

Mitteilung des Senats vom 5. April 2016**Datenschutz bei polizeilicher Telekommunikationsüberwachung**

Die Fraktion der FDP hat unter Drucksache 19/334 eine Große Anfrage zu obigem Thema an den Senat gerichtet.

Der Senat beantwortet die vorgenannte Große Anfrage wie folgt:

1. Wie haben sich die Fallzahlen der Telekommunikationsüberwachung beim Landeskriminalamt (LKA) in den Jahren ab 2010, aufgeschlüsselt nach Jahren und Rechtsgrundlage, entwickelt?

Die Anzahl der Telekommunikationsüberwachungsmaßnahmen nach § 100a Strafprozessordnung (StPO) für die Jahre 2010 bis 2014 ergeben sich aus der nachfolgenden Tabelle. Die Zahlen für 2015 liegen noch nicht vor.

| Jahr | Anzahl der Verfahren | Erst-anordnungen | Verlängerungs-anordnungen |
|------|----------------------|------------------|---------------------------|
| 2010 | 36 | 281 | 43 |
| 2011 | 53 | 352 | 43 |
| 2012 | 23 | 310 | 86 |
| 2013 | 33 | 263 | 48 |
| 2014 | 27 | 250 | 60 |

2. Welche Informationen über Mängel in der Praxis der polizeilichen Telekommunikationsüberwachung (TKÜ) in Niedersachsen sind dem Senat bekannt, und wie bewertet er diese?

Von den Datenschutzbeauftragten des Landes Bremen und des Landes Niedersachsen sind folgende Problemfelder und Mängelpunkte gebündelt benannt worden:

- a) Aussagen zur Risikoanalyse, auch nach Berücksichtigung des Überarbeitungsstands vom 18. Oktober 2012 seien noch unvollständig und in der Folge nicht bestimmbar, ob alle erforderlichen Maßnahmen nach § 7 Abs. 2 Niedersächsisches Datenschutzgesetz (NDSG) (insbesondere Umsetzung/Überwachung zur Fernwartung, Datenexport, Netz/Firewall, Verknüpfung mit anderen Systemen wie Safir u. a.) getroffen worden sind;
- b) des Weiteren sei die erforderliche Mandantenfähigkeit des Verfahrens im datenschutzrechtlichen Sinne nicht erwiesen. Die Beschreibung hierzu lasse erkennen, dass es einer strukturellen Nachbesserung bedürfe;
- c) das Rechte-Rollen-Konzept sei zu vervollständigen;
- d) die Protokollierung sei um die fehlenden Komponenten zu vervollständigen;
- e) die Dokumentenlage sei in Teilen lückenhaft, sodass weder der gesicherte rechtssichere Betrieb noch eine Revisionssicherheit gewährleistet werden könne;

- f) aufgrund des festgestellten sehr hohen Schutzbedarfs sei die Verschlüsselung der Inhalts- und Verkehrsdaten vorzunehmen;
- g) die Fernwartung sei nur mit besonderen, der Schutzstufe „sehr hoch“ angemessenen Sicherheitsmaßnahmen, zulässig.

Diese Beanstandungen sind von den Datenschutzbeauftragten 2013 geäußert worden. Viele Beanstandungen betreffen die nach Auffassung der Datenschutzbeauftragten nicht ausreichende Dokumentation des Verfahrens. Seit 2013 hat das Land Niedersachsen durch seine Behörden an vielen Stellen Nachbesserungen des Verfahrens, insbesondere auch in der Dokumentation, vorgenommen. Nach Auffassung des Senats kann nicht davon ausgegangen werden, dass das System als unter Datenschutzgesichtspunkten insgesamt bedenklich eingestuft werden kann.

3. Welche Kenntnisse hat der Senat über die Behebung dieser Mängel durch das Land Niedersachsen?

Das Niedersächsische Ministerium für Inneres und Sport hat im Namen der Landesregierung auf eine Anfrage der Fraktion der FDP im niedersächsischen Landtag, was das LKA bzw. das Innenministerium seit Oktober 2012 unternommen habe, um die datenschutzrechtlichen Mängel abzustellen, den folgenden Sachstand mitgeteilt (Drs. 17/4865 vom 17. Dezember 2015, Seite 85 ff.):

„In Bezug auf die in der Antwort zur Frage 2 gebündelten Problemfelder ergeben sich aktuell folgende Sachstände:

Zu 2 a) Insbesondere sind die Aussagen zur Risikoanalyse, auch nach Berücksichtigung des Überarbeitungsstands vom 18. Oktober 2012, noch unvollständig und in der Folge nicht bestimmbar, ob alle erforderlichen Maßnahmen gemäß § 7 Abs. 2 NDSG getroffen worden sind.

