LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

LEHRSTUHL FÜR DEUTSCHES, EUROPÄISCHES UND INTERNATIONALES STRAFRECHT, STRAFPROZESSRECHT, WIRTSCHAFTSSTRAFRECHT UND DAS RECHT DER DIGITALISIERUNG
(PROF. DR. MARK A. ZÖLLER)

LMU · Geschwister-Scholl-Platz 1 · 80539 München

Dr. Tanja Niedernhuber

tanja.niedernhuber@jura.uni-muenchen.de

Postanschrift
Prof.-Huber-Platz 2
80539 München

Büroanschrift
Ludwigstr. 29/IV
80539 München

Herr
Präsident des Landtags Nordrhein-Westfalen
André Kuper, MdL
Platz des Landtags 1
40221 Düsseldorf

per E-Mail: anhoerung@landtag.nrw.de

LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

STELLUNGNAHME
18/1253

A14, A09

München, 7.2.2024

Schriftliche Stellungnahme

zum Thema „Persönliche Daten von unschuldig Verfolgten müssen sicher und für die Betroffenen nachprüfbar gelöscht werden – Antrag der Fraktion der FDP, Drucksache 18/5841“

im Rahmen der Anhörung des Rechtsausschusses am 13. März 2024

Sehr geehrter Herr Präsident, sehr geehrter Herr Vorsitzender des Rechtsausschusses, sehr geehrte Damen und Herren Abgeordnete,

für die Einladung zur oben genannten Anhörung und die Gelegenheit zur Stellungnahme möchte ich mich herzlich bedanken. Zum Antrag der Fraktion der FDP, Drucksache 18/5841, nehme ich wie folgt Stellung:

Es ist sehr erfreulich, dass das Land Nordrhein-Westfalen den Datenschutz in der Arbeit der Polizeibehörden ernst nimmt und die verfassungsrechtlich erforderliche Datenlöschung gesetzlich und technisch implementieren möchte. Eine Regelung im Polizeigesetz ist gegenüber einem ausgelagerten Polizei-Datenverarbeitungsgesetz vorzugswürdig, damit die Praxis nicht mit einer unüberschaubaren Anzahl an Gesetzen überfordert wird. Selbst wenn die geplanten Regelungen im Polizeigesetz normiert werden, ist nicht davon auszugehen, dass sämtliche Polizeibeamtinnen und Polizeibeamten diese dann auch kennen. Aus diesem Grund ist eine technische Implementierung der Regelungen zu begrüßen, damit die Anwendung der Datenschutzregelungen für die Praxis möglichst einfach und mit geringstmöglichem Aufwand verbunden ist. Nur wenn die Vorschriften zur Datenverarbeitung und Löschung automatisiert umgesetzt werden, ist gewährleistet, dass die Regeln auch befolgt werden und nicht graue Theorie bleiben.

Es lohnt sich, im Zusammenhang mit dem Regelungsauftrag an die Landesregierung einige Aspekte näher zu beleuchten.

1. Der Landtag beauftragt die Landesregierung, eine Regelung im Polizeigesetz zu schaffen, nach der die Löschung personenbezogener Daten ehemals Beschuldigter als Regelfall normiert wird und nach einem festgelegten Zeitablauf automatisch erfolgt. Die fortdauernde Speicherung ist als Ausnahmefall, der einer besonderen Begründung bedarf, festzuschreiben.

Löschung personenbezogener Daten von unschuldig verfolgten Personen: Regel-Ausnahme-Verhältnis

Nach einem rechtskräftigen Freispruch, der unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens oder der nicht nur vorläufigen Verfahrenseinstellung ohne sog. Restverdacht ist die Speicherung der personenbezogenen Daten der betroffenen Person (im Folgenden „unschuldig verfolgte Person" genannt) gem. § 22 Abs. 3 S. 1 PolG NRW sofort unzulässig. Sobald die Staatsanwaltschaft der Polizei durch die entsprechende Erledigungskennziffer einen solchen Verfahrensausgang und das Nichtbestehen eines Restverdachts mitteilt, sind die personenbezogenen Daten der unschuldig verfolgten Person unverzüglich aus allen Datenbanken zu löschen. Das ist bereits geltendes Recht.

