POSITIONSPAPIER

Digitale Souveränität



Bild: Larson Studio – stock.adobe.com

Gewerkschaft der Polizei

Souveränität
im digitalen Raum

In Zeiten rasanten technologischen Fortschritts und zunehmender globaler Vernetzung gewinnt das Thema „digitale Souveränität“ immer mehr an Bedeutung. Die Fähigkeit, die eigenen digitalen Ressourcen, Infrastrukturen und Daten selbstbestimmt zu kontrollieren und zu schützen, ist entscheidend für die Unabhängigkeit und Sicherheit von Staaten, Wirtschaft und Gesellschaft. Diese Bedeutungszunahme ist nicht nur auf die allgemeine Digitalisierung, sondern auch auf spezifische geopolitische Entwicklungen zurückzuführen. Insbesondere die Erosion von Vertrauen und Verlässlichkeit im transatlantischen Verhältnis, die derzeitigen Kriege und diverse Formen digitaler Angriffe auf IT-Infrastrukturen haben dazu geführt, dass digitale Souveränität rasant an Bedeutung gewinnt. In einer Welt, in der Wirtschaftsspionage, Cyberangriffe, Datenlecks und andere digitale Bedrohungen zunehmend zu den größten Sicherheitsrisiken gehören, ist der unbedingte Wille, digitale Souveränität zu wahren bzw. anzustreben, zu einem entscheidenden Faktor für die nationale, aber auch die internationale Sicherheit geworden.

Der Begriff der digitalen Souveränität ist vielfach von unterschiedlichen Interessengruppen in Gebrauch, wobei eine tiefere Auseinandersetzung mit dem jeweiligen Begriffsverständnis und seinen Implikationen oft ausbleibt. So verstehen beispielsweise Zivilgesellschaft und Bürgerrechtsorganisationen darunter primär die informationelle Selbstbestimmung des Individuums. Für sie bedeutet Souveränität, dass Bürger:innen die volle Kontrolle über ihre eigenen Daten behalten und vor staatlicher Überwachung sowie kommerzieller Ausbeutung geschützt werden. Dagegen sieht die US-amerikanische IT-Branche in dem Begriff meist eher ein technisches Feature oder ein Compliance-Instrument. Für die großen Cloud-Anbieter (Hyperscaler) bedeutet digitale Souveränität vor allem die Bereitstellung spezieller Infrastrukturen, die zwar lokale (deutsche) Sicherheitsvorgaben erfüllen, während jedoch gleichzeitig die technologische Basis weiterhin in den USA verbleibt, mit sämtlichen Risiken durch den CLOUD Act (Zugriff auf Daten im Ausland) und den FISA Act (Überwachung durch Geheimdienste).

Um hier einen klaren Standpunkt zu beziehen, sieht die Gewerkschaft der Polizei die Notwendigkeit, sich einzubringen und zu definieren, was aus polizeifachlicher Sicht unter digitaler Souveränität zu verstehen ist, was diese für polizeiliche Daten, Anwendungen und IT-Infrastrukturen bedeutet und was zu tun ist, um dieser schrittweise näher zu kommen.

Herausgeber:
Gewerkschaft der Polizei
Bundesvorstand
Stromstr. 4, 10555 Berlin
www.gdp.de

Gestaltung und Druck:
Wölfer Druck+Media
42781 Haan



Bild: mat – stock.adobe.com

Kontrolle über Daten und Systeme

Für die Polizei bedeutet digitale Souveränität die uneingeschränkte technologische und rechtliche Selbstbestimmung über ihr digitales Handeln im Rahmen des Rechtsstaats. Sie umfasst die volle Kontrolle über die Datenhaltung, die Gestaltung polizeilicher Anwendungen sowie den sicheren Betrieb der zugrunde liegenden IT-Infrastruktur. In diesem Zusammenhang dürfen Bürger:innen und Wirtschaftsunternehmen zu Recht erwarten, dass ihre Daten bei der Polizei absolut sicher und vor jedem unbefugten Zugriff durch Dritte oder fremde Staaten geschützt sind. Ziel ist es, jede Form von Einflussnahme oder Datenabfluss – insbesondere durch außereuropäische Akteure – dauerhaft auszuschließen.

