



FRANS VAN DER REEP

ist ein inspirierender Vordenker aus den Niederlanden, seit 2003 Professor für Digitales an der Fachhochschule Inholland und seit langer Zeit Senior Strategie-Berater bei KPN. Sein Schwerpunkt: Internet-Einfluss auf Leben und Arbeit. Interviews mit Van der Reep erschienen in zahlreichen niederländischen und internationalen Zeitungen und Zeitschriften. Zudem bloggt und schreibt er über aktuelle Trends in folgenden Bereichen: Strategie, Marketing und Sales, HRM, Finanzen zukunftsweisende Innovationen, ICT und BPM. Er ist regelmäßiger Sprecher bei (internationalen) Fachkonferenzen zu den genannten Themen.

Neue Technologien, die Gesellschaftsordnung und das Rechtssystem

Ein Kommentar von Frans van der Reep

Vier Fünftel aller Menschen finden, dass ein Internetanschluss ein Grundrecht ist. Das haben Forschungen der BBC World Service ergeben. Im Rahmen dieser Forschung wurden insgesamt 27.000 Menschen aus 26 Ländern befragt. Länder wie Finnland und Estland haben bereits bestimmt, dass das Internet zu den Grund-Menschenrechten zählt. Internationale Gremien wie z.B. UNO sind auch dafür. Ein deutscher Richter hat ein ähnliches Urteil gefällt. Fazit dieser Ansichten: Ohne Internet hat man keinen Anschluss zu Großteilen des gesellschaftlichen Miteinanders mehr. In Kürze kann man wahrscheinlich selbst die Parkgebühren ohne Smartphone und Internetzugang nicht mehr bezahlen.

Ist es das, was wir wollen? Und wenn das der Fall ist, müssten dann keine Schranken eingebaut werden? Wenn ein Internetanschluss Grundnutzenfunktion hat, genauso wie Wasser, Abwasser, Wege usw., sollte das nicht von irgendwo grundlegend reguliert werden?

Ja, ich denke, dass ein solches Grundrecht grundsätzlich formuliert werden sollte, aber das Leben sollte auch ohne Internet möglich bleiben. Ich wünsche mir, dass Parkgebühren auch künftig mit Münzen bezahlt werden können und dass wir nicht zu einem teuren Smartphone verurteilt werden.

Grundrechte brauchen Schutz

Die Unternehmen und die Staaten müssen aber dafür verantwortlich sein, dass kein Hacken privater Daten und Internetbetrug möglich sind. Wenn ein Unternehmen gehackt wird und diese Tatsache mich als Kunden benachteiligt, dann muss das betreffende Unternehmen für den Schaden die volle Haftung tragen. Unternehmen sollten gesetzlich verpflichtet werden, hoch sensibel mit den Daten ihrer Kunden umzugehen und das betrifft auch deren Umgang mit den Sicherheitsaspekten neuer Technologien. Aber auch wir Bürger müssen viel aktiver auf diesem Gebiet agieren und unseren Anteil im Kontext des Problems akzeptieren, um Internetbetrug zu vermeiden zu können.

Die digitale Sicherheit hat momentan für viele Unternehmen keine Priorität. Die Banken etwa neigen dazu, die Haftung für einen eventuellen Kartenbetrug oder Phishing nur mit Kulanz zu regeln. Hier dürfen die rechtlichen Regelungen nicht allein von der Politik der kommerziellen Banken abhängen.



... Neue Technologien, die Gesellschaftsordnung und das Rechtssystem

Wer kontrolliert eigentlich die Software?

Wie kommt es, dass die Zulassung für (neue) Software nicht geregelt ist, wo sie doch eine immer eminentere Rolle in unserer Gesellschaft spielt? Für ein neues Auto, ein neues Flugzeug oder Arzneimittel ist eine verfahrensintensive Genehmigung erforderlich. Für Software ist dagegen nichts geregelt. Schauen Sie, was mit den Boeing Dreamliner vor einem Jahr passiert ist. Wenn der FAA, der Luftfahrtinspekteur, findet, dass etwas nicht stimmt, bleibt die ganze Flotte auf dem Grund. Das ist ein wirksamer Impuls, um alles im Sinne der Sicherheit zu regeln. In solchen Prozessen liegen viele Ideen, wie auch eine sichere digitale Welt im Rechtssystem verankert werden kann.

Kontrolliert die Software uns?