Aktuell sieht § 22 Abs. 3 S. 1 PolG NRW allerdings vor, dass die Speicherung personenbezogener Daten von unschuldig Verfolgten nur unzulässig ist, „*wenn sich aus Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat*". Damit ist die Datenspeicherung grundsätzlich zulässig und nur ausnahmsweise unzulässig. Wenn die Rückmeldung an die Polizei unterbleibt oder unvollständig ist,[1] bleiben im Zweifel die Daten gespeichert. Um das Regel-Ausnahme-Verhältnis im oben genannten Sinne zu regeln, wäre es sinnvoll, § 22 Abs. 3 S. 1 PolG NRW zu ändern. Das Gesetz sollte vielmehr formulieren, dass die weitere Datenspeicherung unschuldig verfolgter Personen nach Verfahrensabschluss unzulässig ist, „es sei denn" es besteht ein Restverdacht. Diesen eventuellen Restverdacht muss

[1] Siehe Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, 27. Bericht zum Datenschutz, S. 53.

die speichernde Stelle begründen und – wie bereits nach geltendem Recht (§ 22 Abs. 3 S. 2 PolG NRW) – dessen Gewicht und den Grad des Verdachts dokumentieren. Entsprechend wären auch die Erledigungskennziffern anzupassen. Das Bestehen eines Restverdachts sollte die gesondert zu erwähnende und zu begründende Ausnahme sein, nicht dessen Nichtbestehen.

Sollte ein Restverdacht bestehen oder noch geprüft werden, könnte man auch bei geplanter Fortführung der Speicherung dennoch die Datennutzung erheblich einschränken, indem man die Daten etwa in ein Archiv verschiebt, aus dem sie nur durch bestimmte Personen (etwa den behördeninternen Datenschutzbeauftragten) bei Bedarf – in konkreten Einzelfällen – wieder hervorgeholt werden können. Würde bei einer Polizeikontrolle etwa nur noch angezeigt, dass es zu der kontrollierten Person einen Datensatz im Archiv gibt, aber darüber hinaus keine weiteren Details, wäre das Risiko unzulässiger Verwendung der Daten reduziert und der betroffenen Person schon sehr geholfen.

Löschung personenbezogener Daten anderer Personen nach Zeitablauf

Für die Löschung *zulässig* gespeicherter personenbezogener Daten gibt es keine festen Löschungsfristen, sondern nur Prüffristen. § 22 Abs. 2, 4 PolG NRW schreibt die Festlegung von Prüfterminen fest, zu denen spätestens überprüft werden muss, ob die suchfähige Speicherung von Daten weiterhin erforderlich ist. Diese dürfen bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre nicht überschreiten. Dabei ist diese Begrenzung nur das Höchstmaß, die Festlegung deutlich kürzerer Fristen ist rechtlich ohne weiteres möglich. § 22 Abs. 2 S. 7 PolG NRW verlängert die Prüffristen unter Umständen ganz erheblich, indem nicht jedes Ereignis separat, sondern alle Ereignisse einer Person zusammen betrachtet werden. Diese Regelung kann dazu führen, dass auch nicht benötigte Daten über Jahrzehnte hinweg gespeichert werden, sofern immer wieder neue personenbezogene Daten über dieselbe Person gespeichert werden. Den Fortbestand dieser Regelung könnte man überdenken. Im Sinne des Datenschutzes wäre es vorzugswürdig jedes Ereignis einzeln zu betrachten.

