**Staatliche Betätigung auf sozialen Netzwerken - Fluch oder Segen?**

Durch die immens voranschreitende Digitalisierung nutzen auch staatliche Einrichtungen zunehmend soziale Netzwerke, um eine bessere Kommunikation mit der Bevölkerung zu gewährleisten und dem oft negativ empfundenen Behördenapparat einen Imagewechsel zu verpassen. Dementsprechend sind Behörden, Gemeinden, Ministerien und Politiker inzwischen häufig sowohl auf Facebook als auch auf Twitter vertreten und von dort auch insgesamt überhaupt nicht mehr hinwegzudenken.
Die Polizei München kommunizierte beispielsweise bei dem Anschlag auf das OEZ München im Sommer 2016 via Twitter mit der besorgten Bevölkerung und gab regelmäßige Updates über den aktuellen Stand der Ermittlungen, woraufhin der Pressesprecher der Polizei frenetisch als *Held des Abends* gefeiert wurde.[[1]](#footnote-1)
Gleichwohl versucht der Staat mit der Zeit zu gehen, flexibleren Zugang zu seinen Verwaltungsapparaten zu schaffen und amtliche Bekanntmachungen im Internet zu veröffentlichen.[[2]](#footnote-2)
Zudem kommt bekanntermaßen dem Kontaktaustausch über das Internet vor allem für Politiker und Parteien im Wahlkampf enorme Bedeutung zu.
Jedoch stellt sich die Frage, inwiefern die staatliche digitale Betätigung zu bewerten ist und welcher rechtlichen Verantwortung sich der Staat für die Daten der Besucher seiner Onlineprofile stellen muss.

1. **Staat – Vorbildfunktion?**

Auch wenn staatliche Einrichtungen häufig in der Kritik stehen, so lässt sich dennoch nicht leugnen, dass der Staat als langjährige Konstante dem Bürger stets ein Gefühl der Sicherheit und Transparenz vermittelt und dementsprechend auch eine gewisse Vorbildfunktion innehat.
In der Regel ist dem Bürger nicht klar, welcher privaten Dienstleister und technischen Hilfsmittel sich Behörden bedienen und in den meisten Fällen ist dies auch nicht von Bedeutung.[[3]](#footnote-3)

Dies gilt aber nicht mehr, sobald sich Behörden bei privaten Firmen, wie Facebook oder Twitter, einen Account erstellen, um mit der Bevölkerung zu kommunizieren.[[4]](#footnote-4)

Zwar wird dem Bürger die Möglichkeit eröffnet, hierüber kostenfrei mit der Behörde in Kontakt zu treten, allerdings bezahlt er dies mit einem wesentlich teureren Gut als

Geld - nämlich mit seinen persönlichen Daten.[[5]](#footnote-5)
 Behörden werben durch derartige Aktivitäten für die gewählten Plattformen, unabhängig davon, ob dies bewusst oder unbewusst geschieht.[[6]](#footnote-6)
Dies alleine schon dadurch, indem sie zwangsläufig die Logos der betroffenen privatwirtschaftlichen Unternehmen auf ihrer offiziellen Homepage oder bei offiziellen Auftritten verwenden, um die Bürger überhaupt auf die Nutzung dieser Plattformen aufmerksam zu machen.[[7]](#footnote-7)

Weiterhin suggerieren die Behörden dem Bürger durch ihr Verhalten, dass solche Plattformen unbedenklich nutzbar sind und stempeln diesen quasi eine Art Gütesiegel auf, welches mitunter das beste Werbemittel darstellt.[[8]](#footnote-8)

1. **Rechtliche Hürden am Beispiel des Mediendienstes Twitter**
2. **Konflikt mit Vorschriften des Telemediengesetzes (TMG)**

