

Prüfung intra- und transkulturelle Kommunikation

Termin: September 2013

Der Ausgangstext ist ein Artikel von Ingrid Brodnig, der im *Falter* 28/13 erschienen ist. (Quelle: <http://www.falter.at/falter/2013/07/09/1-000-000-000-000-daten/>)

Bearbeiten Sie die folgenden Aufträge auf Basis der Informationen der Ausgangstexte. Achten Sie auf eine adäquate Textgestaltung in Hinblick auf Textsorte, Zielpublikum, Verwendungszweck usw. der Zieltexte.

Auftrag 1 – Textproduktion A-Sprache/-Kultur (ca. 250 Wörter):

Eine Datenschutzorganisation veranstaltet Projektstage an höheren Schulen Ihrer A-Sprache/-Kultur mit dem Ziel, Schüler_innen für das Thema Datensicherheit zu sensibilisieren. Formulieren Sie einen Brief, der an die lokalen Schulbehörden versendet wird, in dem auf die Problematik hingewiesen und die Durchführung einer solchen Veranstaltung zu diesem Thema angeboten wird.

Auftrag 2 – Textproduktion B-Sprache/-Kultur (ca. 250 Wörter):

Auf der Webpage des internationalen Forschungsprojekts „Datenschutz im digitalen Zeitalter: Positionen internationaler IT-Expert_innen“ wird Ingrid Brodnigs Meinung zusammengefasst dargestellt. Verfassen Sie diese Zusammenfassung, deren Zielpublikum hauptsächlich Wissenschaftler_innen Ihrer B-Sprache/-Kultur sind.

Auftrag 3 – Textproduktion C-Sprache/-Kultur (ca. 250 Wörter):

Eine Informationssendung eines Radiosenders eines Landes Ihrer C-Sprache/-Kultur beschäftigt sich mit den Herausforderungen für die Wirtschafts- und Demokratiepoltik, wie man die Privatsphäre der Bürger_innen besser schützen kann. Verfassen Sie auf Basis der Informationen im Ausgangstext einen einleitenden Text für diese Radiosendung, der vor den dann folgenden Expert_innen-Interviews von der/m Radiosprecher_in vorgetragen wird.

Ausgangstext (797 Wörter):

1.000.000.000.000 Daten

Die USA späht die Internetbevölkerung aus und viele Staaten machen eifrig mit. Ist der Kampf um die Privatsphäre schon verloren?

Die Lage ist trist. So trist, dass sich der deutsche Innenminister Hans-Peter Friedrich vergangene Woche zu einem extremen Ratschlag veranlasst fühlte. Er empfahl quasi ein Internet ohne Google, Facebook oder Twitter. "Wer auch immer fürchtet, dass seine Kommunikation irgendwie abgefangen wird", sagte der CSU-Minister, "soll keine Dienste nutzen, die über amerikanische Server laufen."

Ein gut gemeinter Rat, doch der Großteil unseres Netzes wird von amerikanischen Firmen dominiert, vom Suchmaschinenriesen Google bis zum Computerhersteller Apple. Wer eine Gmail-Adresse besitzt, mit seinen Freunden über Facebook kommuniziert oder ein iPhone besitzt, kann auf amerikanische Dienste nicht verzichten.

Tag für Tag ereilen uns neue Schreckensmeldungen zum Abhörprogramm Prism. Der Guardian berichtet, die USA hätten den umfassendsten Überwachungsapparat seit der Erfindung des Internets aufgebaut, sie würden Bürger außerhalb der USA ausspähen. [...] Wie groß der Datenspeicher der USA sein könnte, zeigt ein internes E-Mail, das der Guardian veröffentlichte. Darin gratuliert sich angeblich eine Untereinheit der NSA selbst. Man feierte "its One Trillionth metadata record". Zu Deutsch: die einebillionste Aufzeichnung von Verbindungsdaten, also wer wann mit wem Kontakt hat.

Eine Billion, das ist ein Einer mit zwölf Nullen dran, und die Zahl stellt womöglich nur einen Bruchteil der Überwachung dar. Wenn all das stimmt, ist die Chance nicht einmal so gering, dass man in den riesigen Datenspeichern Amerikas bereits irgendwo vermerkt wurde. Aber ist der Kampf um die Privatheit tatsächlich schon verloren?

