Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Polizeiliche Recherchen in sozialen Netzwerken zu Zwecken der Gefahrenabwehr und Strafverfolgung

12. März 2012

Mit zunehmender Nutzung sozialer Netzwerke durch Bürgerinnen und Bürger wächst bei Behörden das Interesse an den dort vorhandenen Informationen. Mit einfachen Mitteln, meist schon durch einen Blick auf das Profil, können Behörden eine ganze Reihe von Informationen über die Betroffenen erlangen, dies reicht vom Foto über die Beziehungen zu Freunden, Bekannten und Geschäftspartnern bis hin zur Kommunikation mit Dritten. Genutzt werden diese Möglichkeiten vor allem durch Sicherheitsbehörden für Ermittlungszwecke. Aus datenschutzrechtlicher Sicht sind bei polizeilichen und strafprozessualen Ermittlungen folgende Eckpunkte zu beachten:

I. Verfassungsrechtliche Betrachtung

In sozialen Netzwerken stellen überwiegend natürliche Personen Informationen über sich und teilweise über Andere ein. Hierbei handelt es sich in der Regel um personenbezogene Daten, die dem Schutzbereich des Rechts auf informationelle Selbstbestimmung unterfallen. Daneben eröffnen viele soziale Netzwerke die Möglichkeit der Individualkommunikation, z.B. des Nachrichtenaustauschs mit anderen Nutzern. Hier ist zu prüfen, ob und inwieweit der Schutzbereich des Art. 10 GG eröffnet ist.

1. Ermittlungstätigkeiten können in das **Recht auf informationelle Selbstbestimmung** eingreifen, „wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, **gezielt zusammengetragen**, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt.“[1] Insbesondere handelt sich dann um einen Grundrechtseingriff, „wenn die gewonnenen Informationen einzelnen Personen oder Personenmehrheiten zugeordnet werden.“[2] Auch wenn der Staat grundsätzlich die jedermann zugänglichen Inhalte wie jeder Dritte zur Kenntnis nehmen darf, ist das Grundrecht stets betroffen, wenn die aus öffentlich zugänglichen Quellen

[1] BVerfG, Urteil vom 27.02.2008, 1 BvR 370/07, 1 BvR 595/07, Absatz-Nr. 309.

[2] BVerwG NVwZ 2011, 161, 163 Abs. Nr. 17.

stammenden Daten durch ihre systematische Erhebung, Sammlung und Erfassung einen zusätzlichen Aussagewert erhalten.[3]

2. Ein **Grundrechtseingriff** kann nur in solchen Fällen verneint werden, in denen der Staat allgemein zugängliche Inhalte wie jeder Dritte zur Kenntnis nimmt, ohne diese zielgerichtet zu einer Person zu sammeln (insb. sog. Internetstreife).[4] Ob bereits die bloße Kenntnisnahme und Sichtung von Daten im Internet in das Recht auf informationelle Selbstbestimmung eingreift, richtet sich nach der Rechtsprechung des Bundesverfassungsgerichts im Einzelnen danach, ob dabei ein **schutzwürdiges Vertrauen** des Betroffenen ausgenutzt wird: „Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt nicht schon dann vor, wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt, wohl aber wenn sie dabei ein schutzwürdiges Vertrauen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde."[5]

   Während das Bundesverfassungsgericht in der zitierten Entscheidung für die Fallgestaltung von Internetforen und Chaträumen davon ausging, dass ein solches schutzwürdiges Vertrauen im Internet nur schwerlich entstehen kann, da für die Überprüfung der Identität und Wahrhaftigkeit der Kommunikationspartner keinerlei Mechanismen bereitstehen[6], kann diese Bewertung für die Nutzung von sozialen Netzwerken nicht uneingeschränkt übernommen werden. Denn anders als in Internetforen und Chaträumen kommunizieren in sozialen Netzwerken überwiegend Personen mit echten Identitäten, die meist auch im realen Leben miteinander bekannt sind. Es kann zwar nicht davon ausgegangen werden, dass jede Identität in sozialen Netzwerken echt ist und jede Angabe der Wahrheit entspricht.[7] Im Ergebnis bleibt aber ein wesentlicher Unterschied der sozialen Netzwerke zu der vom Bundesverfassungsgericht beschriebenen Internetkommunikation. Die Welt der sozialen Netzwerke ist in weiten Teilen keine vom Alltagsleben abgekoppelte Parallelwelt im Internet, sondern überwiegend vermengt sich darin die reale Welt mit der virtuellen Welt. Dadurch gibt es in sozialen Netzwerken weitaus mehr Anknüpfungspunkte für die Bildung von schutzwürdigem Vertrauen in die Identität der Kommunikationspartner, als dies in anderen Bereichen des Internet der Fall ist.

