Das Netz fängt nicht auf, sondern ein – Über Bequemlichkeit und die Erosion der Privatsphäre

Hans Metsch

Zusammenfassung: Man muss Edward Snowden schon alleine dafür dankbar sein, dass er uns in unserem Schlaf der Gerechten relativ nachhaltig gestört und eine Diskussion entfacht hat, welche die normale Halbwertszeit der Themen des politischen und gesellschaftlichen Alltags inzwischen deutlich überschreitet. E-Mail und Internet sind extrem hilfreich im privaten und beruflichen Alltag – und dazu noch wunderbar bequem. Wir werden verführt und angeleitet, unsere Privatsphäre und die unserer Patienten dafür aufzugeben. Und wir merken meist nicht einmal, dass und wie wir das tun. Der Artikel gibt einen kurzen Überblick sowie einige praktische Empfehlungen. Er ist in keiner Weise vollständig, sondern möchte anregen, dem Thema gegenüber wach zu bleiben, und plädiert für eine „intelligente Beweglichkeit" im WWW-Dschungel.

Das World Wide Web basiert(e) auf dem wunderbaren Gedanken, dass jeder gibt, was er kann, und nimmt, was er braucht. 2011 ist es 20 Jahre alt geworden und nichts hat jemals unser Leben in so kurzer Zeit so drastisch verändert. Ein Großteil unserer privaten, gesellschaftlichen und wirtschaftlichen Kommunikationsprozesse ist ohne WWW und E-Mail nicht mehr vorstellbar (die E-Mail und das Internet als solches gibt es schon etwas länger; Letzteres entstand aus militärischen und Universitätsnetzwerken in den USA; in Frankreich gab es seit den 1980er-Jahren *Minitel*, das ebenfalls eine Art Vorläufer war; das WWW selbst wurde von Tim Berners-Lee am CERN[1] in Genf entwickelt). Am Anfang war noch einiges an technischem Verständnis nötig, um an den informationellen Segnungen teilzuhaben oder gar selbst dazu beizutragen. Spätestens mit dem sogenannten „Web2.0", dem Mitmach-Internet, änderte sich das jedoch völlig. Heute gibt es für alles vorgefertigte Lösungen, eigene Programmierkenntnisse sind nicht mehr nötig und jeder kann ganz spontan und ohne Vorkenntnisse aktiv und passiv teilnehmen. Zur Spontanität kommt die Bequemlichkeit, und diese beiden haben es inzwischen mühelos geschafft, dem Nutzer und der Nutzerin[2] ein kuscheliges, quasi-familiäres Gefühl zu vermitteln, das die Preisgabe der Privatsphäre fast selbstverständlich werden lässt. So „posten" Kinder und Jugendliche auf Facebook bedenkenlos intime Texte und Fotos („das können ja nur meine Freunde sehen"), und in manchen Foren lassen auch Erwachsene sozusagen „die Hosen runter" und stellen Beiträge ein, die sie nie und nimmer in dieser Form zu Papier bringen und absenden würden. Das betrifft fast alle, auch Akademiker. Ich bin manchmal in Ärzteforen unterwegs und staune wirklich über diese Unbekümmertheit. Der Gedanke scheint zu sein, dass man sich dort ja anmelden müsse und daher „unter sich" sei.

Die Wahrheit ist, dass alles, was im Netz steht, eine Veröffentlichung ist. Und diese Veröffentlichung ist permanent. Jedenfalls meistens. Denn das Internet vergisst nichts. Es hat ein Gedächtnis, z. B. *www.archive.org*. Und die Wahrheit ist auch, dass man sich nicht einbilden darf, man sei dort anonym, nur weil man ein Pseudonym verwendet. Die „Fingerabdrücke", die ein Computer im Internet zurücklässt, machen eindeutige Rückschlüsse leicht möglich. Wenn Sie Lust haben, probieren Sie aus, wie viele Rechner bzw. Browser genau dieselben Identifizierungs-Bits senden, wie der Ihrige: Gehen Sie auf *https://panopticlick.eff.org* und drücken Sie den roten Knopf. Schon 20 Bits, d. h. eine Folge von zwanzig Nullen und Einsen, reichen aus, um über eine Million Rechner eindeutig zu unterscheiden. Und weil die sogenannten IP-Nummern, die allen am Internet teilnehmenden Rechnern zugeordnet sind, regional vergeben werden, kann *jede* Website im Prinzip leicht ermitteln, wo Sie ungefähr mit Ihrem Rechner sitzen.

