Deutsche Universität für Verwaltungswissenschaften Speyer
Postfach 14 09 – D-67324 Speyer
Hessischer Landtag
Der Vorsitzende des Innenausschusses
Schlossplatz 1-3
65183 Wiesbaden

Universitätsprofessor
Dr. David Roth-Isigkeit

Lehrstuhl für Öffentliches Recht, insbesondere Recht der Digitalisierung

Freiherr-vom-Stein-Str. 2
67346 Speyer
Telefon: ++49(0)6232-654-149
E-Mail: ls-oer@uni-speyer.de

02. Mai 2023

Stellungnahme im Rahmen der öffentlichen mündlichen Anhörung
am 15. Mai 2023 des
Innenausschusses des Hessischen Landtags
zum Gesetzentwurf

Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG)

I. Allgemeines

Die Digitalisierung des täglichen Lebens und insbesondere der Arbeitsweise in der öffentlichen Verwaltung rückt die Sicherheit im digitalen Raum aus einer bereichsspezifischen Nische in einen zentralen Fokus der Sicherheitspolitik. Diese Statusveränderung fordert insbesondere die Länder rechtlich und politisch heraus.

Die Sicherheit informationstechnischer Systeme stellt besondere Anforderungen, die sich von klassischer Sicherheitspolitik stark unterscheiden. Cyberangriffe werden punktuell und meist weit entfernt von ihrem eigentlichen Wirkungsort ausgeführt, sind dann allerdings systemseitig kaum zu vermeiden und nur unter größten Schwierigkeiten zu konkreten Verursachern zurückzuverfolgen. Ähnlich wie die Bekämpfung organisierter Kriminalität ist die Cybersicherheit ein Feld, auf dem es sowohl auf Spitzentechnologie als auch auf speziell ausgebildetes Personal ankommt.

Das Land Hessen reagiert dementsprechend auf die wachsenden Gefahren durch die zunehmende Vernetzung und versucht der Bedrohung durch die Einrichtung eigener Verwaltungsstellen sowie gefahrenabwehrrechtlicher Eingriffsgrundlagen entgegenzuwirken. Dies ist ein grundsätzlich begrüßenswertes Anliegen. Kompetenzen im Bereich der Cybersicherheit werden auf allen Ebenen benötigt.

Die immer größer werdende Bedeutung der Cybersicherheit setzt die klassische, dezentrale Sicherheitsarchitektur im Bund und in den Ländern unter Druck. Eine wachsende Anzahl von Bundesländern hat Cybersicherheitsgesetze erlassen und entsprechende Verwaltungsstellen eingerichtet. Gleichzeitig ist die Cybersicherheitspolitik ein eher atypisches Feld der Sicherheitspolitik, weshalb die nun geschaffenen und noch zu schaffenden Sicherheitsgesetze der Länder perspektivisch noch einer Harmonisierung und Überarbeitung bedürfen.

Das Land Hessen folgt damit einer allgemeinen Entwicklung unter den Ländern, wenngleich die notwendige Bündelung von Kompetenzen und die Verfügbarkeit von Spitzentechnologie strukturell eher für die Einrichtung zentraler Behörden auf Bundesebene spricht. Diese spiegelt sich konsequenterweise in einer Verschiebung von Cybersicherheitskompetenzen auf der Ebene der Europäischen Union und der intensiven Zusammenarbeit mit globalen starken Partnern wie etwa den Vereinigten Staaten und dem Vereinigten Königreich.

Welche Lücke in der Cybersicherheitsarchitektur ist angesichts der Aktivitäten auf Bundes- und EU-Ebene nun den Ländern zur eigenen Verantwortung gelassen? Richtig begründet der Entwurf, dass die spezielle Konstellation des Schutzes der *Systeme der Landesverwaltung* es erfordert, auch in den Ländern Behörden zum Schutz der IT-Infrastruktur einzurichten. Geschützt ist damit nicht die Cybersicherheit „allgemein“, wenngleich die geplante Stelle auch private Unternehmen unterstützen dürfen soll, sondern die Sicherheit in der hessischen Landesverwaltung.

Da sich die Cyberbedrohungslage in der Hessischen Landesverwaltung nicht von der Lage im Bund oder in der Privatwirtschaft unterscheidet, wird es eine zentrale Herausforderung darstellen, in der geplanten Organisation eine ähnliche Kompetenzdichte wie auf Bundesebene zu erreichen. Die Aufgabe ist es dann, die Zusammenarbeit mit den zentralen Stellen, insbesondere dem Bundesamt für Sicherheit in der Informationstechnik (BSI), richtig herzustellen.

In der folgenden Stellungnahme gehe ich nur kurz auf mE wesentliche Aspekte ein.

Zur Behördenstruktur (unten II.)

