Die Erstellung von Innovationslösungen durch die Sicherheitsbehörden mit der Wirtschaft und Wissenschaft

- Die Erstellung von Softwarelösungen im behördlichen Auftrag kann nur gelingen, wenn ausreichende Haushaltsmittel und notwendige Priorisierungen von Projekten in den einzelnen zuständigen Landespolizeien oder im Bund vorliegen.

- Kernherausforderung ist hier, dass Bedarfe, Aufgaben einzelner Polizeien und dazu nötige Ressourcen (Personal, Finanzen, politische Zielsetzung etc.) meist getrennt sind. Es bedarf daher stets einer Koordinierung verschiedener Akteure, was Prozesse in die Länge zieht und Enttäuschungen bei den Nutzenden erzeugt.

- Das Programm P20 (früher P2020) sollte diese Herausforderung lösen, wobei sich die Bundesländer teilweise schwertun, um das Programm mit Impulsen zu beleben. (nötige personelle Faktoren auf Landesebene). Auch bleibt das Programm hinter den Erwartungen zurück. Dabei geht es u.a. um Priorisierungen, wo es unterschiedliche Auffassungen gibt.

- Chancen bestehen durch die Einbeziehung aufgebauter Reallabore, u.a. der GovTechCampus in Berlin.

- Lösungen in Reallaboren lassen sich schneller skalieren. Zur Umsetzung stellen Experimentierklauseln zentrale Bausteine dar, um den Rechtsrahmen innovationsoffen und zukunftsorientiert zu gestalten. Bei der Formulierung von rechtssicheren und innovationsoffenen Experimentierklauseln kann eine Handreichung des Bundesministeriums für Wirtschaft und Klimaschutz helfen.[3] Dabei sollte ein einfacher und transparenter Zugang zum Reallabor für alle relevanten Stakeholder (Sicherheitsvorkehrungen inkl.), u. a. für Industrie, Wissenschaft und andere Teilstreitkräfte vorhanden sein. Dabei darf es zu keinen Wettbewerbsnachteilen kommen, etwa durch die strenge Auslegung von Compliance-Regeln. Ggf. bedarf dies auch der Anpassung von Doktrinen. Es dürfen keine Denkverbote bestehen und die Verantwortlichen sollten die Möglichkeit haben, mit eigenen Mitteln zu wirtschaften.
  Dazu bedarf es eines eindeutigen politischen Mandats für den GB BMI.

- Das Reallabor sollte auch über ausreichende solvente Mittel, z. B. Handgeld, Studienmittel oder weitere niederschwellige Sofortmaßnahmen verfügen. Reallabore sind unter dem HUB-Gedanken zu führen, wobei die Sicherheitsbehörden ihren Bedarf und dazugehörige Lösungen suchen (pull) und diese gemeinsam mit der Industrie oder Wissenschaft, unter Einbezug der Nutzenden, entwickelt. Umgekehrt sollte es jedoch auch möglich sein, dass die Industrie proaktiv Lösungsansätze einbringt. Teststellungen müssen skalierbar sein und stets Klarheit über Zielsetzung, Finanzierung und Betriebszeit, auch über Haushaltsjahre hinweg, sicherstellen.
  Operationelle Feldtests (Praxis) müssen ebenso durchführbar sein, wie digitale Simulationen im AR- und VR-Bereich (Simulation), um wo immer möglich auch eine regulatorische Basis zu schaffen. Es bedarf zudem transparenter Vorgaben zur Evaluation von Ergebnissen, über Skalierungsmöglichkeiten der Innovation nach dem Reallabor, sowie Vorgaben zur Veröffentlichung von Ergebnissen und der Einbindung relevanter Partner. Dabei sollten Unternehmen erarbeitete Lösungen auch weiter vermarkten können. Es sollte aber auch Klarheit darüber herrschen, wer Zugriffs- und Eigentumsrechte auf Daten und Lizenzen, sowie ungenutzte digitale Kapazitäten hält.

Grundsätzlich besteht die Option Lösungen selbst zu erstellen, entwickeln zu lassen oder marktverfügbar zu kaufen.

Dies bedingt einen funktionierenden Marktdialog, und den Zugriff auf ein leistungsfähiges Ökosystem aus Staat-Wirtschaft-Wissenschaft.

Die Faktoren Zeit-Kosten-Personal sind dazu abzuwägen.