Was passiert, z.B. wenn wir via Internet physische Gegenstände steuern - Maschine-2-Maschine (M2M)? Was passiert mit einem Auto mit einer IP-Adresse? Dann kann ein Hacker theoretisch den ganzen Verkehr lahmlegen. Das passiert schneller, als wir uns das vorstellen können. Die ersten Brücken wurden auf diese Weise schon geöffnet und Flugzeuge gehackt. Wie wird man diesen Hackern habhaft, wenn sie in anderen Ländern sitzen, vielleicht sogar im Auftrag handeln?

Wie geht man als Bürger mit dem Internet der Dinge (IoT) um? Gibt es für Bürger überhaupt Alternativen? Was muss ich als Niederländer davon halten, dass ab nächstem Jahr in Autos ein Kästchen eingebaut wird, das permanent die Lage meines Autos verschickt, ein Kästchen, das nicht ausgeschaltet werden kann, ein Kästchen, worum ich als Bürger nicht gebeten habe.

Was macht man mit Drohnen, bei denen bereits verschiedene Arten der künstlichen Intelligenz angewendet werden, wodurch sie automatisch die Entscheidung über Mord treffen können?

Wie kommt es, dass kontaktlose Bezahlung weltweit eingesetzt wird, während die Sicherheitsfrage nicht beantwortet ist? Wer haftet für den eventuellen Schaden? Wenn Ihr Schrittmacher gehackt wird, und Sie es nicht überleben: Wer haftet denn dafür? Wie kann ich mich gegen die dunkle Seite der Technologie (the dark side of technology) schützen?

Sollen Unternehmen (ICT) vom rechtlichen Standpunkt aus nur sichere Lösungen ihren Kunden anbieten (Haftplicht)? Als Bürger nehme ich an, dass ich sicher über die Brücke fahren kann. Kann ich dann nicht davon ausgehen, dass auch das Internet geregelt ist, wenn es sich um meinen Schrittmacher, kontaktlose Bezahlung und so viele andere Sachen handelt?

Das sind die Rechtsfragen der Zukunft, der nahen Zukunft, wofür es noch keinen klaren Rahmen gibt. Diesen Prozess aktivieren und die Haftungsfragen regeln - auf diesen Gebieten liegt nicht nur die Herausforderung für das Rechtsinstrumentarium sondern auch für unsere Gesetzgeber.



... Neue Technologien, die Gesellschaftsordnung und das Rechtssystem

Wegen der enormen Abhängigkeit müssen wir die Struktur von ICT als gesellschaftliche Grundstruktur behandeln: the fifth domain. In einer Informationsgesellschaft muss der Informationsstrom ungehemmt fließen können. In solch einer Gesellschaft ist dies ein Grundbedarf. Und es handelt sich nicht nur um einen sicheren Internetanschluss sondern auch um alle Elemente, die man benötigt, um sicher im Internet kommunizieren und Geschäfte abwickeln zu können: E-Erkennung (e-ID), digitale Unterschrift, digitaler Notar usw.

Die neuen Technologien kamen schnell, ziemlich schnell, wodurch sich die rechtlichen Veränderungen auf dem Gebiet verspätet haben - und ja, man kann nur die Missstände konstatieren. Aber das ist kein Vorwurf! Das ist ein Appell, um diese Themen auf die Tagesordnung zu setzen. Die politischen und gesetzlichen Rahmenbedingungen sowie das Verstehen des Umfangs von Cyberkriminalität, passen sich nicht schnell genug an diese Veränderungen an.

Wie geht man mit Sicherheitsproblemen um, die an den Wurzeln eines Rechtsstaates zu sitzen scheinen? Potenzielle Sicherheitsprobleme, die eine Grundlage für Big Brother schaffen und verschiedene Strukturen ins Leben rufen, deren Bestehen vor 10 Jahren noch undenkbar gewesen wäre!

Rechtsschutz, Schutz der Bürger gegen den Staat, der sich immer mehr Befugnisse zuschreibt, die immer öfter demokratische Prinzipien widersprechen, das ist eine eilige Frage. Als erster Schritt wäre z.B. eine ethische Kommission (Gremium) sinnvoll, um zu beurteilen, welche neue Technologien wir brauchen, und welche doch eher eine Gefahr darstellt.

Technologie betrifft heute die gesellschaftlichen Grundordnungen. Entscheidungen darüber dürfen nicht nur von Unternehmen getroffen werden. Hier liegen zahlreiche gesellschaftliche Herausforderungen für die Politiker, wobei Antworten einen Platz in unserem System benötigen. ¶

