„Wir werden von unserem Smartphone entmündigt“

Wie gehe ich heute verantwortungsvoll mit den Daten meiner Klientinnen und Klienten um? Robert Reick vom GwG-Ethikrat im Gespräch mit Netzphilosophin Leena Simon – über Mündigkeit im digitalen Zeitalter und ihren Digitalcourage-Workshop für die GwG, der am 28. Oktober 2022 online stattfindet.

Robert Reick (RR): Unser Gespräch zeichne ich mit einem digitalen Aufnahmegerät und einer SD-Karte auf. Was sollte ich mit der Datei besser nicht tun?
Leena Simon (LS): (lacht) Um mich nicht zu verärgern? Oder um mich nicht zu gefährden?

RR: Um mich richtig zu verhalten – oder zumindest um mich nicht falsch zu verhalten.
LS: Also, ich wäre nicht sehr glücklich, wenn Sie die Datei in irgendeine Cloud legen würden. Zumindest wenn Sie darüber keine eigene Kontrolle haben – und das ist nun mal mit den meisten Clouds so. Dann läge die Datei also auf einem Computer anderer Menschen und Sie wissen nie, wer hier welche Zugriffe hat. Und wenn ich ihnen jetzt private Dinge erzähle oder eine geheime Informantin wäre, dann könnten Sie mich damit durchaus gefährden. Ansonsten ist eine sogenannte SD-Card eine feine Sache: Da wird alles lokal gespeichert. Ein Problem könnte dann ein Transkriptionsservice oder ein Übersetzungsdienst darstellen, weil Sie im Zweifel nicht wissen, was dort mit den Dateien passiert. In jedem Fall sollten Sie sich aber vorab mit einem solchen Dienstleister auseinandersetzen, in dessen AGB zu schauen und alle Beteiligten informieren, damit Sie nicht einen Vertrag zulasten Dritter abschließen. Juristisch regeln ließe sich der Schutz fremder Daten mit einem sogenannten Auftragsverarbeitungsvertrag – kurz: AVV – mit dem Dienstleister. Hiermit wird dieser zum verantwortungsvollen Umgang verpflichtet.

*RR: Im Personzentrierten Ansatz spielen Audiomitschnitte von den Gesprächen mit unseren Klient*innen eine große Rolle – sei es in Forschung, Supervision oder Selbstreflexion. Was droht, wenn man mit diesen meist digital abgespeicherten Dateien nicht sorgsam umgeht?*
LS: Nehmen wir mal Ihren Fall: ein digitales Diktiergerät mit einer SD-Karte. Solange das Gegenüber darüber informiert ist, besteht zunächst kein Problem. Bei einem Handy dagegen wandern Aufnahmen oft vom Benutzer völlig unbemerkt in die Clouds des Smartphone-Herstellers oder Vertragsanbieters. Ob sie dort geschützt und verschlüsselt liegen, weiß man oft nicht. Eine weitere wichtige Frage: Welchen Weg nimmt eine Datei? PC-Betriebssysteme wie Windows geben viele Nutzer*innen-Daten preis – da läge die Datei also nur halbwegs sicher. Sie könnten auch angegriffen worden sein und einen Trojaner auf dem Rechner haben. Aber selbst wenn wir davon ausgehen, dass kein Virus oder Trojaner existiert und die Datei auf Ihrer Festplatte liegt, könnte Ihnen immer noch in der Anwendung etwas schiefgehen – wenn zum Beispiel der Kopfhörerstecker beim Zugfahren rausrutscht oder Fremde beim Transkribieren auf dem Bildschirm mitlesen. All das sollte man bedenken.

RR: Und wenn ich die Datei an meine Supervisorin oder meine kollegiale Intervisionsgruppe senden möchte?
LS: Eine unverschlüsselte E-Mail zu verschicken wäre schon mal keine so gute Idee. Wahrscheinlich ist die Datei ohnehin zu groß für eine E-Mail – und da stellt sich schon wieder die Frage: Wo lege ich sie hin? Bequem ist es natürlich, die Datei in eine Cloud zu packen und den Link zu verschicken – aber da gibt es gleich zwei Probleme: Erstens haben Sie wahrscheinlich nicht geklärt, wie sicher Ihre Datei in dieser Cloud liegt. Und zweitens haben Sie unverschlüsselt einen Zugangslink verschickt. Auf diese Weise können Unbefugte Zugang zu vertraulichen Daten erhalten!