Die Schaffung ressortübergreifender und auf die Binnenstruktur der Verwaltung bezogener Kompetenzen im Innenministerium ist ein atypischer Sonderfall, der der Rechtfertigung bedarf. Diese Rechtfertigung ist mE noch nicht gut genug herausgearbeitet.

Zur „automatisierten Verarbeitung“ der anfallenden personenbezogenen Daten (unten III.)

Der Entwurf spricht nur abstrakt von der automatisierten Verarbeitung personenbezogener Daten, stellt aber nicht hinreichend klar, welchen Grad der Automatisierung diese Bestimmung meint. An welcher Stelle das Eingreifen eines Menschen erfolgt, bzw. wie es ausgelöst wird, bleibt unklar.

II. Zur Behördenstruktur

Der Gesetzentwurf sieht eine Verwaltungsstelle mit ressortübergreifenden Eingriffskompetenzen vor, die gleichzeitig im Geschäftsbereich des Innenministeriums angesiedelt ist. Dadurch werden zwei verschiedene Formen des Behördenaufbaus miteinander verschliffen. Eine solche (atypische) Kombination ist zwar grundsätzlich möglich, verlangt aber nach rechtfertigenden Gründen. Diese spezifischen Gründe, warum die Stelle beim Innenministerium angesiedelt sein soll, und nicht wie bei

ressortübergreifenden Kompetenzen üblich, jenseits einer konkreten Ministerialstruktur, sind mE noch nicht ersichtlich.

Dem Zentrum für Informationssicherheit (ZfIS), inkl. der darin folgende Einbindung der Computer Emergency Response Teams (CERT), sowie des Zentralbeauftragten für Informationssicherheit (CISO) sollen weitreichende Kompetenzen zugewiesen werden. Der Gesetzentwurf sieht ressortübergreifende Kompetenzen vor, die sich insbesondere aus § 5 Abs. 2 Nr. 2 des Gesetzentwurfes ergeben. Das geplante ZfIS soll für die gesamte Landesverwaltung „ohne Amtshilfeersuchen“ eine entsprechende Sicherheitsstruktur bereitstellen.

Insbesondere gilt dies nicht nur in Bezug auf die eigentlich unproblematische Leistung von Assistenz bei der Gewährleistung von Informationssicherheit vertraulicher Daten. Das ZfIS darf nach dem vorliegenden Entwurf eben auch von sich aus Überprüfungen der Gewährleistung der Informationssicherheit initiieren. Besonders hervorzuheben sind die Eingriffsgrundlagen nach § 4 Abs. 2 und 3 des Gesetzentwurfes.

Eine ressortübergreifende Tätigkeit verlangt in der Regel nach einem Legitimationsweg, der nicht nur über ein einzelnes Ressort führt. Für übergreifende Fragen ist in der Regel die Landesregierung zuständig, arg. ex. Art. 104 Abs. 3 der Hessischen Verfassung. § 4 Abs. 1 des Gesetzesentwurfes sieht hier aber nur die für IT- und Cybersicherheit in der Landesverwaltung zuständige Ministerin oder den hierfür zuständigen Ministers vor. Damit werden die für eine ressortübergreifende Tätigkeit notwendigen breiten Legitimations- und Kontrollstränge auf das Innenressort beschränkt.

Das Ressortprinzip gewährleistet in der Regel, dass Ministerinnen und Minister den ihnen zufallenden Geschäftsbereich in eigener Verantwortung leiten. Dazu gehört auch die Kommunikationsinfrastruktur der Ministerien. Im vorliegenden Entwurf wird dieses Ressortprinzip im Hinblick auf einen wesentlichen Teilbereich der Informationssicherheit durchbrochen und schlägt diese Kompetenzen in ihrer gesamten Breite dem Innenressort zu.

Das ist nicht unproblematisch, da über das Ressortprinzip die Gewährleistung demokratischer Legitimation und Kontrolle erfolgt. Die Hausleitung und die Sicherstellung der wesentlichen Arbeitsgrundlagen gehören strukturell jeweils umfassend in den Kompetenzbereich eines Ministers/einer Ministerin, die hierfür auch die politische Verantwortung tragen. Im vorliegenden Entwurf wird diese politische Verantwortlichkeit zum Innenministerium verschoben. Nach der hier gewählten Gestaltung müsste der Innenminister bzw. die Innenministerin die politische Verantwortung für Mängel in der Cybersicherheitsarchitektur tragen. Das kann aber gerade deshalb nicht sein, da diese nach der Grundkonstruktion der Hessischen Verfassung in den Geschäftsbereich der einzelnen Ministerien fallen und die Kompetenzen des ZfIS nur punktuell wirken.