[3] Reallabore – Recht flexibel (bmwk.de)

c) Der Einkauf marktverfügbarer Lösungen durch die Sicherheitsbehörden

- Grundsätzlich sollten marktverfügbare Lösungen im Fokus stehen, um doppelte Entwicklungen (das Rad neu erfinden) zu vermeiden und Ressourcen zu sparen. Voraussetzung dazu ist, dass die Anforderungen an Datenschutz, Informationssicherheit, Transparenz, Interoperabilität sowie Gerichtsfestigkeit der Ergebnisse gesichert werden können.

- Unternehmen benötigen dazu relevante Erfahrungen über Bedarfe und Anforderungen im Umgang mit Sicherheitsbehörden.

- Wichtig ist dabei einen „Lock-In" zu vermeiden oder zumindest zu reduzieren. Eine einmalig gekaufte Lösung darf zu keiner dauerhaften Abhängigkeit von einem bestimmten Lieferanten führen.

- Der Kauf marktverfügbarer Lösungen bedingt einen funktionierenden Marktdialog. Der Markt benötigt Kenntnis darüber, welche Fragestellungen für die Sicherheitsbehörden von Relevanz sind, inkl. eines Feedbacks zu eigenen Lösungsansätzen durch die Behörden.

- Dazu genügt es nicht nur den Markt nach Lösungen zur durchsuchen oder durch Roadshows Ideen der Sicherheitsbehörden zu forcieren. Es gilt einen strukturierten Dialogansatz zwischen Staat-Wirtschaft-Wissenschaft zu implementieren, um Bedarfe der Sicherheitsbehörden mit Kapazitäten, Best Practice etc. der Wirtschaft und Wissenschaft abzugleichen.

- Vor dem Hintergrund der digitalen Souveränität gilt es zu priorisieren, welche Schlüsselaspekte national, europäisch oder international bei befreundeten Nationen beschafft werden können. Dies erfordert auch eine leistungsfähige nationale industrielle Basis. Neue Technologien kommen meist aus dem zivilen Bereich. Daher müssen diese unter Achtung geltenden Rechts in Sicherheitsbehörden adaptiert werden können. Dabei gilt es auch, verfügbare Forschungsansätze in die Praxis zu integrieren.

- Insbesondere die Digitalwirtschaft ist auf Effektivität und Effizienz ausgerichtet. Lösungsansätze werden in wenigen Stunden erdacht und in wenigen Wochen umgesetzt. Produkte bzw. Gewerke werden jedoch erst entwickelt, wenn ein skalierbarer Markt (ausreichender Bedarf, gemessen an Finanzvorlumen, Verständnis zu realem Bedarf von Nutzenden etc.) vorhanden ist. Gelingt dies nicht, so werden sich innovative Unternehmen weiterhin dem zivilen Sektor zuwenden.

- Vergabestellen müssen diesem Umstand Rechnung tragen, u.a. im Bereich der Bearbeitungszeiten, aber auch der Form der Ausschreibung. Ggf. existieren sogar Lösungsansätze, die durch zu enge oder unattraktive Ausschreibungsbedingungen nicht zum Tragen kommen.

- Ein Vorschlag zum verbesserten Marktdialog ist die Durchführung von Marktschautagen zu Themen von Interesse im Rahmen vorkommerzieller Beschaffungsverfahren (PCP). Bei PCP „kaufen öffentliche Auftraggeber Research & Development (R & D) von mehreren konkurrierenden Anbietern, um alternative Lösungsansätze zu vergleichen und das beste Preis-Leistungs-Verhältnis zu ermitteln, das der Markt liefern kann, um seinen Bedürfnissen gerecht zu werden. R & D gliedert sich in Phasen (Lösungsdesign, Prototyping, ursprüngliche Entwicklung und Validierung bzw. Tests einer begrenzten Reihe von ersten Produkten), wobei die Anzahl konkurrierender R&D-Anbieter nach jeder R&D-Phase reduziert wird."[4] Dieses Verfahren wird u. a. auch erfolgreich durch die Cyberagentur des Bundes genutzt, wodurch sich hier Erfahrungswerte adaptieren lassen. Wichtig ist dabei, dass mittels veröffentlichter und konkreter Problembeschreibung die Industrie zum Pitch für die (Teil-)Lösung aufgefordert ist.

[4] Pre-Commercial Procurement - European Commission (europa.eu)

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Stephan Ursuleac | Bereichsleiter Verteidigung & Öffentliche Sicherheit
s.ursuleac@bitkom.org

Verantwortliches Bitkom-Gremium

AK Öffentliche Sicherheit