Die aktuellste Risikoanalyse mit Stand vom 18. Dezember 2012 wurde an die Landesbeauftragten für Datenschutz Niedersachsen und an die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (Datenschutzbehörden) übermittelt. Diese wird fortgeschrieben und im Zusammenwirken mit der Fertigstellung des IT-Sicherheitskonzepts finalisiert.

Ausgehend von der bereits übermittelten Risikoanalyse fehlen aktuell noch bei 31 von 274 aufgeführten Einzelpunkten die Bewertungen des zu betrachtenden Risikos. Die Abarbeitung dieser Einzelpunkte wird mit dem parallelen Aufbau des geplanten Rechen- und Dienstleistungszentrums Polizei im Verbund der norddeutschen Küstenländer ab Frühjahr 2016 berücksichtigt.

Zu 2 b) Des Weiteren ist die erforderliche Mandantenfähigkeit des Verfahrens im datenschutzrechtlichen Sinne nicht erwiesen.

Insbesondere bei der bemängelten Ausgestaltung hinsichtlich der Mandantentrennung und der externen Protokollierung sind aufgrund einer im Mai 2015 mitgeteilten Produktabkündigung durch den Dienstleister keine Änderungen mehr zu erwarten. Vor dem Hintergrund, dass die übermittelten Unterlagen durch das Landeskriminalamt an den Landesbeauftragten für Datenschutz im Rahmen der datenschutzrechtlichen Vorabkontrolle diesbezüglich nicht bemängelt wurden, ist die Systemtechnik, in Bezug auf die Mandantentrennung und die Protokollierung, vom Dienstleister vertragskonform aufgebaut und installiert worden. Es ist beabsichtigt, die im Detail verfeinerten und innerhalb der durch die Datenschutzbehörden erstellten Orientierungshilfen ‚Mandantenfähigkeit, Version 1.0, vom 11. Oktober 2012‘ und ‚Datenschutzgerechte Protokollierung, Rel. 1.0.1, vom 20. August 2010‘ zum Ausdruck gebrachten Anforderungen im Rahmen des unter Punkt 2 a) genannten Rechen- und Dienstleistungszentrums zu berücksichtigen und umzusetzen.

Zu 2 c) Das Rechte-Rollen-Konzept ist zu vervollständigen.

Das Rechte- und Rollen-Konzept wird durch das Landeskriminalamt beständig fortgeschrieben und nach Upgrade/Funktionserweiterung auf den finalen Versionsstand, im Zusammenwirken mit der Fertigstellung des IT-Sicherheitskonzepts, welches auch vollumfänglich für das oben genannte Rechen- und Dienstleistungszentrum Polizei im Verbund der norddeutschen Küstenländer zu berücksichtigen sein wird, finalisiert.

Zu 2 d) Die Protokollierung ist um die fehlenden Komponenten und Maßnahmen zu ergänzen.

Die seitens der Landesbeauftragten für den Datenschutz bemängelten Punkte konnten teilweise behoben werden. In Bezug auf den geforderten Protokollierungsumfang konnten innerhalb der Systemtechnik entsprechende Anpassungen umgesetzt werden. Bezüglich einer zusätzlichen Protokollierungseinheit außerhalb der eigentlichen Systemtechnik wird auf die Beantwortung zu 2 b) verwiesen.

Zu 2 e) Die Dokumentenlage ist in Teilen lückenhaft, sodass weder der gesicherte und rechtssichere Betrieb noch eine Revisionssicherheit gewährleistet werden kann.

Die Übermittlung des durch das Landeskriminalamt bei dem Dienstleister im Rahmen der Auftragsvergabe abverlangten IT-Sicherheitskonzepts verzögerte sich um mehrere Monate. Erst nachdem der Dienstleister den TÜV Süd mit der Erstellung des IT-Sicherheitskonzepts beauftragte, konnte dies dem Landeskriminalamt zur Verfügung gestellt werden.