Die Schlacht verläuft an drei Fronten: einer technischen, einer wirtschaftlichen und einer rechtlichen. Rein technisch gäbe es Möglichkeiten, zumindest nicht ganz so transparent zu sein. Jeder Internetuser kann Software herunterladen, um seine E-Mails zu verschlüsseln, um sein Surfverhalten zu verschleiern oder Anhänge in Mails ohne Zugangscode unlesbar zu machen. Diese Programme heißen PGP (Pretty Good Privacy), TOR oder TrueCrypt. Laut Whistleblower Snowden kann nicht einmal die NSA solche verschlüsselten Nachrichten lesen. Technik ist also ein guter Start.

Jedoch verschlüsselt kaum wer E-Mails und nur wenige nutzen Anonymisierungsdienste wie TOR. Das Problem ist: Je sicherer ein System wird, desto umständlicher und unbequemer muss es auch werden. Es dauert mitunter länger, eine Seite aufzurufen, und der Empfänger der Nachricht muss auch Verschlüsselungstechnologie nutzen, sonst funktioniert das Ganze nicht. Auch gibt es keine Möglichkeit, verborgen via Facebook oder iPhone zu kommunizieren. Kurz gesagt: Software ist eine Lösung, aber eine komplizierte.

Wenn Europa langfristig vor amerikanischen Überwachern sicher sein will, braucht es auch Datensouveränität. Ein Weg dorthin ist die Wirtschaft. Das meint zumindest der österreichische EU-Abgeordnete Josef Weidenholzer (SPÖ). "Hier hätten europäische Unternehmen sogar einen Wettbewerbsvorteil, den starken Datenschutz." Das würden vielleicht auch Konsument/innen in Lateinamerika, Asien oder dem arabischen Raum schätzen. Zunehmend entdeckt auch die EU dieses Thema und versucht langsam, den digitalen Markt zu harmonisieren. So sollen große europäische Webdienste entstehen, die mit den amerikanischen Riesen konkurrieren können.

All das funktioniert nur, wenn Europa tatsächlich den eigenen Datenschutz ernst nimmt. Derzeit scheint das nicht so. Als das Überwachungsprogramm Prism aufflog, hielten sich einige EU-Staaten bedeckt. Das liegt womöglich auch daran, dass sie ein doppeltes Spiel treiben. Öffentlich plädiert die Politik für den Schutz der Privatsphäre, inoffiziell kooperieren ihre Geheimdienste mit den Amerikaner/innen oder betreiben sogar selbst den Lauschangriff aufs Internet. Laut Guardian hat Großbritannien ein ähnliches Programm, bei dem sich der britische Nachrichtendienst ebenfalls Zugang zu Netzwirkabeln verschafft haben soll und angeblich riesige Datenmengen auswertet. In Frankreich berichtete Le Monde erst vergangene Woche, dass dort sowohl Telefonate als auch die Webkommunikation überwacht und Verbindungsdaten auf riesigen Servern gespeichert würden. Auch fehle hier eine "ernsthafte Kontrolle". [...]

Die Demokratie – und die rechtlichen Grundlagen, auf denen sie basiert – ist also wohl die wichtigste Front im Kampf um die Privatheit. Im Kern geht es um zwei Fragen: Wie unkontrolliert dürfen Geheimdienste vorgehen? Und was können andere Staaten gegen derartige Spionage tun? Europa wirkt ohnmächtig, ist es aber gar nicht. Derzeit wird im EU-Parlament die neue Datenschutzverordnung ausverhandelt, ein zentrales Dokument zum Schutz vor allzu großer Neugier von Staaten oder Firmen.

Die neue Verordnung könnte dazu führen, dass US-Firmen nicht länger europäische Grundrechte ignorieren können, sonst drohen hohe Strafzahlungen. Verstößt dann ein US-Unternehmen wie Facebook dagegen, könnten hohe Strafen folgen. [...]

Die Verordnung ist nur eines von vielen Beispielen, wie Europa reagieren kann. Ebenfalls ließen sich Handelsabkommen aufkündigen oder laufende Verhandlungen mit den USA stoppen. Sehr unklar ist jedoch, ob sich Europa dazu durchringen wird. Derzeit scheint sich kein Staat offen mit Amerika anlegen zu wollen.

Die Lage ist trist und sie wird wohl noch trister. Machtlos gegenüber den Geheimdiensten wären Politik und Bevölkerung aber nicht. Von harten Gesetzen über Verschlüsselung bis hin zu alternativen Web-Angeboten – Europa und die einzelnen Staaten könnten sehr wohl etwas tun, sofern die Bevölkerung das einfordert. Verloren ist der Kampf um die Privatheit nämlich dann, wenn sich keiner mehr dafür einsetzt.