„Big Data" – Was wird aus der Schweigepflicht?

Das Netz ist nicht nur ein Netzwerk, sondern auch ein Schleppnetz. Seit die Speicherkapazitäten und die Rechenleistung so angewachsen sind, dass sie der umfassenden Datensammlung keine Hindernisse mehr in den Weg legen, wird diese auch betrieben. Die großen Internetkonzerne wie Google, Facebook, Amazon usw. sammeln alles, was sie kriegen können. Und zwar nicht nur, wenn man ihre Seiten besucht, sondern bei allen Seiten, die auf sie verweisen. Jede Seite, auf der das „Gefällt mir" auftaucht, verbindet den Nutzer sofort und

1 Europäische Organisation für Kernforschung (Conseil Européen pour la Recherche Nucléaire, CERN).

2 Im Folgenden werden nicht immer beide Geschlechtsformen genannt, selbstverständlich sind jedoch Frauen und Männer gleichermaßen gemeint.

automatisch mit Facebook, wo die Daten des Rechners gesammelt werden.

Facebook-Teilnehmer sind nämlich, wie es Richard Stallman formulierte, keine Kunden, sondern sie sind die Ware.[3] Sogenannte *„tracker"* d. h. kleine Einschübe im Code der allermeisten kommerziellen Websites, die den Rechner bei irgendeiner Datensammelstelle melden, arbeiten, ohne dass der normale Anwender das Geringste davon merkt.

Neuerdings gibt es eine weitere bequeme Möglichkeit, seine Daten zu verwalten und für alle Computer und Smartphones synchron verfügbar zu haben: die Cloud. Cloud-Computing heißt, seine Daten auf einen Server im Netz auszulagern und über das Internet aufzurufen, anstatt sie auf der eigenen Festplatte zu speichern. Alle großen Internet- und Telekommunikationskonzerne bieten diese Möglichkeit inzwischen an. Ich bin mir nicht sicher, ob unbefugte Zugriffe auf die eigene Festplatte leichter durchzuführen sind als auf einen Cloud-Server. Sicher scheint mir allerdings, dass Daten auf einem fremden Server der eigenen Kontrolle zumindest teilweise entzogen sind und dass deshalb bei Patientendaten eine solche Auslagerung ohne ausdrückliche Zustimmung der Patienten einen Bruch der Schweigepflicht darstellen würde.

Die Schweigepflicht unterliegt überhaupt einer stetigen Erosion. Ein Beispiel dafür ist die inzwischen übliche *Caller-ID*, d. h. die Übermittlung der anrufenden Nummer beim Angerufenen. Viele Leute gehen nicht mehr ans Telefon, wenn „Unbekannt" anruft. Sie tragen damit – genau wie Ärzte und Psychotherapeuten, die die Rufnummerübermittlung nicht abgeschaltet haben – dazu bei, die Schweigepflicht auszuhöhlen, denn es kommt nicht selten vor, dass Psychotherapeuten und bestimmte Ärzte vertraulich und ohne Kenntnis der Familienangehörigen kontaktiert werden und bei einem Rückruf dann über die übermittelte Telefonnummer leicht zu identifizieren sind. Man mag einwenden, dass das im Zeitalter des persönlichen Handys eine kleine Gefahr ist, aber der bequeme und sorglose Umgang mit diesen Geräten macht die Überprüfung der dort getätigten und empfangenen Kommunikationen in der Regel zu einem Kinderspiel. Bei Festnetzanschlüssen von nicht alleinlebenden Erwachsenen besteht eine hohe Gefahr der Schweigepflichtsverletzung, die aber mittlerweile von Psychotherapeuten wie Patienten klaglos hingenommen wird.

Immer wenn patientenbezogene Daten in irgendeiner Form durchs Netz laufen, sind sie im Prinzip kompromittiert. Man muss sich dann auf die Verschlüsselung verlassen, die zwar für Feld-, Wald- und Wiesen-Hacker ein Hindernis darstellen dürfte, nicht aber für Profis, wie sie z. B. in den Geheimdiensten und an anderen Stellen sitzen. Ich habe den Eindruck, dass die im Juni 2013 durch die Enthüllungen Edward Snowdens bekannt gewordenen Ausspähpraktiken der Geheimdienste für viele Menschen tatsächlich eine Überraschung waren, die das heimelige Internet-Gefühl wenigstens vorübergehend erschüttert haben.