---

[3] BVerwG NVwZ 2011, 161, 163, Abs. Nr. 17.

[4] vgl. BVerfG, a.a.O. Absatz-Nr. 305, 308.

[5] BVerfG, a.a.O., Absatz-Nr. 310.

[6] BVerfG, a.a.O., Absatz-Nr. 311.

[7] Studien über die Ehrlichkeit der Nutzer in sozialen Netzwerken kommen zu unterschiedlichen Ergebnissen: Während einige Studien ergeben, dass falsche Angaben in Profilen durchaus gängig sind - von der falschen Angabe über das Alter oder Beziehungsstatus bis zur Angabe eines falschen Namens - siehe BITKOM, Pressemitteilung vom 18. Mai 2011: „Jedes vierte Mitglied flunkert in sozialen Netzwerken", vom 12. Januar 2010: „12 Millionen Deutsche machen Falschangaben im Web", bescheinigen andere Studien den Nutzern ein großes Maß an Ehrlichkeit, vgl. dazu Der Spiegel 2/2011, „Im Netz der Späher", S. 114, 121: „Überraschend ehrlich geht es bei der Pflege der Profile in diesen Sozialnetzen zu, wie mehrere Studien gezeigt haben. Von kleineren Retuschen abgesehen, präsentieren die Leute sich weitgehend so, wie sie sind. Der Traum vom Internet als Maskenball der Identitäten begeistert nur noch die kleine Minderheit der Rollenspieler."

Im Ergebnis können die Maßstäbe des Bundesverfassungsgerichts für das Vertrauen im Internet im Bereich der sozialen Netzwerke nur so verstanden werden, dass die Schwelle für die Schaffung eines schutzwürdigen Vertrauens nicht so hoch angesetzt werden kann, dass dies nur bei Identitätsüberprüfung mittels Post-Ident-Verfahren oder ähnlicher Mechanismen entstehen kann. Vielmehr muss berücksichtigt werden, dass es in sozialen Netzwerken andere Anknüpfungspunkte für die Entstehung von schutzwürdigem Vertrauen gibt.

Wann die Nutzeraktivitäten in sozialen Netzwerken im **Einzelfall** schutzwürdiges Vertrauen genießen, kann nicht allein objektiv entschieden werden, da die Entstehung von Vertrauen durch subjektive Faktoren beeinflusst wird. Es sind daher stets alle Umstände des Einzelfalls zu würdigen. Anknüpfungspunkte für die Bildung von **Vertrauen** können insbesondere folgende Umstände sein:

1. Der Personenkreis, dem Informationen zugänglich werden, ist durch bestimmte Merkmale eingegrenzt.

2. Die Anzahl der Personen, denen die Informationen zugänglich werden, ist gering.

3. Die Einrichtung des Zugriffs auf die Daten ist eingeschränkt und wird überprüft (z.B. durch den Nutzer selbst, indem er bestimmt, welchen Personen er als „Freunden“ Zugriff auf Daten gewährt, durch einen Gruppenmoderator, der über die Aufnahme von Nutzern in geschlossene Gruppen entscheidet oder durch Nutzungsbeschränkungen für ein soziales Netzwerk, für das besondere Teilnahmebedingungen erfüllt werden müssen).