Der Schutz vor Einflussnahme muss sich auch auf die gezielte Initialisierung oder Verstärkung von Vorurteilen („Bias“) innerhalb von KI-Modellen erstrecken. Nur durch echte digitale Autonomie kann die Polizei ihre Integrität und den Schutz privater sowie geschäftlicher Daten gemäß europäischen Standards garantieren.

Letztlich bildet diese Souveränität das Fundament für das Vertrauen der Gesellschaft in eine moderne, handlungsfähige und grundrechtskonforme Polizeiarbeit.

Aus Sicht der GdP reicht eine allgemeine Beschreibung und Definition des Begriffes der digitalen Souveränität nicht aus. Vielmehr ist es geboten, diesen mit konkreten und umsetzbaren Forderungen und Maßnahmen auszufüllen.

Unsere Forderungen auf einen Blick

1. Rechtssicherheit
2. Strategie zur Reduzierung technologischer Abhängigkeiten
3. Der Faktor Mensch – Qualifizierungsoffensive für digitale Souveränität
4. Neue Sicherheitskriterien in Ausschreibungs- und Vergabeverfahren
5. Kritische Bewertung der Wirksamkeit von „No-Spy-Klauseln“
6. Gewährleistung einer souveränen Datenhaltung
7. Rechtskonforme Systemgestaltung
8. BSI-konforme Infrastrukturgestaltung
9. Eigentums- und Nutzungshoheit
10. Vollständiger Verbleib sensibler Speichermedien
11. Exklusiver physischer Zutritt
12. Finanzierung

1. Rechtssicherheit

Sämtliche polizeiliche Daten sowie die zugrunde liegende IT-Infrastruktur unterliegen ausnahmslos deutschen und europäischen Rechtsnormen. Ein Zugriff durch Dritte – insbesondere durch Behörden oder Regierungen fremder Staaten auf Basis extraterritorialer Gesetze (wie beispielsweise dem US-CLOUD-Act) muss durch rechtliche, organisatorische und technische Maßnahmen kategorisch ausgeschlossen werden.

2. Strategie zur Reduzierung technologischer Abhängigkeiten

Erarbeitung und Umsetzung verbindlicher Konzepte innerhalb der Polizeibehörden zur schrittweisen Loslösung von (insbesondere proprietären) außereuropäischen Soft- und Hardware- sowie Cloud-Lösungen. Ziel ist der Aufbau einer digitalen Souveränität durch Steigerung der behördlichen technischen Fähigkeiten sowie Diversifizierung, die den Einsatz von Open-Source-Technologien und nationalen sowie europäischen Alternativen forciert.

3. Der Faktor Mensch – Qualifizierungsoffensive für digitale Souveränität

Digitale Souveränität verlangt polizeiliche Kernkompetenz im Umgang mit modernsten Technologien. Die aktuellen Initiativen zur Einrichtung von „KI-Büros“ in den Polizeiverbänden zeigen deutlich, dass zukunftsfähige Systeme auch fundiertes internes Wissen erfordern. Um die kritische Abhängigkeit von externen IT-Dienstleistern nachhaltig zu reduzieren, muss jetzt eine umfassende Qualifizierungsoffensive eingeleitet werden. Der Fokus liegt dabei auf dem gezielten, tiefgreifenden Aufbau von behördeneigenem Know-how in den Schlüsselbereichen Data Science und Softwareengineering. Nur durch diese gezielte Aus- und Fortbildung wird die Polizei befähigt, souveräne Systeme eigenständig, kompetent und rechtssicher zu bedienen.