Auftritte auf Twitter sind als Telemedien zu qualifizieren, mithin ist das TMG anwendbar.[[9]](#footnote-9) Grundsätzlich dürfen personenbezogene Daten ohne Einwilligung des Betroffenen oder ohne Eingreifen einer Rechtsvorschrift nicht verarbeitet werden.
Auf Twitter hinterlässt jeder Nutzer einen digitalen Fußabdruck, da der Dienst zunächst die Nutzerdaten verarbeiten muss, um überhaupt die Nutzung zu ermöglichen.[[10]](#footnote-10) Nachdem der Nutzer die Twitter-Seite verlässt, entfällt das Erfordernis zur Speicherung der IP-Adresse sowie anderer datenschutzrechtlich relevanter Informationen.[[11]](#footnote-11)

Jedoch können ausweislich des TMG Daten ausnahmsweise weiterverarbeitet werden, wenn diese dafür verwendet werden, *pseudonyme Nutzungsprofile zu Werbezwecken* zu erstellen, wovon praktisch jede Reichweitenanalyse, die Twitter bei einem Besuch auf der Seite vornimmt, umfasst wird.[[12]](#footnote-12) Auf diese Weise erstellte Nutzungsprofile dürfen jedoch auf keinen Fall mit Klardaten der Besucher zusammengeführt werden, um zu vermeiden, dass Nutzer auf diese Art identifiziert werden können.[[13]](#footnote-13)
Allerdings führt Twitter ausweislich seiner Datenschutzrichtlinie gerade diese Daten zusammen und sieht auch kein Widerspruchsrecht der Nutzer gegen die Erstellung solcher Profile vor.[[14]](#footnote-14) Damit wird die zentralste Schutzvorschrift des deutschen TMG, nämlich die des § 15 Abs. 3 Satz 2 und Satz 3, nicht eingehalten.[[15]](#footnote-15) Ab Mai 2018 treten einige europarechtliche Verordnungen in Kraft, welche *lex speciales* einige Anwendungsbereiche des deutschen Datenschutzrechts verdrängen.[[16]](#footnote-16) Dabei bleibt die praktische Umsetzung der durchaus widersprüchlichen und teils unklaren Verordnungen abzuwarten.[[17]](#footnote-17)

Festzuhalten bleibt, dass Nutzer durch das Verwenden von Twitter zumindest in ihren Rechten aus dem deutschen TMG verletzt werden.[[18]](#footnote-18)

1. **Datenschutzrechtliche Verantwortung**

Fraglich ist überdies, inwiefern hoheitliche Stellen für etwaige Verletzungen datenschutzrechtliche Verantwortung übernehmen müssen.[[19]](#footnote-19) Im Kern geht es dabei darum, ob nach der derzeit noch geltenden europäischen Datenschutzrichtlinie (DS-RL) eine hoheitliche Stelle, die einen Twitter-Auftritt zur Verfügung stellt, die stattfindenden Datenverarbeitungen selbst bestimmt oder durchführen lässt.[[20]](#footnote-20) Bisher wird diese Verantwortlichkeit weitgehend von Rechtsprechung und Literatur abgelehnt, denn im Endeffekt haben Seitenbetreiber keine Kontrolle über Datenverarbeitungsprozesse auf sozialen Netzwerken.[[21]](#footnote-21)
Dagegen kann angeführt werden, dass in der heutigen digitalisierten Welt nahezu alles mittels Arbeitsteilung abläuft mithin die unmittelbare Kontrolle über eigene Datenverarbeitungsprozesse und IT-Systeme hierdurch zur Ausnahme geworden ist.[[22]](#footnote-22)
Allerdings verweist die Rechtsprechung darauf, dass letztlich zwischen dem Betreiber einer Seite und dem die Infrastruktur betreibenden Unternehmen kein Vertrag zustande kommt, es somit also keine Auftragsdatenverarbeitung gibt, für welche die hoheitliche Stelle verantwortlich gemacht werden könnte.[[23]](#footnote-23) Damit verbleibt die datenschutzrechtliche Verantwortung bei dem sozialen Netzwerk.
Diese Ansicht lässt reichlich Raum für Kritik, da Zweifel darüber bestehen, ob tatsächlich allein ein formell abgeschlossener Vertrag eine datenschutzrechtliche Verantwortung auslösen kann, obwohl es faktisch (auch nach dem europarechtlichen Verständnis von Verantwortung) bereits genügt, dass die Datenverarbeitung *im Interesse* oder *zu Gunsten* des Seitenbetreibers erfolgt.[[24]](#footnote-24) Dementsprechend wäre eine Verantwortlichkeit von hoheitlichen Stellen nicht gänzlich zu verneinen, wenn man bedenkt, dass diese eigene Ziele verfolgen und auch die Wahl des sozialen Netzwerks in der Hand haben.[[25]](#footnote-25)
Diesbezüglich bleibt das Urteil des EuGH[[26]](#footnote-26) abzuwarten, welchem im Rahmen eines Vorabentscheidungsverfahrens vom OVG Schleswig[[27]](#footnote-27) bezüglich seiner Facebook-Entscheidung einige gleichgelagerte Rechtsfragen vorgelegt wurden.[[28]](#footnote-28)