Leena Simon, graduierte Philosophin, IT-Beraterin und Netzpolitologin; Schwerpunktthemen ihrer Tätigkeit sind digitale Mündigkeit und Technikpaternalismus; sie arbeitet u. a. für das Anti-Stalking-Projekt im Frieda Frauenzentrum in Berlin und für Digitalcourage e. V.
(Foto: Alexander Altmann)

RR: Was wäre denn eine sichere Lösung?
LS: Wenn Sie keine eigene Cloud und keinen eigenen Server betreiben, sollten Sie mit einem Passwort arbeiten. Dieses sollten Sie nicht unverschlüsselt versenden. Um eine E-Mail zu verschlüsseln, eignet sich zum Beispiel der bewährte Standard OpenPGP. Um wirklich sicherzugehen, sollten Sie aber auch schon die Audio-Datei selbst verschlüsseln. Hier rate ich zu VeraCrypt, eine Software, die auf allen drei Betriebssystemen plattformübergreifend funktioniert und sich recht problemlos bedienen lässt. Eine derart verschlüsselte Datei könnten Sie dann sogar getrost in eine Cloud legen, weil weder Cloudbetreiber noch Dritte mit der Datei in dieser Form etwas anfangen könnten. Wenn Sie dann noch

das Passwort mit verschlüsselter E-Mail an die Supervisionsgruppe senden, ist alles in Ordnung.

RR: Auf unserer jüngsten Delegiertenversammlung wurde beschlossen, dass unsere Mitglieder solche sensiblen Daten generell nicht mehr mit dem Smartphone aufnehmen, speichern oder abspielen dürfen. War das nach Ihrer Einschätzung eine sinnvolle Entscheidung?
LS: Absolut. Den meisten Menschen ist überhaupt nicht klar, was mit dem Smartphone alles möglich ist. Wenn man eine Netzwerkanalyse macht und nur mal schaut, welche Daten von einem Smartphone in zwei Minuten wohin geflossen sind, dann reibt man sich die Augen! Weil das Smartphone in unheimlich viele Richtungen Kontakt aufnimmt – das kann man nicht einfach kontrollieren oder gar verändern.

*RR: Gibt es denn abseits von Smartphone-Abstinenz und Verschlüsselungstechniken auch noch simplere Wege für einen verantwortungsvollen Umgang mit Klient*innen-Daten?*
LS: Natürlich kann ich auch immer noch auf USB-Sticks beziehungswiese USB-Schnittstellen vertrauen – wenn ich meine Supervisionsgruppe ohnehin persönlich treffe. Aber auch der USB-Stick müsste verschlüsselt werden und zwar wieder auf genau die eben beschriebene Weise. Da ist also nicht viel gewonnen. Und wenn USB-Sticks über mehrere PCs wandern, besteht wieder die Gefahr der Virenübertragung. Da sollten also alle ein sicheres System haben. Nur: Wie betreibe ich ein sicheres System? Meiner Meinung nach lässt sich heute ein Windows-Rechner gar nicht mehr sicher betreiben. Ein Virenscanner vermittelt einem letztlich nur ein gutes Gefühl – aber das ist im Prinzip das Schlimmste: Er beruhigt unser Gewissen und lässt uns glauben, wir müssten nichts mehr sonst tun.

RR: Man zahlt ja auch Ablass!
LS: Stimmt leider. In der IT-Sicherheit bezeichnen viele den Virenscanner als „Schlangenöl". Ich selbst sehe das zwar nicht ganz so kritisch, denke aber auch: Der Virenscanner verkauft seine Updates, das ist sein Geschäftsmodell, und wenn es keine neuen Viren gibt, fällt dieses Geschäftsmodell in sich zusammen. Da muss man keine Verschwörungen unterstellen, sollte aber wachsam gegenüber unheilvollen Allianzen bleiben. Separat davon ist zu betrachten, dass Virenscanner nur bekannte Viren finden können und keine bisher unbekannten.