Es sollte dann auch eine Regelung über die maximale Speicherdauer sowie über die weiteren Prüffristen nach weiterer Speicherung geschaffen werden. Wenn die weitere Speicherung be-

stimmter personenbezogene Daten also beispielsweise nach zehn Jahren weiterhin erforderlich ist, soll die Speicherung nicht automatisch für weitere zehn Jahre möglich sein. Vielmehr soll sich daran eine kürzere Frist zur erneuten Prüfung der weiteren Speicherung anschließen. Diese müsste in der Kennzeichnung des Datensatzes vermerkt werden. Eine ähnliche Regelung enthält bereits § 22 Abs. 5 S. 3, 4 PolG NRW für die weitere Speicherung personenbezogener Daten von Kontakt-, Begleit- und Auskunftspersonen.

Verschiedene Speicherorte

Das aus datenschutzrechtlicher Perspektive größte Problem ist die Vielzahl verschiedener Speicherorte. In Zeiten zunehmend digitaler und vernetzter Polizeiarbeit landen Datensätze nicht nur lokal auf einem Computer der bearbeitenden Polizeidienststelle. Personenbezogene Daten werden häufig gleich an mehreren Orten gespeichert. Dabei bedienen sich die Polizeibehörden in Nordrhein-Westfalen nicht nur selbstverwalteter Datenbanken, sondern teilen personenbezogene Daten in verschiedenen Zusammenhängen mit anderen Behörden, wie etwa den Polizeibehörden anderer Bundesländer oder Bundespolizeibehörden.

Es gibt mehrere verschiedene Datenbanken,[2] in denen von Polizeibehörden erhobene personenbezogene Daten gespeichert werden. Das sind lokale und regionale Speicherorte, etwa zur elektronischen Aktenführung, Fallbearbeitung und Vorgangsverwaltung. Daneben werden unter bestimmten Voraussetzungen die personenbezogenen Daten aus polizeilichen Verfahren an überregionale Verbunddateien wie INPOL-neu des Bundeskriminalamts, verschiedene Spezialdateien wie z.B. die Rechtsextremismus- und die Antiterrordatei sowie das internationale Schengener Informationssystem SIS weitergeleitet. Außerdem findet in bestimmten überregionalen Fällen ein Datenaustausch in sog. Gemeinsamen Zentren (z.B. dem Gemeinsamen Terrorismusabwehrzentrum – GTAZ) oder auf andere Weise mit Behörden anderer Länder statt. Dabei ist es üblich, dass die Datensätze jeweils kopiert und damit in verschiedenen Systemen gespeichert werden. Die gespeicherten personenbezogenen Daten können sich daher schnell verselbstständigen und auf verschiedenen Wegen verbreiten, ohne dass die ursprünglich fallbearbeitende

[2] Einen Überblick bieten etwa folgende Seiten: https://www.bundesarchiv.de/DE/Content/Downloads/KLA/abschlussbericht-polizeiliche-fachverfahren.pdf?__blob=publicationFile und https://polizeidatenbanken.de/polizei-datenbanken/datenbanken-der-polizei/ (jeweils zuletzt abgerufen am 6.2.2024).

Polizeibehörde die gesicherte Kontrolle über den Verbleib oder auch die Aktualisierung der Daten behält. Datenschutzrechtlich ist sicherzustellen, dass die zu löschenden personenbezogenen Daten aus allen lokalen, regionalen, überregionalen und internationalen Datenbanken gelöscht werden, in die sie Eingang gefunden haben. Darüber hinaus sind auch alle Stellen zur Löschung aufzufordern, die zu löschende Daten zuvor erhalten haben.