1. **Spannungsverhältnis zu Grundrechten**

Weiterhin steht die Präsenz von hoheitlichen Stellen auf sozialen Netzwerken in einem Spannungsverhältnis zu Grundrechten, an welche diese - im Gegensatz zu Privaten - unmittelbar gebunden sind.[[29]](#footnote-29) Dabei geht es in erster Linie um das Recht auf informationelle Selbstbestimmung, welches Schutz vor nicht gewollter Preisgabe und Verwendung persönlicher Daten bietet. [[30]](#footnote-30) Ein mittelbarer Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung kann darin gesehen werden, dass rein faktisch die Datenverarbeitung der Nutzungsdaten von Besuchern der Selbstdarstellung staatlicher Einrichtungen dient, mithin diesen zurechenbar ist.[[31]](#footnote-31) Zwar können Eingriffe in das Recht auf informationelle Selbstbestimmung aufgrund einer gesetzlichen Grundlage gerechtfertigt sein, jedoch fehlt es wie oben dargestellt bei Twitter-Auftritten gerade an einer solchen.[[32]](#footnote-32)

1. **Politische Relevanz**

Auch in politischer Hinsicht ergeben sich durchaus Widersprüchlichkeiten, beispielsweise dadurch, dass staatliche Behörden diese Dienste verwenden und praktisch dafür werben, jedoch im gleichen Atemzug durch die demnächst geltende europäische Datenschutzgrundverordnung oder durch erheblich in der Kritik stehende Gesetze wie das Netzwerkdurchsetzungsgesetz (NetzDG) gegen *Hate Speech* auf sozialen Netzwerken energischer vorgegangen werden soll.[[33]](#footnote-33)
Zudem äußern sich Politiker wie der US-Präsident Donald Trump mittlerweile via Twitter und anderen sozialen Netzwerken zu brisanten Themen und lösen dadurch ein kontroverses Meinungsbild in der Bevölkerung aus.[[34]](#footnote-34) Bürger laufen Gefahr, verunsichert zu werden, was sich in der Folge teils in Politikverdrossenheit und Protestwahlen niederschlägt.
Ein Beispiel hierfür kann in den *Fake News* gesehen werden, die Trumps Berater während des Wahlkampfes verbreiteten, um das Stimmungsbild der Bevölkerung künstlich gegen Rivalin Hillary Clinton aufzuheizen.[[35]](#footnote-35)

1. **Fazit**

Zusammenfassend lässt sich nicht leugnen, dass der Staat gegenüber dem Bürger eine gewisse Verantwortung bezüglich der Datenverarbeitung auf sozialen Netzwerken innehat und dass in Zukunft einige Veränderungen zum Schutze persönlicher Daten getroffen werden müssen.
Zwar ist es wichtig, dass der Staat im Zuge der Digitalisierung mit der Zeit geht und technische Kanäle errichtet, um eine modernere und flexiblere Kommunikation mit der Bevölkerung vor allem in Verwaltungsangelegenheiten zu eröffnen, jedoch wird der Weg über soziale Netzwerke nicht der Datenschutzverantwortung und Vorbildfunktion des Staates gerecht.
Weiterhin verursachen leichtfertig verfasste Twitter-Tweets und schlecht durchdachte Gesetzesentwürfe in der aktuellen politischen Umbruchphase Verunsicherungen in dem politischen Meinungsbild der Bevölkerung.