Bild: KI-generiert



Bild: KI-generiert

4. Neue Sicherheitskriterien in Ausschreibungs- und Vergabeverfahren

Wir fordern den konsequenten Ausschluss von IT-Dienstleistern aus allen öffentlichen Ausschreibungs- und Vergabeverfahren, bei denen eine Einflussnahme durch ausländische Nachrichtendienste oder antidemokratische Überzeugungen des Führungspersonals erkennbar sind oder nicht zweifelsfrei ausgeschlossen werden können. Wenn Unternehmen ihre technologische Basis in enger Abstimmung mit Geheimdiensten entwickelt haben, ist eine Trennung zwischen ziviler Nutzung und nachrichtendienstlicher Verwertung faktisch nicht mehr überprüfbar. Bei einer nachgewiesenen Historie enger Kooperation mit ausländischen Diensten muss zwingend davon ausgegangen werden, dass im Konfliktfall fremde Staatsinteressen über die vertragliche Vertraulichkeit gegenüber deutschen und europäischen Kunden gestellt werden. Ein solches Risiko der „doppelten Loyalität“ (Double Allegiance) ist mit dem Schutzbedarf staatlicher Infrastruktur, der freiheitlich demokratischen Grundordnung und der digitalen Souveränität unvereinbar. Wer die Integrität unserer Verwaltung sichern will, darf keine Dienstleister beauftragen, die strukturell in fremde Sicherheitsapparate eingebunden sind.

5. Kritische Bewertung der Wirksamkeit von „No-Spy-Klauseln“

Es ist zu berücksichtigen, dass vertragliche Zusicherungen durch außereuropäische Gesetze faktisch ausgehebelt werden können, da diese Anbieter zur Datenherausgabe an Behörden des jeweiligen Staates verpflichtet sein können. Auch deutsche oder europäische Tochterunternehmen müssten sich diesen gesetzlichen Vorgaben beugen und Daten herausgeben, ohne den Kunden darüber informieren zu dürfen.

6. Gewährleistung einer souveränen Datenhaltung

Das physische Hosting sämtlicher polizeilicher Daten und Anwendungen hat vorrangig im Inland oder bei nachweislich vertrauenswürdigen Partnern innerhalb der EU zu erfolgen. Durch den Betrieb in zertifizierten, staatlich kontrollierten Rechenzentren wird sichergestellt, dass die Datenhoheit ausschließlich der deutschen bzw. europäischen Gerichtsbarkeit unterliegt und physische wie digitale Zugriffsbefugnisse dritter Staaten ausgeschlossen sind. Es erfolgt kein internationales Routing des Datenverkehrs. Entsprechende resiliente Redundanzen sind vorzusehen.



7. Rechtskonforme Systemgestaltung

Bei der Entwicklung und dem Betrieb polizeilicher IT-Systeme ist die Einhaltung des BDSG und der DSGVO durch technische und organisatorische Maßnahmen sicherzustellen. Hierbei müssen insbesondere die Prinzipien der Datensparsamkeit sowie des Schutzes besonders sensibler Datenkategorien bereits im Systemdesign verankert sein, um unbefugte Profilbildungen oder Zweckentfremdungen auszuschließen. Ebenso haben sich IT-Dienstleister zur Einhaltung von BDSG und DSGVO zu verpflichten.

8. BSI-konforme Infrastrukturgestaltung

Sämtliche IT-Komponenten und Fachanwendungen müssen den Sicherheitsanforderungen des jeweils gültigen BSI-Grundschutzes entsprechen. Durch die Implementierung und regelmäßige Fortschreibung eines aktuellen Sicherheitskonzepts wird gewährleistet, dass die polizeiliche IT-Infrastruktur nach den BSI-Standards betrieben wird und somit der Ausfallsicherheit und Datensouveränität Rechnung getragen wird.

