Facebook, Freund, Genosse

— Facebook als Waffe der Strafverfolger —

Datensicherheit & Datenschutz
causa-finita.com
info@causa-finita.com

10. Juni 2015

Wir arbeiten mit den Strafverfolgungsbehörden für die Sicherheit online und offline zusammen.[1]

Was passiert eigentlich, wenn ein deutsches Gericht versucht, ein Benutzerprofil bei Facebook zu beschlagnahmen? Diese Frage ist nicht einfach zu beantworten. Ausgehend von einem Beschluss des AG Reutlingen vom 31. Oktober 2011 (Az. 5 Ds 43 Js 18155/10) kann man festhalten, dass Facebook zumindest im Jahr 2011 und im konkreten Fall nicht dazu zu bewegen war, die Nutzerdaten herauszugeben. Nachdem sich die deutsche Filiale für nicht zuständig erklärt hatte, wurde der Richter von Facebook Irland an den Hauptsitz von Facebook in den USA verwiesen. Dort wurde eine Herausgabe der Daten ohne formelles Verfahren in den USA verweigert. Doch bevor es zu einem langwierigen Verfahren in den USA kam, gab der Anklagte die Daten selbst heraus. Würde Facebook sich immer konsequent weigern und hätte der Staat sonst keinen Zugriff auf Facebook, wäre die Angelegenheit durchaus tragbar. Doch leider ist die Sache nicht so einfach, denn Facebook erklärt sich grundsätzlich zur Zusammenarbeit mit Strafverfolgungsbehörden bereit. Einen Einblick in die Kooperation von Facebook mit staatlichen Stellen gibt der "Transparenzbericht" von Facebook, der aufschlüsselt, wie viele Anfragen es von staatlicher Seite angeblich gab, wie viele Nutzerprofile von diesen Anfragen betroffen waren und in wie vielen Fällen eine Weitergabe von Daten stattgefunden hat. Facebook verschweigt aber, welche Daten weitergegeben wurden und spricht lediglich von "Percentage of requests where some data produced". Nun speichert Facebook bekanntermaßen viele Informationen und welche Datensätze weitergegeben wurden, kann nicht nachvollzogen werden. Was Facebook speichert, hat die Initative "europe vs. facebook" auf ihrer Website aufgeschlüsselt. Dort findet man auch Informationen, wie man seine eigenen, bei Facebook gespeicherten, Daten einsehen kann.

Tabelle 1: Anfragen aus Deutschland laut Facebook-Transparenzbericht

Zeitraum	Anzahl der Anfragen	Betroffene Profile	Datenweitergabe
Juli 2014 - Dezember 2014	2,132	2,611	34.29%
Januar 2014 – Juni 2014	2,537	3,078	33.94%
Juli 2013 – Dezember 2013	1,687	1,950	37.88%
Januar 2013 – Juni 2013	1,886	2,068	37.00%

Geheimdienste & Facebook: PRISM

Was die Zusammenarbeit mit Geheimdiensten angeht, scheint die Mitarbeit von Facebook aber deutlich weiter zureichen, als im "Transparenzbericht" eingeräumt. Aus den Snowden-Dokumenten lässt sich entnehmen, dass die NSA mit dem Programm "PRISM" seit 2009 Zugriff auf die Server von Facebook hat. Wie "PRISM" genau funktioniert und wie weit die Kollaboration von Facebook mit der NSA reicht, lässt sich nicht sagen. Dass Daten von Facebook durch die NSA an den BND oder den Verfassungsschutz weitergegeben werden, ist definitiv nicht ausgeschlossen, lässt sich aber nicht beurteilen.

[1] https://www.facebook.com/safety/groups/law/

Exkurs I: Social Media Monitoring

Social Media Monitoring ist eigentlich eine Technik aus dem Marketingbereich. Durch eine systematische, kontinuierliche und themenspezifische Suche, Erhebung, Aufbereitung, Analyse, Interpretation und Archivierung von Inhalten aus sozialen Medien soll die Möglichkeit geschaffen werden Markttrends des eigenen Unternehmens oder der Konkurrenz zu verfolgen. Damit lässt sich dann z.B. die Reichweite einer Werbekampagne erfassen. Es liegt auf der Hand, dass solche Techniken auch für staatliche Akteure interessant sind und deshalb laufen sowohl beim BND, als auch bei Bundeswehr und Verfassungsschutz Projekte, die eine Echtzeitanalyse der sozialen Netzwerke ermöglichen sollen.