Es bleibt zunächst abzuwarten, wie der Gesetzgeber in Zukunft auf die rechtlichen und tatsächlichen Hürden des staatlichen Internetauftritts reagieren wird.

1. <http://www.zeit.de/gesellschaft/zeitgeschehen/2016-07/polizei-muenchen-amoklauf-attentat-oez-schuesse> (zuletzt abgerufen am: 18.01.2018). [↑](#footnote-ref-1)
2. *Engeler,* MMR 2017, 651. [↑](#footnote-ref-2)
3. *Wewer,* ZRP 2016, 23. [↑](#footnote-ref-3)
4. *Wewer,* ZRP 2016, 23. [↑](#footnote-ref-4)
5. *Wewer,* ZRP 2016, 23. [↑](#footnote-ref-5)
6. *Wewer,* ZRP 2016, 23. [↑](#footnote-ref-6)
7. *Wewer,* ZRP 2016, 23. [↑](#footnote-ref-7)
8. *Wewer,* ZRP 2016, 23. [↑](#footnote-ref-8)
9. *Engeler*, MMR 2017, 651, 652. [↑](#footnote-ref-9)
10. *Engeler,* MMR 2017, 651, 652. [↑](#footnote-ref-10)
11. *Engeler,* MMR 2017, 651, 652. [↑](#footnote-ref-11)
12. *Engeler,* MMR 2017, 651, 652. [↑](#footnote-ref-12)
13. *Engeler,* MMR 2017, 651, 652. [↑](#footnote-ref-13)
14. *Engeler,* MMR 2017, 651, 652. [↑](#footnote-ref-14)
15. *Engeler,* MMR 2017, 651, 652. [↑](#footnote-ref-15)
16. *Engeler,* MMR 2017, 651, 652. [↑](#footnote-ref-16)
17. *Engeler,* MMR 2017, 651, 653. [↑](#footnote-ref-17)
18. *Engeler,* MMR 2017, 651, 653. [↑](#footnote-ref-18)
19. *Engeler*, MMR 2017, 651, 653. [↑](#footnote-ref-19)
20. *Engeler,* MMR 2017, 651, 653. [↑](#footnote-ref-20)
21. *Engeler,* MMR 2017, 651, 654. [↑](#footnote-ref-21)
22. *Engeler,* MMR 2017, 651, 654. [↑](#footnote-ref-22)
23. *Engeler,* MMR 2017, 651, 654. [↑](#footnote-ref-23)
24. *Engeler,* MMR 2017, 651, 654. [↑](#footnote-ref-24)
25. *Engeler,* MMR 2017, 651, 654. [↑](#footnote-ref-25)
26. Vorabentscheidungsersuchen des BVerwG v. 14.4.2016 – EuGH Aktenzeichen C-210/16. [↑](#footnote-ref-26)
27. OVG Schleswig, Urt. v. 04.09.2014, 4 LB 20/13; vgl. nachfolgend
BVerwG, EuGH-Vorlage v. 25.02.2016 – Aktenzeichen C – 210/16. [↑](#footnote-ref-27)
28. *Engeler,* MMR 2017, 651, 654. [↑](#footnote-ref-28)
29. *Engeler,* MMR 2017, 651, 655. [↑](#footnote-ref-29)
30. *Engeler,* MMR 2017, 651, 655. [↑](#footnote-ref-30)
31. *Engeler,* MMR 2017, 651, 655. [↑](#footnote-ref-31)
32. *Engeler,* MMR 2017, 651, 655. [↑](#footnote-ref-32)
33. *Wewer,* ZRP 2016, 23, 25. [↑](#footnote-ref-33)
34. <http://www.sueddeutsche.de/politik/neuer-us-praesident-wie-twitter-praesident-trump-themen-setzt-1.3281817> (zuletzt abgerufen am: 18.01.2018). [↑](#footnote-ref-34)
35. <http://www.sueddeutsche.de/politik/neuer-us-praesident-wie-trumps-team-fake-news-streut-1.3283617> (zuletzt abgerufen am: 18.01.2018). [↑](#footnote-ref-35)