Das so entstandene Vertrauen muss nach der Rechtsprechung des Bundesverfassungsgerichts **schutzwürdig** sein. Hier ist eine objektive Betrachtung möglich. Dabei ist etwa zu berücksichtigen, ob die Eingrenzung einer Gruppe nach Merkmalen tatsächlich eine Abgrenzbarkeit gewährleistet oder wie die Überprüfungsmechanismen bei geschlossenen Gruppen ausgestaltet sind. Auch ist zu berücksichtigen, ob und inwieweit die Nutzungsbedingungen des Betreibers dem Nutzer die tatsächliche Herrschaft über die Vertraulichkeitseinstellungen ermöglichen. So verliert etwa ein Nutzer sein schutzwürdiges Vertrauen in die Beschränkung der Zugriffsmöglichkeiten nicht deshalb, weil der Anbieter des sozialen Netzwerks ohne sein Zutun die Nutzungsbedingungen ändert und dadurch z.B. die Zugriffsmöglichkeiten Dritter erweitert. Im Grundsatz ist davon auszugehen, dass zumindest unter den oben in Ziffer 3 genannten Voraussetzungen ein schutzwürdiges Vertrauen besteht, denn der Nutzer oder die Gruppe von Nutzern hat durch eine Einschränkung der Zugriffsrechte deutlich gemacht, dass die Inhalte nicht an jedermann gerichtet sind. Solange die Polizei keine positiven Anhaltspunkte dafür hat, dass der Nutzer oder die Gruppe von Nutzern gleichwohl auf Vertrauen verzichten, muss sie davon ausgehen, dass ein schutzwürdiges Vertrauen in die Identität der Kommunikationspartner besteht. Dies gilt umso mehr, je sensibler die Informationen sind, die in diesem Kreis ausgetauscht werden und je schutzwürdiger der betroffene Personenkreis ist. So sind bei betroffenen Kindern und Jugendlichen andere Maßstäbe anzulegen als bei Erwachsenen.

3. Ein Eingriff in das durch **Artikel 10 GG** geschützte **Telekommunikationsgeheimnis** wird nur im Ausnahmefall vorliegen. Das Bundesverfassungsgericht unterscheidet im Schutzbereich des Art. 10 Abs. 1 GG zwischen der Überwachung einer

Telekommunikation „von außen“ sowie der Überwachung „von innen“, d.h. Überwachung in der Weise, dass staatliche Stellen sich als Kommunikationspartner (unter Legende) an der Kommunikation beteiligen. „Steht im Vordergrund einer staatlichen Ermittlungsmaßnahme nicht der unautorisierte Zugriff auf die Telekommunikation, sondern die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner, so liegt darin kein Eingriff in Art. 10 Abs. 1 GG. Die staatliche Wahrnehmung von Inhalten der Telekommunikation ist daher nur dann am Telekommunikationsgeheimnis zu messen, wenn eine staatliche Stelle eine Telekommunikationsbeziehung von außen überwacht, ohne selbst Kommunikationsadressat zu sein. Das Grundrecht schützt dagegen nicht davor, dass eine staatliche Stelle selbst eine Telekommunikationsbeziehung zu einem Grundrechtsträger aufnimmt“[8]. Das Bundesverfassungsgericht nimmt einen Eingriff in Art. 10 GG bei einem Eindringen in Kommunikationen im Internet (gedacht ist immer an das Eindringen in Chaträume) nur an, wenn dafür Zugangsschlüssel genutzt werden, die die staatliche Stelle ohne Willen der Kommunikationspartner erhoben hat.

II. Einfachgesetzliche Zulässigkeit

Für die Zulässigkeit von Recherchen ergibt sich daraus Folgendes:

1. Recherchen ohne Ausnutzung schutzwürdigen Vertrauens / allgemein zugängliche Daten

Sichten die Behörden Daten aus sozialen Netzwerken, die sich an jedermann oder an einen nicht abgrenzbaren Personenkreis richten, liegt darin nicht unbedingt ein Grundrechtseingriff (siehe oben). Ein solcher liegt jedoch vor, wenn Daten zielgerichtet erhoben und zusammengetragen werden. Eine zielgerichtete Beschaffung personenbezogener Daten stellt zumindest eine Erhebung im Sinne des allgemeinen Datenschutzrechts dar, für die es einer gesetzlichen Grundlage bedarf.

