Analyse des Systems «Octagon»

Kurzfazit
Octagon ist ein strukturierter Versuch, Gewaltrisiken zu erfassen – aber die Ankreuz-Logik ohne Begründungsfelder, dehnbar formulierte Merkmale, unklare Basisraten sowie fehlende Beleg- und Audit-Pflichten machen das System anfällig für Bias, Übergriffigkeit und Rechtsverletzungen. Ohne harte Verfahrenssicherungen kollidiert es schnell mit EMRK Art. 8 (Privatsphäre) und dem Schweizer Datenschutzgesetz (revDSG).

1) Problemzonen beim Ausfüllen durch Polizei, Justiz und Nachrichtendienst
Das Formular erlaubt Bewertungen ohne Begründung, Quelle oder Kontext. Viele Merkmale sind unpräzise (z.B. «Schwarz-Weiss-Denken», «feindselig gegenüber Gruppen») und eröffnen subjektiven Interpretationsspielraum. Besonders schutzwürdige Kategorien (Gesundheits- oder politische Daten) werden erfasst, ohne klare rechtliche oder fachliche Schranken. Es fehlt eine verbindliche Definition, wie «aktuell» oder «historisch» ein Verhalten zu werten ist, und es gibt keine standardisierten Basisraten. Ohne Audit- oder Teamverfahren entstehen intransparente Einzelurteile.

2) Risiko von Bauchentscheiden («Handgelenk × Pi»)
Die Kreuzchen-Methode begünstigt Confirmation Bias, Labeling und Scheingenauigkeit. Ohne Pflicht zur Begründung oder Quellenangabe können falsche oder voreingenommene Einschätzungen jahrelang im System bestehen bleiben. Besonders heikel ist die Erfassung von politisch oder gesundheitlich sensiblen Merkmalen ohne gerichtliche oder ärztliche Verifikation. Damit droht eine Verletzung der Unschuldsvermutung und des Verhältnismässigkeitsprinzips.

3) Zentrale Fragen an Aufsicht und Exekutive
1. Welche gesetzliche Grundlage erlaubt die Bearbeitung solcher Daten? 2. Welche Datenarten gelten als besonders schützenswert, und wie wird deren Bearbeitung begründet? 3. Wie wird die Datenqualität überprüft (Begründungspflicht, Peer-Review, Schulung)? 4. Welche Aufbewahrungsfristen und Löschverfahren gelten? 5. Wer hat Zugriff, und werden Zugriffe protokolliert? 6. Wie kann eine betroffene Person Auskunft und Löschung verlangen? 7. Welche unabhängigen Kontrollen (Datenschutz, Parlament) finden statt? 8. Wie werden Missbrauch und politische Profilierung verhindert? 9. Gibt es Daten zur Wirksamkeit und Treffergenauigkeit des Systems?

4) Grundrechts- und Datenschutz-Einordnung
Die Verarbeitung fällt klar unter Art. 8 EMRK (Privatsphäre). Eingriffe sind nur rechtmässig, wenn sie gesetzlich geregelt, notwendig und verhältnismässig sind. Das revidierte Datenschutzgesetz verlangt Transparenz, Zweckbindung, Datenminimierung und Korrektheit. Besonders schützenswerte Daten (Gesundheit, Politik, Religion) dürfen nur mit klarer Rechtsgrundlage und strengen Schutzmassnahmen bearbeitet werden.

5) Bewertung der Rubriken auf Sachdienlichkeit
Viele Rubriken sind nur dann aussagekräftig, wenn sie durch Fachleute mit klaren Definitionen und Belegen ausgefüllt werden. Die Erfassung von Persönlichkeitsmerkmalen oder psychischen Belastungen ohne Fachgutachten ist wertlos bis gefährlich. Dagegen sind objektiv überprüfbare Kriterien (z.B. dokumentierte Gewalthandlungen, Zugang zu Waffen, akute Bedrohungen) sachdienlich.

6) Erforderliche Mindest-Safeguards
• Pflicht-Freitext pro Flag mit Quelle, Datum und Kontext • Vier-Augen-Prinzip und dokumentierte Reviews • Strengere Freigaben für Gesundheits- und Politdaten • Automatische Löschfristen und Protokolleinsicht • Betroffenenrechte (Auskunft, Berichtigung, Löschung) • Externe Datenschutz- und Parlamentsaufsicht • Validierung des Systems anhand realer Fälle