In der Informationstechnologie gibt es zwei Ansätze, um diese Aufgabe zu bewältigen:
1. Ein Originaldatensatz wird bei Herausgabe an eine andere Behörde von dieser in Kopie gespeichert und mit Herkunftsangaben gekennzeichnet. Die herausgebende Stelle muss alle empfangenden Stellen über Aktualisierungen und Löschungen des Originaldatensatzes informieren. Die empfangenden Stellen müssen die Aktualisierungen und Löschungen entsprechend in ihren Kopien vornehmen.
2. Der Originaldatensatz wird nur an einem einzigen Speicherort gespeichert und alle Stellen, die die Informationen benötigen, erhalten lediglich Einsicht in den Originaldatensatz (oder nur die benötigten Teile davon), nicht jedoch eine Kopie (sog. „Single Source of Truth“[3]). In den Datenbanken der anderen Behörden wird nicht die Kopie des ganzen Datensatzes, sondern nur ein Verweis auf die Existenz und den Speicherort des Originaldatensatzes hinterlegt.

Aktuell setzen die Polizeibehörden in Nordrhein-Westfalen ebenso wie in anderen Bundesländern auf den erstgenannten Ansatz. Dass die Aktualisierung und Löschung nicht reibungslos funktioniert, weil es vor allem an der aufwändigen Kommunikation hapert, hat die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen im 27. Bericht zum Datenschutz auf Seite 53 moniert. Um den Datenschutz in verfassungsrechtlich gebotener Weise zu gewährleisten, muss daher entweder die Kommunikation zwischen den datenspeichernden Behörden vereinfacht und technisch unterstützt oder der zweitgenannte Ansatz gewählt werden. Wenn die technischen Hürden einer Einsichtnahme in den Originaldatensatz niedrig, der Kopierschutz der Daten jedoch hoch wäre, hätte der zweite Ansatz erhebliches datenschutzrechtliches Potenzial.

[3] https://en.wikipedia.org/wiki/Single_source_of_truth (zuletzt abgerufen am 6.2.2024).

2. Der Landtag beauftragt die Landesregierung, eine Regelung im Polizeigesetz zu schaffen, die sicherstellt, dass Beschuldigte bürokratiearm in einem automatisierten Verfahren darüber informiert werden, welche polizeiliche Stelle in welchem Umfang personenbezogene Daten über sie gespeichert hat.

Eine solche Regelung ist sehr zu begrüßen. Aktuell ist der Aufwand, den Bürgerinnen und Bürger für eine Auskunft über die zu ihrer Person gespeicherten Daten betreiben müssen, groß. Allein schon den richtigen Ansprechpartner herauszufinden, kann bei der großen Anzahl verschiedener möglicher Speicherorte für personenbezogene Daten sehr schwierig sein.

Zu bedenken ist dabei allerdings, dass sich die Regelung an den gesetzlichen Benachrichtigungspflichten orientieren sollte. Eine uneingeschränkte Auskunft über die zur eigenen Person gespeicherten Daten in Echtzeit oder auch nur zu der Tatsache der Speicherung durch eine bestimmte Behörde stünde im Widerspruch zu den Benachrichtigungspflichten über polizeiliche Maßnahmen. Durch eine solche Auskunft könnten verdeckte Ermittlungsmethoden, etwa eine Telekommunikationsüberwachung, vereitelt werden. Im schlimmsten Fall könnten sogar Menschenleben gefährdet werden. Die Benachrichtigungsvorschriften sehen daher vor, dass die betroffenen Personen nicht in jedem Fall sofort und uneingeschränkt von polizeilichen Maßnahmen zu benachrichtigen sind. In manchen Fällen kann eine Benachrichtigung zunächst zurückgestellt und später nachgeholt werden. Beispiele hierfür nennt etwa § 101 Abs. 5 S. 1 StPO: „*Die Benachrichtigung* [über eine verdeckte Ermittlungsmaßnahme, Anm. T.N.] *erfolgt, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten, im Fall des § 110a auch der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers möglich ist.*“ Ähnlich formuliert § 33 Abs. 2 PolG NRW: „*Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, des Bestandes des Staates, von Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, möglich ist. Im Falle des Absatzes 1 Nr. 3 erfolgt die Benachrichtigung erst, sobald dies auch ohne Gefährdung der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers oder der Vertrauensperson möglich ist. Wird wegen des zugrunde liegenden Sachverhaltes*