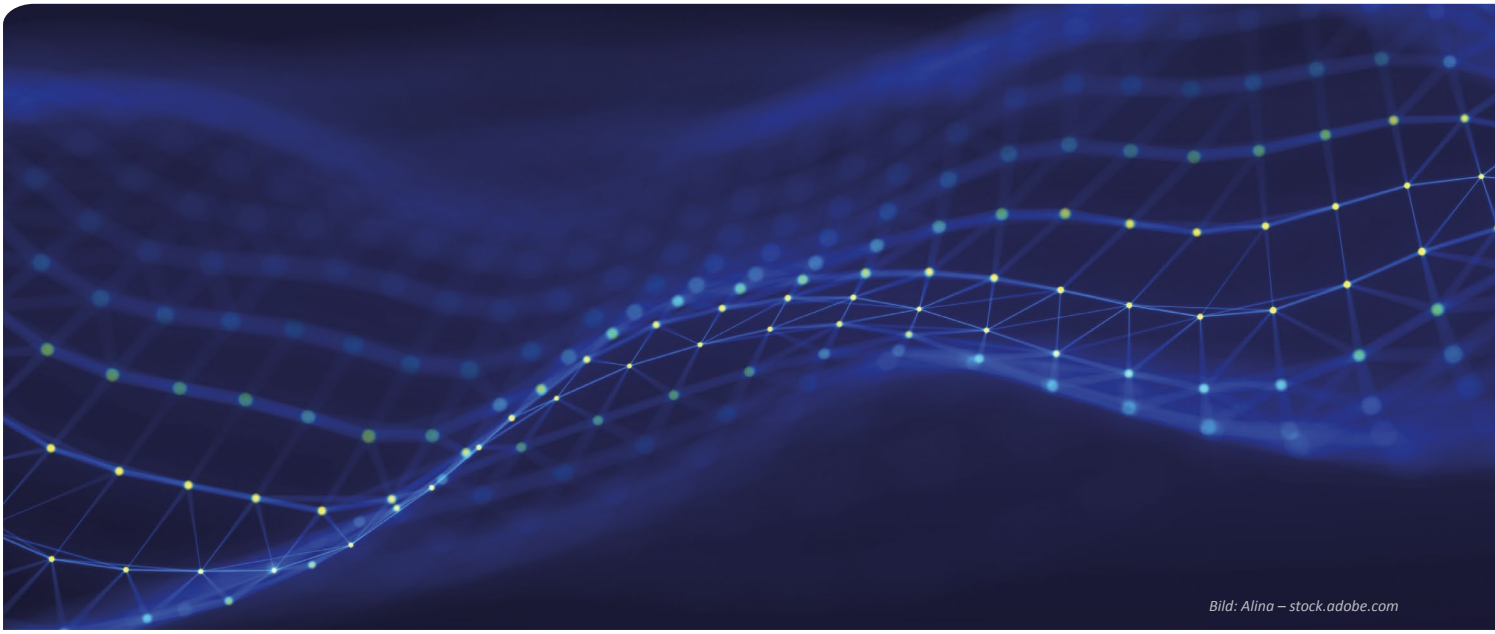


Bild: Alina – stock.adobe.com

9. Eigentums- und Nutzungshoheit

Die gesamte Hardware sowie die Netzwerk- und Firewall-Infrastruktur für kritische polizeiliche Anwendungen und polizeiliche Daten befinden sich im unmittelbaren Eigentum der zuständigen Polizeibehörde. Hierdurch wird eine exklusive Nutzung sichergestellt, die jegliche Mitbenutzung durch unbefugte Dritte ausschließt und die physische wie logische Kontrolle über die sensiblen IT-Ressourcen jederzeit in staatlicher Hand belässt.

10. Vollständiger Verbleib sensibler Speichermedien

Um den unbefugten Abfluss polizeilicher Daten bei Hardwaredefekten oder -austauschen auszuschließen, verbleiben sämtliche defekten oder ausgetauschten Speichermedien im Rahmen von Defective Media Retention (DMR-Vereinbarungen) dauerhaft im Besitz und Eigentum der zuständigen Polizeibehörde. Eine Rücksendung an den Hersteller oder Dienstleister ist kategorisch ausgeschlossen, wodurch die physische Datenhoheit und die anschließende zertifizierte Vernichtung durch die Polizei sichergestellt werden.



Bild: KI-generiert

11. Exklusiver physischer Zutritt

Die alleinige Entscheidungsgewalt über den physischen Zugang zu Standorten der IT-Infrastruktur liegt bei der zuständigen Polizeibehörde. Der Zutritt ist auf einen eng definierten Personenkreis zu begrenzen, wobei eine erfolgreich abgeschlossene Sicherheitsüberprüfung (SÜ) zwingende Voraussetzung für jede Form des physischen Zugangs ist.

12. Finanzierung

Die Digitalisierungsziele sind nur mit einer zukunftsorientierten Finanzierungsstrategie umsetzbar. Innerhalb der EU sollten solidarische Modelle für eine stufenweise Weiterentwicklung der digitalen Fähigkeiten der Sicherheitsbehörden entwickelt werden.



Notizen

Gewerkschaft
der Polizei