

Zensur und Spitzel: Europa verspielt seine Zukunft im Internet

Deutsche Wirtschafts Nachrichten, Ronald Barazon | Veröffentlicht: 01.07.17 22:58 Uhr

Der Staat kann als „Großer Bruder“ mit Trojaner-Viren alle Computer angreifen. Aber Unternehmen, die Daten verwenden, werden kriminalisiert. Deutschland verspielt seine digitale Zukunft.



Heiko Maas, Sigmar Gabriel, Thomas de Maiziere und Bundeskanzlerin Angela Merkel am 07.09.2016 in Berlin im Bundestag mit ihren Smartphones. (Foto: dpa)

Eine „Strafrechtsreform“ hat den Überwachungsstaat ermöglicht

Am Freitag, den 30. Juni 2017, hat der Bundestag das „Netzwerkdurchsetzungsgesetz“ beschlossen, mit dem die sozialen Netzwerke an die Kandare des Staates genommen werden sollen. Die Begründung soll in der Öffentlichkeit für Zustimmung sorgen: Facebook und Co müssen Hassbotschaften und Mitteilungen, die Straftaten betreffen, prompt aus dem Netz entfernen. Sonst drohen heftige Strafen. Damit müssten doch die Bürger und Wähler einverstanden sein, meint man offenbar in der Bundesregierung.

Das Gesetz von Freitag ist aber im Zusammenhang mit einem Beschluss des Bundestages acht Tage zuvor zu sehen. Am 22. Juni wurde möglichst unauffällig im Rahmen eines Pakets an Novellierungen in mehreren Gesetzen die Anwendung des „Staatstrojaners“ legalisiert. Man kann von einer kleinen „Strafrechtsreform“ durch die Hintertüre sprechen: Der Staat kann künftig in ausnahmslos jeden Computer einen elektronischen Spion einschleusen, ohne die Betroffenen zu informieren. Damit wurde der Weg zum umfassenden Überwachungsstaat frei gemacht. Selbstverständlich gibt es die obligaten Schutzbehauptungen, wonach nur bei begründetem Verdacht auf Straftaten Polizei, Justiz und Finanz in die Computer eindringen können. Selbstverständlich werden die Maßnahmen nur auf rechtsstaatlicher Basis erfolgen. Allerdings gerät ein Unternehmen sehr leicht mit dem Gesetz in Konflikt: Die praxisfernen Regeln bei der Versendung von E-Mails sind kaum einzuhalten.

Jede Internet-Plattform ist durch die Gesetze bedroht.

Unter diesen Umständen ist die Feststellung, dass das neue „Netzwerkdurchsetzungsgesetz“ nicht E-Mail-Anbieter, Messenger, journalistische Angebote oder Karriereplattformen betreffen würde, nicht sehr überzeugend. Die Betonung, es gehe „nur“ um soziale Netzwerke mit „mindestens zwei Millionen registrierten Nutzern in Deutschland“, vermag auch nicht zu beruhigen: Im Gesetz sind die sozialen Netze nicht genannt, es gibt keine Liste der betroffenen Organisationen. Somit kann jede Internet-Plattform als soziales Netzwerk im Sinne des Gesetzes eingestuft und entsprechend Gegenstand von staatlichen Maßnahmen sein. Auch die Mindestverbreitung ist kein Schutz für die zahllosen anderen Plattformen im Netz: Da genügt ein Verdacht einer Behörde, um die Überwachungsmaschinerie in Gang zu setzen.

Die vergangenen Tage brachten also den vorläufigen Höhepunkt der Welle von Einschränkungen der Menschenrechte. Für den Start sorgte ursprünglich der Terrorismus: Nachdem Terrorattacken nur in Form von Meuchelmorden erfolgen, konnte man noch für eine stärkere Überwachung zum Schutz der Bevölkerung argumentieren. Von allem Anfang an war aber vor einem Missbrauch zu warnen. Mittlerweile wird mit Hinweisen auf den Terrorismus und nun auf die Verleumdungen und Falschmeldungen in den sozialen Netzwerken der gläserne Bürger geschaffen und der Staat zum „Großen Bruder“ Orwellscher Prägung gemacht.

Staatstrojaner sind in ganz Europa auf dem Vormarsch

Das Thema Staatstrojaner ist nicht nur in Deutschland aktuell. In Frankreich findet bereits seit längerem eine facettenreiche Diskussion statt: In einer Phase machte sich vergangenes Jahr der Senat für die Anwendung stark, die damalige Regierung war aber für eine stärkere Einschränkung. In Österreich musste der Justizminister einen entsprechenden Entwurf im vergangenen Jahr zurückziehen, das Thema wird derzeit nicht heftig diskutiert.

Die Problematik der umfangreichen Rechte staatlicher Stellen zeigt sich an einer Bestimmung, die in Österreich die Bekämpfung von „Staatsfeinden“ ermöglicht. Ausgelöst wurde diese Maßnahme durch eine Gruppe von Staatsverweigerern, die die Gesetze nicht achten und sogar in eigenen Gerichten Verfahren und Verurteilungen gegen Vertreter des Staates organisieren wollten. Der neue Paragraph beantwortet aber nicht die Frage, wann ist eine kritische Aktivität „staatsfeindlich“, wo ist die Grenze zwischen einer legitimen Protestbewegung oder einer kritischen Berichterstattung und einer „staatsfeindlichen“ Aktion zu ziehen.