In der Analyse der weit über 1 000 DIN-A4-Seiten starken Dokumentation wurden durch das Landeskriminalamt wiederkehrend Defizite festgestellt, sodass diese in großem Umfang durch den Dienstleister nachgebessert werden mussten. Bedingt durch die weiterhin vorliegenden Anpassungs- und Ergänzungserfordernisse in der Ausgestaltung der verwendeten Systemtechnik muss auch die Dokumentenlage weiterhin angepasst werden.

Erste Auszüge wurden am 21. Mai 2013 im Gesamtumfang von 556 DIN-A4-Seiten erstellt und an die Datenschutzbehörden übermittelt. Die inhaltliche Abstimmung dazu dauert an.

Zu 2 f) Aufgrund des festgestellten sehr hohen Schutzbedarfs ist die Verschlüsselung der Inhalts- und der Verkehrsdaten vorzunehmen.

Auch bei der ganzheitlichen Verschlüsselung aller im System vorhandenen Inhalts- und Verkehrsdaten sind tiefgreifende Veränderungen innerhalb der Systemtechnik erforderlich, die im Rahmen des aktuellen Projekts, unter Verweis auf die Produktabkündigung des Dienstleisters, nicht mehr zu gewährleisten sind.

Vor diesem Hintergrund wurden besondere Schutzmaßnahmen gegen einen unzulässigen räumlichen Zutritt und somit auch zur Verhinderung eines ungewollten Dateizugriffs getroffen.

Zu 2 g) Die Fernwartung ist nur mit besonderen, der Schutzstufe ‚sehr hoch‘ angemessenen Sicherheitsmaßnahmen zulässig.

Im Rahmen der am 11. Oktober 2012 durchgeführten Inaugenscheinnahme durch die Datenschutzbehörden wurde von diesen entsprechender Nachbesserungsbedarf in der Ausgestaltung des Fernwartungszugangs geäußert.

Aufgrund dessen erfolgte bereits im direkten Anschluss eine konzeptionelle Neubetrachtung der Umsetzungsmöglichkeiten für die Fernwartung.

Nach Analyse der am Markt zur Verfügung stehenden Möglichkeiten wurden zu Beginn des Jahres 2013 erste Beschaffungsmaßnahmen initiiert und eine neue und restriktivere Zugangsmöglichkeit durch den in Anspruch genommenen Dienstleister geschaffen. Nach Abschluss der Aufbau- und Testphase, der konzeptionellen Betrachtungen und abschließenden Abstimmung mit dem Dienstleister wurde die neue Fernwartungslösung am 13. Mai 2013 in Betrieb genommen. Das neue Fernwartungskonzept wurde im Mai 2013 an die Datenschutzbehörden übermittelt.“

4. Wie bewertet der Senat den im 37. Jahresbericht der Landesdatenschutzbeauftragten des Landes Bremen festgestellten fehlenden Fortschritt bei der Behebung der Mängel?

Die Landesbeauftragte hat in ihrem 37. Jahresbericht insbesondere angemahnt, dass noch keine neuen Unterlagen in diesem wie auch in anderen polizeilichen Verfahren bei ihr eingegangen seien. Wie der Senat in seiner Stellungnahme zum 37. Jahresbericht der Landesbeauftragten für den Datenschutz (Drs. 19/44

vom 11. August 2015) ausgeführt hat, lag in Bezug auf die Telekommunikationsüberwachung noch kein neuer Sachstand vor, über den die Landesbeauftragte hätte unterrichtet werden können.

5. Inwieweit betreffen die von der Datenschutzbeauftragten des Landes Niedersachsen festgestellten Mängel auch die Praxis der polizeilichen TKÜ im Land Bremen?

Das Landeskriminalamt Niedersachsen betreibt allein die technische Seite der Telekommunikationsüberwachung als Dienstleister im Auftrag des Landes Bremen. Die Verfahren selbst werden von den Polizeien in Bremen und Bremerhaven nach Maßgabe der Vorschriften der Strafprozessordnung geführt. Für die Anordnung sind allein die bremische Staatsanwaltschaft und bremische Gerichte zuständig. Die Ergebnisse der Telekommunikationsüberwachung sind nur den bremischen Polizeibehörden zugänglich.