be sceptical

Dass Ermittlungsbehörden nicht auf die Nutzung von Facebook als Ermittlungswerkzeug verzichten wollen, liegt auf der Hand. Allein Facebooks "Klarnamenpflicht" ist hervorragend geeignet, die Anonymität der Nutzer aufzuheben. Wer in Zukunft seinen PGP-Key bei Facebook hinterlegt, kann zugeordnet und mit verschlüsselter (und damit per se verdächtiger) Kommunikation in Verbindung gebracht werden. Doch die Polizei stoppt nicht bei der Identitätsfeststellung. Facebook wird in Bild und Text auch auf Hinweise zu Straftaten oder Verbindungen zwischen Personen und Gruppen durchsucht. Dabei ist für das Durchsuchen von "öffentlichen" Inhalten oder solchen, die "Freunde von Freunden" sehen können, keine besondere Hürde zu überwinden. Die Grundlage für strafrechtliche Ermittlungen ist die Generalklausel der §§ 161, 163 StPO, für präventive Maßnahmen greift die Generalklausel des jeweiligen Polizeirechts. Auf dieser Grundlage dürfen auch Personen "geaddet" werden, um Inhalte für "Freunde" anzusehen und zwar dann, wenn die "Freundesliste" keine wirksame Barriere gegen nicht vertrauenswürdige Personen darstellt. Das Anlegen von Fake-Profilen zur Informationsgewinnung ist also rechtlich zulässig. Hoch umstritten ist aber, ab wann es sich dabei um den Einsatz eines eines nicht-öffentlich ermittelnden Polizeibeamten (noeP) oder den Einsatz eines verdeckten Ermittlers handelt. Das spielt eine Rolle, weil für den Einsatz eines verdeckten Ermittlers – im Gegensatz zum noeP – die höheren Anforderungen der §§ 110a ff StPO (z.B. Vorliegen einer Straftat von erheblicher Bedeutung, Zustimmung der Staatsanwaltschaft) zu erfüllen sind. Im Grundsatz liegt der Einsatz eines verdeckten Ermittlers vor, wenn ein Polizeibeamter mit einer falschen Legende und auf Dauer (mindestens dreimal Kontakt zum Betroffenen) tätig wird. Das Anlegen eines Facebook-Profils unter einem falschen Namen und mit einigen, wenigen Informationen wird allerdings noch nicht als Anlegen einer Legende interpretiert. Vielmehr soll die Entscheidung an Hand von verschiedenen Kriterien getroffen werden, wobei insbesondere die Intensität der Zugangskontrolle durch den Anbieter (Facebook), die Glaubwürdigkeit des Ermittler-Profils, aber auch die Anzahl der Freunde des Betroffenen eine Rolle spielt. Außerdem soll es für den Betroffenen nachteilig sein, wenn er sich unter einem falschen Namen bei Facebook bewegt, da er dann ja wissen muss, dass man sich auch mit falschen Informationen anmelden kann. Schlussendlich kann der Einsatz natürlich auch einfach rechtswidrig sein und die erlangten Informationen finden gar nicht oder auf anderem Wege Einzug in die Ermittlungsakte, was man dann nur schwer nachweisen kann.

Exkurs II: Social Plugin aka "Like-Button"
Der "Like-Button" von Facebook oder ähnliche Plugins, z.B. von Google+ oder Twitter, können von Webseiten-Betreibern in die eigene Website eingebunden werden, um Besuchern das einfache Teilen von Inhalten zu ermöglichen. Das Einbinden sorgt allerdings dafür, dass bereits beim Aufruf der Website persönliche Daten an die jeweilige Website übertragen werden. Dies geht soweit, dass der Aufruf jeder einzelnen Website protokolliert und mit dem (eingeloggten) Nutzerprofil verknüpft wird. Aus diesem Grund ist das Einbinden von Social Plugins sogar nach deutschem Datenschutzrecht unzulässig.

Weitere Literatur:

- Warum man sein Facebook-Konto löschen sollte: causa-finita.com/ich-glaub-bei-dir-zwitscherts
- Strafverfolgung in Sozialen Netzwerken von Dr. Saleh Ramadan Ihwas, ISBN 978-3-8487-1547-3
- Anfrage der Linkspartei zur Nutzung sozialer Netzwerke zu Fahndungszwecken (BT-Drucksache 17/6587)
- Zu Fragen rund um Social Plugins: www.datenschutzbeauftragter-info.de