Geheimdienste heißen aber Geheimdienste, weil ihre Operationen geheim und illegal sind. Es gibt inzwischen in den westlichen Demokratien zwei sehr mächtige Instanzen, die keinerlei demokratischer Kontrolle mehr unterliegen: die Finanzmärkte und die Geheimdienste. Politiker, die erwarten, im parlamentarischen Aufsichtsausschuss die Wahrheit über die Tätigkeit der Geheimdienste zu erfahren, sind bestenfalls naiv. Ein Dienst wie die NSA verfügt über eine unvorstellbare Computer-Power und auch über die Spezialisten, die sie bedienen können. Weil die meisten großen Computerkonzerne amerikanisch sind und selbst weltweit Daten sammeln, wird die NSA mit ziemlicher Sicherheit ihre Leute an allen Schaltstellen sitzen haben, auch global an den Backbones und den Internet-Knoten, über die der Datenverkehr läuft. Die Datenauswertung geschieht algorithmisch in den Rechenzentren, also mit einer nahezu grenzenlosen Kapazität und Geschwindigkeit. Vorbei sind die Zeiten der „Firma Horch und Guck", wo irgendwelche Schlapphüte ihre durch Observation gewonnenen Erkenntnisse auf Schreibmaschinen tippten. Jedoch ist dieses Bild noch in den Köpfen, was effektiv verhindert, sich das Ausmaß und die Genauigkeit der Spionage heutzutage überhaupt vorzustellen. Man macht sich ja schon kaum noch Gedanken über die Tatsache, dass viele Smartphones nicht wirklich abgeschaltet werden können, ohne sie zu zerstören, und dass sie, solange sie überhaupt noch funktionieren, Signale aussenden, die ihre Ortung auf wenige Meter genau möglich machen.

Was diese Aktivitäten angeht, ist die Schlacht um die Datensicherheit – und in erheblichem Umfang auch die Privatsphäre – für die Bürger endgültig verloren. Trotzdem kann und sollte man natürlich auf niedrigerer Ebene noch etwas dafür tun, auch wenn das leider deutlich auf Kosten der Bequemlichkeit geht. Dazu in aller Kürze ein paar Empfehlungen, die natürlich nicht vollständig sein können und je nach Ihrem eigenen Kenntnisstand bzw. den Besonderheiten Ihres Rechners vielleicht durch eine Beratung beim IT-Spezialisten Ihres Vertrauens ergänzt werden sollten.

Was tun?

Die sicherste Lösung

Sie können für alle Praxisdaten einen Rechner verwenden, der keine Außenverbindung hat. Außer der verschlüsselten Abrechnungsdatei werden von dort keinerlei Patientendaten auf andere Geräte übertragen, vor allem nicht auf Smartphones oder Tablets.

Updates des Praxisprogramms, Abrechnungsdateien etc. können Sie für den Transport zwischen den Geräten auf Memory-Sticks kopieren und die Abrechnung nach dem Versenden wieder löschen.

Jetzt zu den etwas weniger sicheren, aber noch immer gangbaren Maßnahmen

Rechner-Einstellungen
Für Internet und E-Mail können Sie ein eigenes Nutzerkonto verwenden, das keine sogenannten Admin-Rechte hat, sodass unbefugte Zugriffe auf Ihren

3 Vgl. www.heise.de/tp/artikel/35/35152/1.html

Rechner erschwert werden. Erlauben Sie nicht, dass der Rechner Passwörter speichert. Verwahren Sie Ihre Passwörter an einem sicheren Ort.

Passwörter
Verwenden Sie sichere Passwörter. Die Stärke von Passwörtern können Sie im Internet prüfen, beispielsweise unter *www.wiesicheristmeinpasswort.de.* Es ist ratsam, verschiedene Passwörter für verschiedene Anwendungen zu benutzen und sie immer mal wieder zu ändern.

W-LAN
Ein offenes W-LAN (WiFi) ohne Verschlüsselung und Passwort ist eine wirklich schlechte Idee.

Firewall
Die meisten DSL-Router haben eine eingebaute Firewall, die dazu dient, bestimmte Internetverbindungen zu überwachen und ggf. zu unterbinden. Man sollte jedoch zusätzlich eine weitere auf dem Rechner haben. Für Windows gibt es z. B. Zone-Alarm (*www.zonealarm.de*), und für Apple Macintosh gibt es Little Snitch (*www.obdev.at/littlesnitch*). Damit kann man Internet-Verbindungen des Rechners überwachen und selektiv regulieren.