6. Wann und in welcher Art und Weise hat sich der Senator für Inneres am Prozess der Mängelbeseitigung beteiligt?

Die Polizei Bremen wurde bereits zu Beginn der eigentlichen Projektierungsphase personell bei der Erstellung der Leistungsverzeichnisse, Vergabeunterlagen und Konzepte eingebunden. Auch nach Erteilung des Zuschlags erfolgte die weitere Einbindung der Polizei Bremen auf Basis von durchgeführten Arbeits- und Expertentreffen aus den Bereichen Polizei, IT-Sicherheit und Datenschutz.

7. Steht der Senator für Inneres im Rahmen der Mängelbeseitigung in Kontakt mit seinem niedersächsischen Amtskollegen, den Landesbeauftragten für Datenschutz der Länder Bremen und Niedersachsen, dem LKA Niedersachsen und der Polizei Bremen? Wenn ja, wann und in welcher Art und Weise haben Gespräche stattgefunden und im Einzelnen zu welchen Ergebnissen geführt?

Sowohl zwischen den Innenverwaltungen als auch zwischen den Polizeibehörden der Länder Bremen und Niedersachsen haben auf verschiedensten Ebenen Kontakte stattgefunden. Aufgrund der seit Jahren bestehenden vielfältigen Kontakte kann nicht im Einzelnen nachvollzogen werden, welche Ergebnisse sich daraus jeweils ergeben haben.

8. Wie bewertet der Senat den Umstand, dass aufgrund der bekannten Mängel TKÜ-Erkenntnisse vor Gerichten keinen Bestand haben könnten?

Die rechtlichen Voraussetzungen für die Anordnung und Durchführung von Telekommunikationsüberwachungsmaßnahmen ergeben sich aus der Strafprozessordnung. Die Anordnung von Maßnahmen unterliegt jeweils der richterlichen Kontrolle. Hier liegen grundsätzlich keine Verfahrensmängel vor. In Bezug auf die Durchführung der Telekommunikationsüberwachung, also die technische Seite der Überwachung, haben die Datenschutzbeauftragten Anforderungen an das Verfahren gestellt. Dies bedeutet aber nicht, dass das Verfahren an sich unsicher wäre, also etwa Verfahrensdaten für Dritte zugänglich wären oder Daten nicht korrekt erhoben oder zugeordnet würden. Auch die Datenschutzbeauftragten haben dies nicht behauptet. Die Forderungen der Datenschutzbeauftragten haben Aspekte der Dokumentation sowie der internen Absicherung und Administration zum Gegenstand. Für den Senat ist nicht ersichtlich, dass sich dies auf die Rechtmäßigkeit der Telekommunikationsüberwachung und der dabei erhobenen Daten auswirken könnte.

9. Sieht der Senat Bedarf, das bestehende Verwaltungsabkommen mit Niedersachsen zu aktualisieren und entsprechend der aufgetretenen Mängel anzupassen?

Der Senat sieht es als erforderlich an, das bestehende Verwaltungsabkommen mit Niedersachsen zu überarbeiten, um die Zusammenarbeit im Bereich der Telekommunikationsüberwachung an die weiter entwickelten technischen Möglichkeiten anzupassen und insgesamt eine neue Grundlage für die Kooperation zu schaffen. Darüber besteht im Übrigen Einvernehmen zwischen den Innenverwaltungen beider Länder. Dieses Erfordernis besteht unabhängig von den Feststellungen der Datenschutzbeauftragten.

10. Wie plant der Senat die Kontrolle der gemeinsamen polizeilichen TKÜ und des gemeinsamen Rechen- und Dienstleistungszentrum (RDK) vor dem Hintergrund, dass ein Teil der von der Landesdatenschutzbeauftragten Niedersachsens festgestellten Mängel Verschlusssachenanweisungen enthalten und dementsprechend der Geheimhaltung unterliegen?

Durch eine Anlage zur beabsichtigten Neufassung des Verwaltungsabkommens sollen Einzelheiten der Auftragsdatenverarbeitung, dabei auch der Kontrolle, geregelt werden. Vorgesehen werden soll u. a., dass sich der Auftragnehmer der Kontrolle durch die Landesbeauftragte für den Datenschutz der Freien Hansestadt Bremen unterwirft, soweit personenbezogene Daten aufgrund des Auftrags der Freien Hansestadt Bremen verarbeitet werden.

11. Wie sollen nach Ansicht des Senats die Landesdatenschutzbeauftragte und die Bremische Bürgerschaft ihre Kontrollfunktion in diesem Rahmen ausüben können?