Soweit es sich bei einer Erhebung und weiteren Verarbeitung solcher Daten nicht um schwerwiegende Eingriffe handelt, weil die erhobenen Daten allgemein zugänglich sind, reichen die **Generalbefugnisse** aus dem Polizeirecht oder aus §§ 161, 163 StPO als Rechtsgrundlage in der Regel aus. Voraussetzung ist hiernach, dass die Kenntnis der Daten für die Durchführung eines strafrechtlichen Ermittlungsverfahrens oder zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist.

Diskutiert wird in diesem Zusammenhang immer wieder die Frage, ob die Polizei ihre Recherchen in den allgemein zugänglichen Bereichen offen durchführen muss oder ein **Pseudonym** verwenden darf. Die Strafprozessordnung fordert nicht für jegliche nach außen nicht als solche erkennbare Ermittlungsmaßnahme eine besondere gesetzliche Grundlage, die den Strafverfolgungsbehörden ein verdecktes Vorgehen erlaubt. Weniger grundrechtsintensive Maßnahmen können auch nach §§ 161, 163 StPO nicht offen ausgeübt werden. Um eine solche Maßnahme handelt es sich bei Recherchen ohne Ausnutzung eines schutzwürdigen Vertrauens, da der Betroffene für diese Daten kein Interesse daran zum Ausdruck bringt, dass diese nur bestimmten Personen zugänglich sein sollen. §§ 161, 163 StPO umfassen in diesem Bereich also auch die pseudonyme

---

[8] BVerfG vom 27.02.2008, Absatz-Nr. 290.

Nutzung. Für die Verwendung von Pseudonymen spricht ein weiteres Argument: Zugriffe von Nutzern sind für den Betreiber eines sozialen Netzwerks beobachtbar: Betreiber können technisch mitprotokollieren, auf welche Profile Ermittler oder potenziell ermittelnde Behörden zugegriffen und welche Links (z.B. zu Bildern, Pinnwandeinträgen oder auch Kontakten des betroffenen Nutzers) sie angeklickt haben. Insbesondere im Ausland ansässige soziale Netzwerke speichern auf unbestimmte Zeit Daten über ihre Nutzer und deren Verhalten; diese Daten werden dann insbesondere dazu ausgewertet, um Nutzern individuell auf sie zugeschnittene Werbung zu präsentieren. Selbst wenn der Betreiber kein eigenes Interesse an einer Auswertung der Daten hat, um das Ermittlungsverhalten deutscher Polizeibehörden zu analysieren oder potenziell Verdächtige zu identifizieren, kann dies durchaus im Interesse staatlicher ausländischer Stellen sein, denen das für sie gültige Rechtssystem Zugriff auf diese Daten einräumt.

2. Recherchen unter Ausnutzung schutzwürdigen Vertrauens / nicht allgemein zugängliche Daten

Die Erhebung von Daten in sozialen Netzwerken unter Ausnutzung eines schutzwürdigen Vertrauens stellt in jedem Fall einen Grundrechtseingriff dar. In den meisten Fällen ist das Recht auf informationelle Selbstbestimmung betroffen. Nur, wenn ohne den Willen der Kommunikationspartner deren Zugangsschlüssel durch die Polizei genutzt werden, ist von einem Eingriff in Artikel 10 GG auszugehen (siehe oben). Der Eingriff in beide Grundrechte bedarf einer hinreichend normenklaren und verhältnismäßigen gesetzlichen Grundlage.

Als typische Maßnahme für die Erlangung von Inhaltsdaten aus einer elektronisch geführten Kommunikation ist bislang die Sicherstellung oder **Beschlagnahme** solcher Daten nach §§ 94 ff. StPO, entweder beim Betroffenen oder beim Diensteanbieter, durchgeführt worden. Diese Maßnahme kommt grundsätzlich auch für die über ein soziales Netzwerk ausgetauschten Inhaltsdaten in Betracht. Die Sicherstellung oder Beschlagnahme ist in der Regel als offene Maßnahme ausgestaltet. Speziell zur Beschlagnahme von E-Mails beim Provider fordert das Bundesverfassungsgericht, dass der Postfachinhaber „im Regelfall zuvor von den Strafverfolgungsbehörden unterrichtet wird, damit er jedenfalls bei der Sichtung seines E-Mail-Bestands seine Rechte wahrnehmen kann.“[9] Dies ist für die Sicherstellung und Beschlagnahme, insbesondere bei vorangehender Durchsuchung, grundsätzlich durch § 35 und § 98 Abs. 2 Satz 6 StPO gewährleistet.[10]

Führt die Polizei anstelle einer Sicherstellung oder Beschlagnahme heimlich eigene Recherchen in geschützten Bereichen eines sozialen Netzwerks durch, umgeht sie damit das Prinzip der Offenheit.

