Durch das Sicherheitspolizeigesetz rückt der gläserne Bürger näher. Das darf der ÖVP nicht gleichgültig sein.

von Christian Mertens

"Endziel der Entwicklung muss eine totale Informationserfassung und -verarbeitung sein; dazu muss der Bürger im Rahmen seiner täglichen Verrichtungen auch seiner Auskunftspflicht genügen." Ist das ein Zitat aus einem aktuellen Änderungsentwurf zum Sicherheitspolizeigesetz? Oder aus einer noch geheimen Richtlinie der Europäischen Union? Keine Sorge: Die Passage stammt aus dem fantastischen Roman "Ypsilon minus" des Österreichers Herbert W. Franke, der schon 1976 die düstere Dystopie einer totalitären Technokratie entwarf, in der elektronische Überwachungsanlagen die absolute Kontrolle ermöglichen.

Das Bedürfnis nach Befriedigung eines subjektiven Sicherheitsbedürfnisses, aber auch die höhere Bequemlichkeit durch größtmögliche Datenvernetzung lässt viele vergessen, wie gefährdet unsere Privatsphäre ist. Die Möglichkeiten, die das Sicherheitspolizeigesetz vorsieht - Onlinedurchsuchung von Festplatten mittels Trojaner, Abfrage von Handystandortdaten ohne Zustimmung eines Richters, das Abhören von Telefongesprächen, das Lesen von SMS oder das Ermitteln von Gesprächspartnern -, sind da nur der Anfang. Nicht von ungefähr schlagen Unternehmen wie T-Mobile Alarm. Es bleibt ein unangenehmer Beigeschmack, auch für den unbescholtenen Bürger, wenn man sich vergegenwärtigt, wie "flexibel" die Polizei das Zauberwörtchen "Gefahr" auslegen kann und wer den Spielraum des berechtigten Einsatzes interpretieren darf. Ob jeder der Versuchung widerstehen kann, Informationen über den vermeintlichen Nebenbuhler, die unliebsame Nachbarin oder einen lästigen Verwandten zu beschaffen? Man hat aus der Polizei gerade zuletzt auch schon anderes gehört.

Unter dem Schlagwort der "Vereinfachung" werden immer mehr Daten auf Karten oder andere Träger gespeichert und abrufbar. Schon im Herbst 2006 warnte die Wiener Ärztekammer vor möglichem Datenmissbrauch infolge einer geplanten elektronischen Krankenkarte, die die komplette Krankheitsgeschichte eines Patienten enthalten soll. Hacker könnten die Daten missbräuchlich verwenden, etwa durch Weitergabe an interessierte Firmen. Personalchefs könnten dann vorweg zum Beispiel Krebskranke oder Menschen mit psychischen Problemen unter den Bewerbern aussondern. Es muss aber nicht gleich Kriminalität im Spiel sein: Beim Surfen im Internet hinterlassen wir erkennbare virtuelle "Duftmarken", die von Suchmaschinen aufgestöbert und eifrig verwertet werden. Das nächste Werbemail kommt bestimmt!

Der Grundsatz von Licht und Schatten der Technik gilt auch für den Arbeitsplatz: In vielen Betrieben werden die von den Mitarbeitern besuchten Internetsites registriert und ausgewertet, ebenso die Adressaten der E-Mails. Die Argumentation: Computer inklusive der zugeordneten Mailadressen sind nach Ansicht des Dienstgebers in dessen Besitz und somit nicht als "persönlich" anzusehen. Ein Vergleich der Privatsphäre des E-Mail-Verkehrs mit dem Briefgeheimnis wird daher vielfach nicht anerkannt. Formulierungen in Betriebsvereinbarungen oder Dienstordnungen gestatten meist eine private Nutzung "im unumgänglichen Ausmaß", was natürlich eine "Gummiformulierung" ist und bei "Bedarf" gegen unliebsame Dienstnehmer verwendet werden kann - Mobbing der anderen, der virtuellen Art.

Schließlich trägt noch die immer häufigere Videoüberwachung zur Einengung unserer Privatsphäre bei. In U-Bahnen, auf öffentlichen Plätzen, im Kaufhaus, in Museen oder jüngst in Gemeindebauten werden immer neue Videokameras installiert. Was als Sicherheitsmaßnahme gegen Gewalt und Kriminalität gut gemeint sein kann, hat auch eine andere Facette: Manche stehen so stundenlang bei ihrer Arbeit unter Beobachtung und bei "Bedarf" - siehe oben. Außerdem: Wer kriminelle Akte im Sinn hat, wird eben in eine nicht überwachte Zone ausweichen, bis auch diese unter elektronischer Beobachtung steht. Das Spiel lässt sich ad infinitum fortsetzen, bis der letzte Flecken öffentlichen Raums von Videokameras aufgezeichnet wird.

Zusammenfassend: Jede der oben skizzierten Maßnahmen für sich ist argumentierbar. Die Gefahr liegt in der ausufernden Konzentration und im möglichen Missbrauch. Wer kontrolliert die Kontrolleure? 2005 rügte die Europäische Kommission Österreich dafür, dass die Kontrolle der Daten nicht unabhängig genug erfolge. Auch der Innenminister sollte sich daran erinnern, dass für die ÖVP - die sich in ihrem "Wiener Programm" als christdemokratische Partei definiert - die "Achtung der Menschenwürde der Ausgangspunkt unseres politischen Handelns" ist. Explizit heißt es dort sogar: "Gefahren für die Freiheit, die sich aus neuen technischen Entwicklungen ergeben, muss rechtzeitig vorgebeugt werden." Die modernen christdemokratischen Parteien Europas nach 1945 verstanden sich ja gerade als Antwort und Gegenkonzept zum menschenverachtenden, alles kontrollierenden Totalitarismus nazistischer oder stalinistischer Art.

In der veröffentlichten Meinung dominiert der parteitaktische Hickhack rund um Regierung und Neuwahlen. Das ist ärgerlich. Größere Sorgen sollte uns aber bereiten, dass wir darüber vergessen, über die wirklich wichtigen gesellschaftspolitischen Probleme zu reden. Eines der drängendsten ist die schleichende Beschneidung unserer Privatsphäre durch immer neue Datensammlungen und Überwachungseinrichtungen. Sonst erinnert uns die Realität eines Tages an die düstersten Kapitel der utopischen Literatur.

Christian Mertens ist Historiker und Mitbegründer der sozialliberalen Initiative Christdemokratie (ICD) in der ÖVP.