ein strafrechtliches Ermittlungsverfahren geführt, ist vor Benachrichtigung der in Absatz 1 genannten Personen die Zustimmung der zuständigen Strafverfolgungsbehörde einzuholen." Darüber hinaus gibt es weitere, gesetzlich geregelte Gründe, aus denen eine Benachrichtigung unterbleiben kann. Diese Beschränkungen müssen berücksichtigt werden. In diesem Zusammenhang wäre eine technische Regelung sinnvoll, die es den Sachbearbeiterinnen und Sachbearbeitern ermöglicht, unkompliziert in der Datenverwaltungssoftware anzugeben, ob die Benachrichtigung noch zurückgehalten und damit auch die Daten aus der Auskunft ausgenommen werden sollen. Dabei ist die Ausnahme von Daten aus der Auskunft restriktiv zu handhaben, um den Auskunftsanspruch der betroffenen Person nicht auszuhöhlen.

Zu beachten sind auch Aspekte der Datensicherheit. Eine automatisierte Abfrage muss sicherstellen, dass nur die betroffene Person selbst ihre Informationen erhalten kann und die Informationen nicht durch Dritte abgefangen werden können.

Um mehr Sicherheit vor Missbrauch zu bieten, sollten bei einer automatisierten Anfrage nicht die konkret gespeicherten Daten, sondern nur die speichernden Stellen mit Kontaktdaten sowie ein Hinweis auf die zu schaffende Zentralstelle angezeigt werden. In einem nächsten Schritt könnte die betroffene Person über die zu schaffende Zentralstelle Auskunft über die konkret gespeicherten Daten erhalten. Darüber hinaus sollten betroffene Personen erfahren können, ob und an welche weiteren Stellen die speichernde Stelle ihre personenbezogenen Daten weitergeleitet oder wem sie Einsicht gewährt hat.

Neben den Suchergebnissen sollte ein Hinweis darauf erscheinen, dass die bloße Speicherung personenbezogener Daten durch die Polizei noch keine Aussage darüber trifft, in welcher Rolle die betroffene Person gegenüber der Polizei in Erscheinung getreten ist (etwa als Störer, Verdächtige, Beschuldigter, Opfer, Zeugin oder Kontaktperson). Dadurch können Ängste von Bürgerinnen und Bürgern ebenso wie eine Stigmatisierung im persönlichen Umfeld vermieden oder zumindest reduziert werden.

Für Personen ohne Internetzugang oder ohne Computerkenntnisse sollte die zu schaffende Zentralstelle – aber idealerweise auch wohnortnah jede Polizeidienststelle – die automatisierte Abfrage vornehmen können.

3. Der Landtag beauftragt die Landesregierung, eine Zentralstelle zu schaffen, der gegenüber Betroffene ihre Auskunfts- und Löschungsansprüche durchsetzen können.

Es kann für Betroffene mitunter sehr schwierig sein, herauszufinden, welche staatliche Stelle Daten über sie gespeichert hat. Daher ist es sehr bürgerfreundlich und sinnvoll, eine Zentralstelle zu schaffen, an die sich Betroffene wenden können. Ob diese eine auf Polizeibehörden beschränkte Zuständigkeit haben oder Auskunft über alle Daten speichernden staatlichen Stellen in Nordrhein-Westfalen geben soll, ist eine politische Entscheidung. Am bürgerfreundlichsten wäre sicherlich die letztgenannte Ausgestaltungsmöglichkeit.

Wie bereits in meiner Stellungnahme vom 23.5.2023 (Stellungnahme 18/576) auf Seite 9 ausgeführt, könnte eine solche Zentralstelle an die Dienststelle der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen angegliedert werden.

Mit freundlichen Grüßen

Dr. Tanja Niedernhuber