In Bezug auf die Kontrolle durch die Landesbeauftragte für den Datenschutz der Freien Hansestadt Bremen wird auf die Antwort zu Frage 10 verwiesen. Die Landesbeauftragte berichtet dem Parlament regelmäßig in ihren Jahresberichten.

12. Wie stellt der Senat sicher, dass die festgestellten Mängel in der Praxis der polizeilichen TKÜ in Niedersachsen nicht auch bei der gemeinsamen TKÜ und dem Betrieb des RDK im Verbund der norddeutschen Küstenländer auftreten?

Die Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein haben sich darauf verständigt, ein gemeinsames Rechen- und Dienstleistungszentrum zur Telekommunikationsüberwachung der Polizeien im Verbund der norddeutschen Küstenländer (RDZ) einzurichten und zu betreiben. Die Landesdatenschutzbeauftragten der genannten Länder haben zu dem Entwurf des gemeinsamen Staatsvertrags Stellung genommen. Die Stellungnahme ist im Entwurf berücksichtigt worden. Das RDZ soll in einem Projekt bis zur Aufnahme des Wirkbetriebs errichtet und begleitet werden. Dabei wird auch der Aspekt „Datenschutz“ eines der Themenschwerpunkte sein.

13. Plant der Senat die Ratifizierung des Staatsvertrags zur gemeinsamen polizeilichen TKÜ und den Betrieb des RDK im Verbund der norddeutschen Küstenländer auch für den Fall, dass die beschriebenen Mängel im Rahmen der bestehenden Verwaltungskooperation mit Niedersachsen nicht vollumfänglich behoben werden?

Die Zeichnung des Staatsvertrags zum Rechen- und Dienstleistungszentrum zur Telekommunikationsüberwachung der Polizeien im Verbund der norddeutschen Küstenländer steht unmittelbar bevor. Ohne Zeichnung und Ratifizierung des Staatsvertrags durch alle beteiligten Länder kann das Projekt zur Errichtung des RDZ nicht starten. Ein Zusammenhang des Staatsvertrags mit der derzeitigen Kooperation zwischen Bremen und Niedersachsen besteht demgegenüber nicht.

14. Stimmt der Senat zu, dass Maßnahmen zu Telekommunikationsüberwachung einen weitreichenden Eingriff in die Grundrechte der Bürgerinnen und Bürger darstellen, aus dem sich eine besondere Sorgfalt in der Ausgestaltung und Durchführung dieser Maßnahmen ergibt?

Der Senat teilt die Auffassung der Fragesteller.

15. Inwiefern stimmt der Senat zu, dass vor dem Hintergrund des weitreichenden Eingriffs in die Grundrechte der Bürgerinnen und Bürger die datenschutzrechtliche Sorgfalt in der Ausgestaltung und Durchführung von TKÜ-Maßnahmen höher zu bewerten ist als ein möglicher positiver Kosteneffekt durch eine Durchführung dieser Maßnahmen in Kooperation mit anderen Ländern?

Der Senat sieht zwischen den beiden Teilaspekten keinen Widerspruch. Er geht davon aus, dass durch ein gemeinsames Rechen- und Dienstleistungszentrum beide Teilaspekte erfolgreich miteinander verbunden werden können.

16. Aus welchen Gründen stimmt der Senat der Einrichtung eines gemeinsamen RDK im Verbund mit den norddeutschen Küstenländern unter Federführung des LKA Niedersachsen angesichts der bekannten erheblichen Mängel in der Praxis der polizeilichen TKÜ in Niedersachsen zu?

Der Senat nimmt Bezug auf die Antwort zu Frage 13. Die Beschaffung und der Betrieb einer eigenen Anlage zur Telekommunikationsüberwachung wäre wegen des steigenden technischen Aufwands, der eine regelmäßige Anpassung an veränderte Technologien erfordern würde, allein aus Kostengründen nicht sinnvoll.

17. Liegen Ausweichkonzepte für den Fall vor, dass die festgestellten datenschutzrechtlichen und technisch-organisatorischen Mängel in der Praxis der polizeilichen TKÜ in Niedersachsen nicht vollumfänglich behoben werden können, und wenn ja, wie sehen diese aus?

Die bremische Anlage zur Telekommunikationsüberwachung ist veraltet und musste außer Betrieb genommen werden. Die Neubeschaffung und der Betrieb einer eigenen Anlage nur für Bremen wäre aus Kostengründen nicht verantwortbar.