RR: Wie steht es mit Firewalls?
LS: Eine Firewall scannt nicht meinen Systeminhalt nach bekannter Angriffssoftware, sondern sie funktioniert eher wie eine Membran zwischen meinem PC und dem Internet: Bestimmte Verbindungen unterbindet und blockiert sie. Der Erfolgt hängt davon ab, wie ich meine Firewall eingestellt und trainiert habe. Man kann ihr zum Beispiel am Anfang „sagen", dass sie jede Verbindung unterbindet – und dann definiert man nach und nach genau die Ausnahmen für Anwendungen und Adressen, die man bewusst zulassen möchte und schaltet verschiedene Verbindungen wieder frei. Wenn man dabei aber etwas falsch macht, zum Beispiel zu großzügig Ausnahmen definiert, ist das System leider auch nicht mehr sicher.

RR: Haben Sie denn auch eine gute Lösung für den Umgang mit Viren und Trojanern?
LS: Nehmen wir Windows als Beispiel: Hier ist es ab Version 10 gar nicht mehr möglich, das System sicher zu machen. Wenn ich mich aber entscheide, mit diesem Risiko zu leben, ist bei Windows zumindest eine ausreichend gute Firewall eingebaut. IT-Experten in meinem Umkreis empfehlen in diesem Setting gar keinen zusätzlichen Virenscanner mehr, sofern man die Firewall und die anderen internen Schutzsysteme gut eingestellt hat.

RR: Aber Ihre Patentlösung ist das auch noch nicht, oder?
LS: Die Lösung ist natürlich, wie schon angedeutet, freie Software zu benutzen. Firefox, Linux und vieles mehr. Das ist auch alles inzwischen für den „Heimanwender" geeignet, sofern man sich das richtige Betriebssystem aussucht. Hier bietet sich zum Beispiel Linux Mint an. Das System ist sehr einfach zu installieren und zu benutzen. Hier habe ich auch die Möglichkeit, direkt bei der Installation das gesamte System zu verschlüsseln. Alles lokal Gespeicherte ist dann schon mal in ziemlich guter und sicherer Umgebung aufgehoben. Aber sobald ich es dann an andere weitergebe, greift für den Transport wieder all das, was ich vorhin schon zu Verschlüsselung und Passwort gesagt habe.

RR: Vor der Pandemie galt für viele die persönliche Begegnung als fast unersetzbar – nun sind aber doch manche Supervisionsgruppen und Weiterbildungen ins Netz abgewandert. Wenn auf so einem Treffen auf Zoom oder MS-Teams eine Audiodatei abgespielt wird, ist doch wahrscheinlich der Damm gebrochen – ganz unabhängig davon, wie die Datei zuvor gespeichert war, oder?
LS: Ja, richtig. Das gilt schon für die Inhalte ihrer eigenen Unterhaltungen dort. Bei den bekannten Anbietern ist mir bislang nur bekannt, dass sie sehr stark die Nutzungsmetadaten kontrollieren und ich weiß nicht, wie intensiv sie selbst die Inhalte auswerten. Möglich wäre das aber natürlich. Eigentlich habe ich keinen Anlass, dieser Plattform zu vertrauen. Wenn ich mir mit einer Vereinbarung mit einer US-amerikanischen Firma wie Zoom zusichern lasse, dass Zoom die Daten nicht missbräuchlich auswertet, könnte ich mir zwar einreden, dass ich juristisch abgesichert sei, doch ob das wirklich zutrifft, ist höchst zweifelhaft. Denn der amerikanische „Cloud Act" und die europäische DSGVO sind hier inkompatibel. Das hat der europäische Gerichtshof kürzlich in dem Urteil „Schrems II" bestätigt. Bei Nicht-EU-Plattformen wie Zoom weiß ich de facto nicht, was mit den Daten passiert. Ich wäre da vorsichtig.

RR: Was erwartet die Teilnehmenden beim Workshop, den Sie am 28. Oktober für die GwG zu diesen Themen anbieten?

LS: Im Workshop werde ich eine Einführung in die Verschlüsselungstechniken PGP und VeraCrypt geben. PGP ist extra für E-Mails gebaut worden und bequem in der Anwendung für genau diesen Bereich. VeraCrypt ist vielfach nutzbar, man kann ganz verschiedene Verschlüsselungen damit vornehmen. Ich habe beispielsweise schon Frauenhäuser in VeraCrypt geschult, was nötig ist, da häusliche Gewalt heute leider oft digitale Wege findet. Aber mit diesen beiden Werkzeugen und etwas Übung können die Teilnehmenden künftig sensible Daten von Klient*innen sicher austauschen.