E-Mail
E-Mails sind kein sicheres Medium. Ihre Verschlüsselung ist möglich, z. B. mit Truecrypt (*www.truecrypt.org*), aber nicht ganz einfach, weil Absender und Empfänger denselben Schlüssel benötigen. Für die Kontaktaufnahme des Psychotherapeuten an den Patienten sollte eine Genehmigung vorliegen, die aber implizit besteht, wenn der Patient selbst den Kontakt initiiert. Machen Sie bei Sendungen an mehrere Empfänger *unbedingt* Gebrauch von der Versendeart BCC (*Blind Carbon Copy*), bei der die Empfänger in den Kopfzeilen der E-Mail nicht angezeigt werden. Ellenlange offene Empfängerlisten entspringen oft einem durchaus freundlichen Transparenzgedanken, sind aber „fette Beute" für Spammer (falls ein Virus oder Trojaner sie – oder Ihr Outlook-Adressbuch, das Sie ebenfalls leer lassen sollten – ausliest). Antworten Sie nie auf Spam, auch nicht, um sich vom Verteiler abzumelden. Damit haben Sie nämlich „gestanden", dass E-Mails an diese Adresse gelesen werden und sie kann (und wird) dann weiterverkauft werden.

Browser-Einstellungen
(am Beispiel Firefox; genaue Anleitung gibt es unter *www.support.mozilla.org/de/products/firefox*):

- Blockieren Sie Pop-up-Fenster.
- Verbieten Sie Tracking (fraglich, ob das viel nützt, aber man kann es mal probieren. Ghostery (s. u.) ist besser.)
- Verwenden Sie den Private Browsing Mode oder stellen Sie die Browser-History so ein, dass sie, samt Cache-Speicher, Formularen, Suchbegriffen und evtl. noch aktiven Log-ins beim Schließen von Firefox gelöscht wird. Schließen Sie den Browser dann regelmäßig. Lassen Sie ihn möglichst nicht tagelang im Hintergrund offen.
- Erlauben Sie keine Cookies von Drittseiten. Behalten Sie andere Cookies, bis Firefox geschlossen wird. Sie können bestimmte Ausnahmen definieren, etwa solche, in denen Seiteneinstellungen gespeichert sind, die Sie immer wieder brauchen, beispielsweise Spracheinstellungen bei YouTube usw. Es sei an dieser Stelle vermerkt, dass es inzwischen Cookies gibt, die kaum noch löschbar sind und damit ähnlich wie Trojaner arbeiten. Siehe dazu: *www.heise.de/tp/blogs/6/150231*.
- Verbieten Sie die unauthorisierte Installation von *Add-ons*/Erweiterungen.
- Blockieren Sie gemeldete Angriffs-Seiten oder Fälschungen von Seiten (Firefox verbindet sich automatisch mit einigen Diensten, die diese Informationen bereitstellen.)
- Verbieten Sie auch dem Browser die Speicherung von Passwörtern.
- Lassen Sie den Browser warnen, wenn eine Website Sie automatisch mit einer anderen Website verbinden will (sogenannter *Redirect*).

Browser-Erweiterungen
Für manche Browser gibt es sogenannte Erweiterungen (*Extensions, Add-ons*). Hier sind einige wichtige am Beispiel Firefox aufgeführt:

- *NoScript*: Erlaubt die selektive Abschaltung von Javascript, das auf fast allen Websites verwendet wird. Weil es aber Schadcode enthalten kann, sind Sie auf der sicheren Seite, wenn Sie es generell verbieten und nur bei vertrauenswürdigen Websites einschalten.
- *AdBlock Plus*: Unterbindet selektiv oder global die Werbung auf Websites.
- *Ghostery*: Findet und unterbindet die meisten „tracker" (abonnieren Sie dazu eine entsprechende Liste).
- *HTTPS Everywhere*: Prüft, ob eine verschlüsselte Verbindung (*https*) möglich ist und wählt sie ggf. aus.
- *BetterPrivacy*: Löscht sogenannte Flash-Cookies, die relativ hartnäckig sind und durch die normalen Cookie-Löschungen nicht gefunden werden. Vorsicht: Löscht damit u. U. auch gespeicherte Einstellungen von Computerspielen.