Verdeckte Ermittlungsmaßnahmen stellen gegenüber offenen Maßnahmen grundsätzlich einen schwerwiegenderen Grundrechtseingriff dar. Bereits aus diesem Grund ist fraglich, ob die Generalklauseln der Polizeigesetze oder §§ 161, 163 StPO als Rechtsgrundlage für verdeckte Recherchen in dem geschützten Bereich der sozialen

---

[9] BVerfG, NJW 2009, 2431, 2437, Absatz-Nr. 94.

[10] Näher dazu BVerfG, a.a.O (Fn.9), Absatz-Nr. 95.

Netzwerke in Betracht kommen. Die Zweifel werden dadurch verstärkt, dass zum Teil sensible Inhaltsdaten erhoben werden können und die Streubreite der Maßnahme mitunter sehr groß sein kann, da auch die Beiträge sämtlicher anderer Nutzer erhoben werden. Das Gewicht eines solchen Eingriffs kann das einer verdeckten Telekommunikationsüberwachung erreichen oder gar übersteigen. Dabei ist zu bedenken, dass die Telekommunikationsüberwachung üblicherweise nur die während der laufenden Überwachungsmaßnahme ausgetauschten Inhalte erfasst. Recherchen in sozialen Netzwerken können zeitlich weit darüber hinausgehende Inhalte erfassen, da die dort eingestellten Inhalte in der Regel nicht flüchtig sind. So können etwa bei einem Blick auf das nicht öffentlich zugängliche Profil in einem sozialen Netzwerk Daten erhoben werden, die weit in die Vergangenheit zurück reichen. Zudem erschließen sich sozusagen auf einen Click sämtliche Beziehungen der Zielperson zu anderen Nutzern des sozialen Netzwerks. Aus diesen Gründen bestehen erhebliche Bedenken gegen eine Anwendbarkeit der Ermittlungsgeneralklauseln für Recherchen in geschützten Bereichen.

Spezielle Vorschriften, die die verdeckte Maßnahme erlauben, sind allenfalls in einigen Fällen anwendbar. Die Anwendbarkeit des § 100a StPO oder entsprechender Regelungen für die Telekommunikationsüberwachung in den Polizeigesetzen scheidet im Regelfall aus, da das Eindringen als Kommunikationspartner in eine Kommunikation keine Maßnahme in diesem Sinne ist.[11] § 110a StPO kommt als Rechtsgrundlage nur bei bestimmten Straftaten und nur als letztes Mittel in Betracht. Für Maßnahmen gegen einen bestimmten Beschuldigten ist zudem nach § 110b Abs. 2 StPO die Zustimmung des Gerichts erforderlich. Ähnliches gilt für Maßnahmen nach den Polizeigesetzen der Länder, die an bestimmte Gefahrenschwellen geknüpft sind und teilweise ebenfalls einen Richtervorbehalt vorsehen.

Sobald die Voraussetzungen der speziellen Befugnisnormen nicht erfüllt sind und angesichts der Eingriffsintensität heimlicher Recherchen zweifelhaft ist, ob die Maßnahmen auf die Generalklauseln gestützt werden können, besteht erhebliche Rechtsunsicherheit. Möglicherweise wird im Ergebnis der Gesetzgeber gefordert sein, die bestehende Rechtsunsicherheit zu beseitigen, indem er entweder die notwendigen Rechtsgrundlagen schafft oder durch eine Klarstellung Eingrenzungen für die schon bestehende Praxis vornimmt.

[11] Siehe dazu BGH, NJW 1994, 596; BVerfG NJW 2002, 3619.