Ausspähen von Daten vs. Berufsverschwiegenheit

Die Enthüllungen über das Ausspähen des elektronischen Datenverkehrs und des globalen Internets sind vermutlich für nur wenige hinreichend spezialisierte Kollegen mandatsträchtig. Ich hoffe, dass ihre Zahl so rasant steigt wie die Breite der Erkenntnis über die datennackte Welt zunimmt. Sie werden gebraucht.

Die Politik und damit auch der Gesetzgeber versagen (sich), wirksam zu handeln oder handeln zu wollen, weil sie ein (großer) Teil des Problems sind: Die Enthüllungen sind peinlich im ursprünglichen Sinn des Wortes. Pein, weil offenbar wird, dass die dafür bestimmten Kontrollmechanismen gewollt oder ungewollt nicht funktioniert haben. Pein, weil der demokratiewidrige Kasus aufgedeckt wurde. Pein, weil die Politik nicht mehr so unverhohlen vom Datenmissbrauch Nutzen ziehen kann.

Offenbar wird aber auch, dass es keine wirksame Kontrolle über personenbezogene oder sensible Daten von Unternehmen überhaupt gibt. Die Vernetzung über das weltweite Internet wendet Technologien an, die nur die kennen, die sie installieren, bis ihnen ein Hacker auf die Spur kommt, der die Erkenntnisse daraus wiederum – mit kurzatmigem Vorsprung – zu seinen Zwecken nutzt: Ein epidemischer Wettlauf ohne Gegenmittel. Da die Geheimdienste geheim arbeiten, gibt es auch niemanden, der sie kontrollieren kann. Die parlamentarischen Kontrollgremien, fachlich kaum versiert, sind bloßes Alibi.

Die Datenausspähung und die dahinter stehenden Systeme bedrohen die Anwaltschaft und jede zur Berufsverschwiegenheit verpflichtete Disziplin. Wie lässt sich die Unsicherheit des elektronischen Datenverkehrs mit der zivilrechtlich, strafrechtlich und berufsrechtlich sanktionierten Berufsverschwiegenheit vereinbaren? Das Internet ist ein unkontrollierter Selbstbedienungsladen für Geheimdienste, private Kommunikationsunternehmen, Täter und Opfer des Datenmissbrauchs. Es ist deshalb für den geschützten Informationsaustausch nicht mehr zu gebrauchen. Wie kann dann der Gesetzgeber noch seine Vorhaben verfolgen, künftig den gerichtlichen Schriftverkehr nur noch elektronisch abzuwickeln? Die Halbwertzeit dafür heute staatlich angedachter Sicherheitssysteme dürfte der Rasanz, Sicherheitssysteme zu knacken, nicht gewachsen sein.

Der Zwang zum elektronischen Datenverkehr mit Gerichten und Behörden ist unter heutigen Erkenntnissen mit der absoluten Pflicht zur Berufsverschwiegenheit nicht zu vereinbaren. Dort wie im E-Mail-Verkehr gibt es für den zur Berufsverschwiegenheit verpflichteten Berufsträger bei aller Sorgfalt keine Kontrolle über die Daten und keine Erkenntnismöglichkeit festzustellen, wer und auf welchen Wegen auf Daten zugreift und wie und wann verwendet.

Die Pflicht zur Berufsverschwiegenheit ist nur eine Seite. Die Vertraulichkeit des Anwalt-Mandanten-Verhältnisses ist ebenso in Gefahr. Wird es abgewertet, weil wir als Berufsträger die Vertraulichkeit nicht mehr sichern können? Darf ich als Rechtsanwalt und/oder Notar noch an einem internationalen elektronischen Datenaustausch mit vertraulichen Vertragswerken über eine M&A-Transaktion teilnehmen, wenn, wie wir jetzt wissen, Unbefugte beliebig mitlesen und Informationen missbrauchen können? Wie werden Gerichte entscheiden, wenn durch den Datenmissbrauch dem Mandanten ein Schaden entsteht? Reicht das Argument: „Ich wusste es nicht, ich konnte den Datenmissbrauch nicht verhindern?“ Gab es bis zu den Veröffentlichungen in Wikileaks oder von *Snowden* einen Vertrauensschutz und gibt es ihn auch weiter? Und wie lange? Mache ich mich strafbar oder schadensersatzpflichtig? Was sagt die Haftpflichtversicherung dazu? Geben die täglichen neuen Enthüllungen Anlass, den Vertrauensschadenhaftpflichtversicherer auf eine Gefahrenerhöhung nach § 23 VVG hinzuweisen?

Wie weit gehen die Sorgfaltspflichten des Anwalts, wenn wir die Mechanismen, Sicherheitsprogramme beliebig außer Funktion zu setzen, gar nicht kennen? Welche Sorgfaltspflichten habe ich, Verschlüsselungsprogramme anzuwenden und ihre Wirksamkeit zu überprüfen, wenn man aus den USA im Zusammenhang mit den NSA-Enthüllungen hört, dass Regierungen sogar Verschlüsselungsunternehmen unter Druck setzen, ihre Techniken zum ungenierten Datenzugriff durch Behörden zu offenbaren oder zu schließen? In welchem Umfang kann und muss ich prüfen, ob die Daten in einer Cloud im Nirvana des Internet gespeichert werden und wer darauf Zugriff hat oder haben könnte? Die Warnung, amerikanische Server zu vermeiden und deutsche zu nutzen, scheint zu verpuffen, nachdem die Kooperation der Geheimdienste über alle Grenzen hinweg bekannt wurde, und anscheinend sogar auf geheimstaatlichen Vereinbarungen beruhen soll. Darf ich auf Behörden vertrauen, die selber Opfer und Täter zu sein scheinen?

Ich habe keine Lösung. Ich kann nur anstoßen, darüber offen zu reden. Muss uns der Gesetzgeber mit der Gefahr anderweitigen Missbrauchs von der Einhaltung der Berufsverschwiegenheit per Gesetz freistellen, wenn die Provider von Kommunikationsnetzen mit oder ohne staatliche Unterstützung die Sicherheit ihrer Dienste nicht garantieren können, gleichwohl aber jedermann darauf angewiesen ist? Das wird schwierig, weil uns der Staat gegen sich selber schützen müsste.

Rechtsanwalt und Notar Dr. Ekkehard Helmig, Wiesbaden