Auch wenn der Gesetzentwurf in seiner Begründung formuliert: „Die Einrichtung einer Zentralstelle für Informationssicherheit entbindet die einzelnen Stellen der öffentlichen Verwaltung nicht von ihrer Pflicht, selbständig für eine angemessene Sicherheit bei dem Betrieb ihrer informationstechnischen Systeme zu sorgen“ scheint dies in der Praxis unrealistisch. Tatsächlich, dafür sprechen auch die umfassenden Eingriffsgrundlagen, wird diese Aufgabe der Zentralstelle überantwortet. Die in § 12 Abs. 1 und Abs. 2 des Gesetzentwurfes vorgenommene Begrenzung im Hinblick auf Fälle, in denen das Landesdatennetz betroffen ist, überzeugt nicht. Denn in der Praxis werden die Stellen (wie auch die Gesetzesbegründung zu Abs. 2 feststellt) wohl auf das Datennetz zur Erfüllung ihrer Aufgaben zurückgreifen.

Querschnittsaufgaben, d.h. solche Aufgaben die ressortübergreifend erledigt werden müssen, vertragen sich schlecht mit dem klassischen Muster des Behördenaufbaus in Deutschland.

Cybersicherheitspolitik und insbesondere die Abwehr von Gefahren für die Informationssysteme in der Landesverwaltung ist eine solche Querschnittsaufgabe. Die Komplexität der in der modernen Gesellschaft anfallenden Aufgaben tendiert dazu, die klassischen Aufbaumuster des Behördenaufbaus in Frage zu stellen. Dies ist im Hinblick auf die wichtige Funktion von Legitimation und Kontrolle, die dieser Aufbau im verfassungsrechtlichen Schema übernimmt, nicht unproblematisch. Gleiches gilt für die Systeme der Kommunen und die Garantie der kommunalen Selbstverwaltung.

Insbesondere im Hinblick auf die ressortübergreifende Tätigkeit wäre ein Modell wie in Baden-Württemberg mit der Einrichtung einer (rechtlich ungenau bezeichneten) „Cybersicherheitsagentur“ als Landesoberbehörde zu präferieren gewesen. Denn selbst, wenn dem Innenministerium die Fachaufsicht über eine unabhängige Behörde zugewiesen wird, ist dies der Struktur der ressortübergreifenden Tätigkeit näher als eine unmittelbare Integration in die Verwaltungsstruktur eines anderen Ressorts. Gerade im digitalen Bereich haben sich solche „Beauftragten“, die jenseits der Ministerialstruktur stehen, bewährt.

Abgemildert werden könnte das Problem der ressortübergreifenden Kompetenzen durch klare Vorgaben für parlamentarische Berichtspflichten und parlamentarische Kontrollen. Diese könnten, insbesondere wenn Einzelfälle betroffen sind, dem § 5 Abs. 10 BSIG oder, wenn es um allgemeine Berichtspflichten der parlamentarischen Kontrolle geht, aus § 13 BSIG entnommen werden. Eine klarere Strukturierung im Hinblick auf die durchaus beträchtlichen Eingriffskompetenzen der Behörde im Hinblick auf Legitimation und parlamentarische Kontrolle wäre wünschenswert und durch verhältnismäßig einfache Anpassungen möglich.

III. Zur „automatisierten Verarbeitung“ der anfallenden personenbezogenen Daten

Soweit das Gesetz ein abgestuftes Verfahren vorsieht, das im ersten Schritt eine automatisierte, rein technische Auswertung der anfallenden Daten vorsieht, im zweiten Schritt eine manuelle Bearbeitung erlaubt, so ist der Begriff einer automatisierten Verarbeitung genauer zu definieren.

Automatisierung kennt, wie aus der rechtlichen Diskussion insbesondere im Verwaltungsverfahrensrecht klar geworden sein sollte, verschiedene Stufen. Die vollständig automatisierte Verarbeitung sieht keinerlei Eingreifen eines/-r menschlichen Bearbeiter/-in mehr vor. Bei einer teilweise oder teilautomatisierten Bearbeitung sind an den einzelnen Schritten, insbesondere der Definition von Kriterien, noch Menschen beteiligt. Diese Unterscheidung ist jedoch nicht binär, sondern kennt viele Zwischenschritte, die etwa daran anknüpfen, an welcher Stelle im Arbeitsprozess durch einen Menschen Kriterien definiert werden können.

Im Gesetzentwurf ist der Grad der Automatisierung und insbesondere die Tiefe der Automatisierung noch unbestimmt. Das könnte letzten Endes auch verfassungsrechtlich bedenklich sein. Denn in Fragen der Automatisierung ließe sich etwa schärfen, an welchem Punkt, insbesondere an welchem Zeitpunkt, die automatisierte Verarbeitung beginnt und nach welchen Kriterien sie sich richtet. Können Kriterien für die automatisierte Verarbeitung schon mit Blick auf ein bestimmtes Verdachtsmoment erstellt werden, das dann wiederum erlauben würde, auf konkrete Fälle rückzuschließen. Eine mögliche Schärfung dieses Passus ließe sich etwa aus § 8a Absatz 1 BSI-G entnehmen, der die automatisierte Verarbeitung zumindest etwas bestimmter beschreibt.