RR: Noch ein paar weniger technische Fragen zum Schluss: Auf Ihrer Website ist zu lesen, dass Sie sich unter anderem mit dem Thema digitale Mündigkeit beschäftigen. Was verstehen Sie darunter?
LS: Mündigkeit bedeutet heute vor allem Verantwortung zu übernehmen – für sich und sein eigenes Leben und Fortbestehen. Kant hat Mündigkeit auf die Gesellschaft angewendet und gesagt: Genauso wie ein Jugendlicher heranreifen muss und dann immer mehr Verantwortung für sein Leben übernimmt, müssen auch wir als Gesellschaft uns aus unserer selbstverschuldeten Unmündigkeit befreien. Das wiederum angewendet auf die digitale Welt, auf die Kommunikationswelt – letztlich sind ja alle digitalen Handlungen Kommunikationshandlungen – bedeutet das: Ich übernehme Verantwortung für mein eigenes Handeln im Netz und ich übernehme Verantwortung für meine Kommunikationsgemeinschaft. Ich trage dafür Sorge, dass ich mir und anderen nicht schade. Und ich bin auch dann bereit, mich dem Leben im digitalen Bereich zu stellen statt zu sagen: „Da kenne ich mich nicht aus und deswegen bin ich nicht zur Verantwortung zu ziehen." Wenn ich meiner Verantwortung gerecht werden will, muss ich mich so mit den Geräten und der Technologie vertraut machen, dass die Verantwortung für mich zumindest überschaubar wird. Das ist eine Haltungsfrage. Dazu muss ich nicht viel wissen, sondern kann sofort damit anfangen. Wenn ich aber digitale Mündigkeit praktiziere, bleibt es nicht aus, dass ich mich zunehmend mit Technik befasse und auch mehr darüber lerne. Einfach weil ich oft in Situationen komme, in denen ich Verantwortung übernehmen und dann prüfen muss, ob ich das überhaupt kann.

RR: Was meinen Sie: In welche Richtung steuert unsere Gesellschaft angesichts der Digitalisierung?
LS: Leider genau in die entgegengesetzte: Unsere Geräte und Verträge werden immer intransparenter. Es wird immer unklarer, was da eigentlich alles passiert. Und wenn es nach den Firmen geht, sollten wir das auch gar nicht wissen. Die Bestrebungen gehen meiner Einschätzung nach immer mehr in eine Richtung, in der die oder der Einzelne gar nicht mehr mündig entscheiden kann. Wenn zum Beispiel mein Smartphone ohne mein Einverständnis und mein Zutun meine Daten ungefragt in eine Cloud legt, kann ich natürlich nicht verantwortungsvoll damit umgehen, weil ich gar nicht weiß, dass das passiert. Wir werden von unserem Smartphone und anderen Geräten bzw. deren Konstrukteuren zunehmend entmündigt. Noch weiter geht das zum Beispiel bei Apple: Hier bekommt man als Nutzer*in bei der eigentlich komfortablen Umzugsfunktion für neue Geräte keinerlei Auswahlmöglichkeiten mehr angeboten. Auch im Großen gibt es diese Entwicklung: So werden ganze Länder praktisch nur noch von Facebook mit Internet und somit auch nur noch von Facebook mit Nachrichten und Informationen versorgt. Wir wissen, dass da die Algorithmen stark aktiv sind und genau die Nachrichten in den Vordergrund rücken, die ganz viel Engagement hervorrufen: Nachrichten, auf die viel reagiert wird. Also nicht nur Katzenvideos, sondern auch Lügen- oder Hassnachrichten. Langfristig unterhöhlen diese Entwicklungen hier und anderswo Demokratie und Freiheit.

Interview: Robert Reick, Mitglied des GwG-Ethikrats
(Bearbeitung: Elena Winter)

Der Digitalcourage-Workshop für GwG-Mitglieder findet am 28. Oktober von 9 bis 12 Uhr online statt. Informationen unter barg@gwg-ev.org.