Suchmaschinen

Es gibt sehr gute Alternativen zu Google, z. B. die europäischen Suchmaschinen Ixquick (*www.ixquick.com*) und Startpage (*www.startpage.com*). Beide sammeln keine IP-Nummern; Ixquick bietet einen Proxy-Service (d. h. Ihre Anfrage wird als Anfrage von Ixquick weitergeleitet, sodass Ihre eigenen Rechnerdaten nicht übertragen werden) und Startpage sucht mithilfe der Google-Engine, ohne aber Ihre Daten zu sammeln (*www.startpage.com/deu/protectprivacy.html).*

Soziale Netzwerke

Patiententermine etc. über Facebook (oder ein anderes soziales Netzwerk) auszumachen, ist sehr bedenklich. In sozialen Netzwerken ist nur eines sicher: dass nichts sicher ist.

Bewertungsportale/Foren

Was über uns von anderen ins Internet gestellt wird, ist kaum noch überschaubar. Sich selbst gelegentlich in Suchmaschinen und in Bewertungsportalen aufzurufen, ist weniger eine narzisstische Selbstbespiegelung als eine lästige Pflicht. Bewertungsportale sind eine Schnapsidee, wenn Sie mich fragen. Unter dem Deckmantel der Transparenz und des Wettbewerbs wird dem Betrug (man schreibt seine eigenen Bewertungen von verschiedenen Rechnern aus) und manchmal auch der Verleumdung Tür und Tor geöffnet. Schauen Sie also ab und zu wenigstens in den großen Portalen nach. Einige der größten sind:

- www.weisse-liste.arzt-versichertenbefragung.aok-arztnavi.de
- www.vdek-arztlotse.de
- www.jameda.de
- www.arzt-auskunft.de/de/alles-ueber-die-arzt-auskunft/empfehlungspool.html
- www.docinsider.de

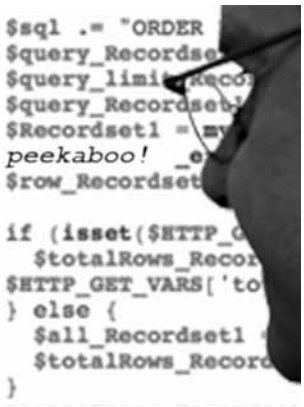
Weitere finden Sie über Suchmaschinen („Arztbewertung"). Nicht in allen ist Psychotherapie aufgeführt.

Hier noch einige Verweise zur weiteren Lektüre

- Ein psychotherapeutischer Kollege hat eine schöne Website zum Thema Schweigepflicht gemacht: *www.schweigepflicht-online.de*
- Laufende Nachrichten zu Sicherheitsthemen gibt es bei: *www.heise.de/security*
- Ausführliche Zusammenfassung der NSA-Affäre ebenfalls bei Heise (Stand: Dezember 2013): *www.heise.de/extras/timeline*
- Rechtssicherheit in der Cloud: *www.e-recht24.de/artikel/blog-foren-web20/7115-rechtssicher-in-der-cloud-ihre-daten-beidropbox-icloud-google-drivea-co.html*
- Ratgeber Cloud-Computing: *www.techfacts.de/ratgeber/cloud-computing-im-detail*
- Zeit-Serie: Mein digitaler Schutzschild: *www.zeit.de/serie/mein-digitaler-schutzschild*
- Leitfaden Schweigepflicht der LPK-BW und der LÄK-BW: *www.lpk-bw.de/archiv/news2011/pdf/110329_leitfaden_schweigepflicht_und_datenschutz.pdf*

Ein persönliches Wort zum Schluss

Ich bin schon ziemlich lange im Internet unterwegs. So lange, dass ich das Wahre, Gute und Schöne des ursprünglichen Gedankens noch erkenne und wertschätze. Deshalb tut es mir leid, hier der Überbringer weitgehend schlechter Nachrichten zu sein, und ich hoffe, dass wir es vielleicht doch noch schaffen, den Nutzen zu mehren und so viel Schaden wie noch möglich abzuwenden. Aber ganz bequem wird es wohl nicht werden.



***Hans Metsch**, Dipl.-Psych., ist niedergelassener Psychologischer Psychotherapeut und Kinder-/Jugendpsychotherapeut, akkreditierter Supervisor für Verhaltenstherapie und Systemische Therapie/Familientherapie, Autor verschiedener Internet-Projekte und seit 2001 Webmaster der Landespsychotherapeutenkammer Baden-Württemberg.*

Dipl.-Psych. Hans Metsch

70839 Gerlingen
praxis@psyon.de

Für die Durchsicht des Manuskripts danke ich Herrn Johny Varsami und Frau Ass. jur. Stephanie Tessmer, beide LPK-BW.