Die EU-Verordnung befreit die Staaten vom Datenschutz

Nachdem die EU die Grundrechte als festen Bestandteil ihres Rechtsgutes sieht, könnte man meinen, die Vorgehensweise insbesondere des deutschen Bundestags in den letzten Tagen würde gegen EU-Recht verstoßen. Das ist nicht der Fall.

Hier sei aus der „Datenschutz-Grundverordnung“ vom April 2016 zitiert, die ab Mai 2018 in der gesamten EU gilt:

Artikel 1, Ziffer 2: (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

Und einige Zeilen weiter heißt es:

Artikel 2, Ziffer 2, lit. d: Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

Somit eröffnet das EU-Recht einen Freibrief für die Errichtung des Überwachungsstaats.

Die EU-Verordnung macht ein modernes Marketing unmöglich

Dieselbe Verordnung macht aber die Verwendung von Daten für die Unternehmen schwer bis unmöglich, wodurch sich eine extreme Bremse für die europäische Wirtschaft ergibt: Personenbezogene Daten dürfen von einem Unternehmen nur verwendet werden, wenn vorweg die Betroffenen ihre Einwilligung geben. Dieser Grundsatz bestand schon bisher, wird aber durch die neue Verordnung verschärft. Bei Verletzungen sind Strafen bis zu 20 Mio. Euro vorgesehen. Außerdem muss in jedem Mitgliedstaat eine Aufsichtsbehörde tätig sein, die für die Durchsetzung der Bestimmungen sorgt.

Mit dieser Regelung wird die Werbung über den Versand von E-Mails drastisch eingeschränkt. Es erfolgt auch eine Verletzung des Gleichheitsprinzips: Man kann beliebig Briefe an Personen senden, aber keine E-Mails. Es wird noch grotesker: Juristen empfehlen, Briefe mit der Bitte um die Genehmigung zur Zusendung von E-Mails zu schreiben. Niemand fragt, ob man in einer Zeitung ein Inserat oder auf der Straße ein Plakat lesen will. Die Möglichkeit, sich gegen die Flut von Prospekten zu wehren, ist bescheiden. Aber der E-Mail-Versand wird kriminalisiert.

Ausgelöst wurde diese Bestimmung durch die Flut an obskuren Mails von dubiosen Absendern. Nur diese Absender werden nicht erreicht, diese lassen sich von der EU-Verordnung und den nationalen Datenschutzgesetzen beeindrucken, da sie von nicht auffindbaren Servern aus arbeiten. Belastet werden die regulär tätigen Unternehmen, die eine jedermann zugängliche Adresse haben: Diesen nimmt man ein modernes Instrument der Werbung, das vielen, vor allem kleineren Unternehmen enorme Zukunftschancen eröffnet. In der Praxis zeigt sich, dass auch die großen Firmen diesen Weg zu den Kunden brauchen, doch wird dieser Umstand noch nicht in allen Vorständen erkannt. Mancher mag die Illusion pflegen, dass die Bekämpfung der E-Mail-Werbung nur den Kleinen schade.

US-Regelung behindert trotz Strafen die Praxis nicht

Dass die zahllosen, anonymen Mails lästig sind, wird wohl niemand bestreiten. Statt – wieder einmal – mit einer Missbrauchsbekämpfung die anvisierten Täter nicht zu treffen, aber der Wirtschaft zu schaden, würde sich ein Blick in die Praxis in den USA empfehlen.

Auch in den USA gibt es eine gesetzliche Regelung, den so genannten „CAN-SPAM-Act“. Auch in den USA gibt es Strafen. Für jedes einzelne E-Mail, bei dem die Regeln verletzt werden, kann die Strafe bis zu 40.654 Dollar betragen. Allerdings bekämpft man nicht praxisfremd den Versand von E-Mails. Die einzuhaltenden Regeln sind nachvollziehbar:

- Es muss klar erkennbar sein, wer das E-Mail versendet: Der Absender muss über die E-Mail-Adresse, über die domain identifizierbar sein.
- Die Betreff-Zeile muss den Inhalt klar benennen.
- Das Mail muss als Werbung bezeichnet werden.
- Den Empfängern sind der genaue Firmen-Name und die Post-Adresse bekannt zu geben.
- Die Empfänger müssen problemlos in der Lage sein, eine weitere Zusendung abzulehnen. Die Streichung muss spätestens 30 Tage nach der entsprechenden Mitteilung erfolgen. Eine Verletzung dieses Grundsatzes ist die entscheidende Grundlage für eine Strafe.

Mit diesen Auflagen sollte wohl jedes Unternehmen problemlos arbeiten können.

Die Europäer sollten sich an diese Vorgaben halten und entsprechende Bestimmungen schaffen. Besonders sinnvoll ist die Verpflichtung, nicht nur die E-Mail-Adresse und die Homepage, sondern auch den Firmennamen und die Adresse bekannt zu geben. Man könnte diese Vorschriften auch ergänzen und verlangen, dass jeder Absender eine fixe IP-Adresse haben muss, die leicht nachvollziehbar zu sein hat. Mails von Absendern, die diese Auflagen nicht erfüllen, müssten bereits von den Betreibern der Server automatisch gelöscht werden.

Es gibt also ausreichend Möglichkeiten für eine sinnvolle Regulierung, die aber nicht den europäischen Unternehmen die Nutzung eines entscheidenden Instruments des modernen Marketings erschwert bis unmöglich macht.

Die Bekämpfung der Marktbeherrschung ist wie trommeln wider den Erfolg der anderen

Der Schutz der Privatsphäre vor dem Staat und die Möglichkeit, sich auf dem Markt frei zu bewegen, sind die für die meisten Bürger entscheidenden Themen im Zusammenhang mit dem Datenschutz. Die aktuelle Entwicklung zeigt den Staat, der zum „Großen Bruder“ wird, und ein EU-Regelwerk, das die Wirtschaft behindert.

Umfangreich diskutiert werden allerdings andere Fragen, die zwar die Politik und die Wissenschaft beschäftigen, aber das breite Publikum weniger berühren.

- Für Aufregung sorgt der Umstand, dass die Geheimdienste sich Zugriff zu jedem Computer verschaffen können. Allerdings sind diese Aktivitäten schwerer zu kritisieren, wenn das Parlament

Gesetze beschließt, die den Behörden die Platzierung von Trojaner-Viren erlaubt. Bei den Geheimdiensten mag man noch hoffen, dass sie tatsächlich in erster Linie Terroristen und andere Feinde ausspionieren. Die Bürokratien können die einfachen Bürger unter Druck setzen.

- Ärgerlich ist der Zugang, der Google und anderen großen Internet-Firmen offen steht. Aus den Suchanfragen und den Texten der E-Mails lassen sich leicht die Konsumgewohnheiten und Interessen der Nutzer ablesen. In der Folge aufgerufene Internet-Seiten werden dann unschwer mit entsprechenden Werbungen bestückt. Diese Praxis ist durch die Behörden schwer zu unterbinden.
- Die vor wenigen Tagen von der EU-Kommission gegen Google ausgesprochene Strafe von 2,42 Mrd. Euro hat zwar europaweit durchaus Applaus geerntet, dürfte aber noch viele Jahre den Europäischen Gerichtshof beschäftigen. Die Begründung lautet: Das Unternehmen habe seine marktbeherrschende Stellung bei der Shopping-Suche zugunsten nahestehender Betriebe missbraucht. Der Vorwurf der Marktbeherrschung ist immer problematisch, da man einer Firma den Erfolg ankreidet. Vor allem hat die Aktion einen besonders schalen Beigeschmack, da kein europäisches Unternehmen eine vergleichbare Suchmaschine geschaffen hat. Die kritisierten Querverbindungen sind durch Unternehmenstrennungen korrigierbar.
- Zur Orientierung: Das Standard Oil Konglomerat von Rockefeller wurde 1890 aufgrund des Sherman Antitrust Act wegen der „Marktbeherrschung“ in viele Firmen (Esso, Mobil und 32 andere) aufgeteilt, die alle weiterhin Rockefeller und seinen Partnern gehört haben. Viele wurden Jahrzehnte später wieder zu ExxonMobil vereinigt.
- Zur Beruhigung der europäischen Politik und der Behörden beschließen die großen Internet-Unternehmen laufend Wohlverhaltensregeln und verbessern die so genannte „Corporate Governance“. Tatsächlich wird sich aber wenig ändern, weil in den USA keine nennenswerte Datenschutz-Gesetzgebung existiert. Die Regelungen beschränken sich darauf, den Geheimdiensten eine größtmögliche Freiheit beim Zugang zu den gewünschten Daten zu sichern. Wie Google auf das Kaufverhalten der Nutzer einwirkt, interessiert die Politik nicht.
- Die US-amerikanischen Firmen sollten beim Umgang mit Daten europäischer Bürger zur Beachtung der EU-Regeln angehalten werden. Dafür wurde 2000 die Safe-Harbor-Vereinbarung geschlossen, die 2016 vom EU-US-Privacy-Shield abgelöst wurde. Die europäischen Kritiker bezweifeln die Wirkung, Präsident Donald Trump hat bereits im Jänner eine Einschränkung per Dekret verfügt, das EU-Parlament hat im April in einer Resolution das Funktionieren des Shield in Frage gestellt.

Das groteske Ergebnis der aktuellen Datenschutz-Politik in Europa: Die EU wird Google, Amazon, Facebook, Apple nicht in die Knie zwingen. Aber ein mittelständisches Unternehmen darf potenziellen Kunden keine Werbe-Mails senden. Und die Geheimdienste agieren nach Belieben und Gutdünken.

Ronald Barazon war viele Jahre Chefredakteur der Salzburger Nachrichten. Er ist einer der angesehensten Wirtschaftsjournalisten in Europa und heute Chefredakteur der Zeitschrift „Der Volkswirt“ sowie Moderator beim ORF.