STIFTUNG DATENSCHUTZ

Aus Sicht der Stiftung Datenschutz

Die gewohnte Überwachung

Frederick Richter, LL. M.

Manchmal lasse sich der Wald vor lauter Bäumen nicht erblicken, heißt es. Kann dies auch bei Überwachungsmaßnahmen passieren? Wann reden wir überhaupt von „Überwachung"? Und wann sollten wir das tun? Um den Überblick zu behalten, ist ab und an eine Gesamtschau anzuraten.

Der Gedanke ist nicht neu. Die Bürgerrechtsorganisation digitalcourage e. V. betont seit Jahren die Notwendigkeit einer „Überwachungsgesamtrechnung".[1] Eine solche lässt sich durchaus aus der Rechtsprechung des Bundesverfassungsgerichts ableiten.[2] Aus dem Urteil zur Vorratsdatenspeicherung von 2010 spricht, dass staatliche Maßnahmen zur Überwachung nicht nur einzeln, sondern auch in ihrer Summe betrachtet werden müssten. Der Gesetzgeber ist daher gezwungen, bei der Erwägung neuer Speicherungspflichten oder -berechtigungen die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen in den Blick zu nehmen.[3]

Das Ganze betrachten – auf allen Ebenen

Ein solch holistischer Blick sollte aber für eine echte Gesamtschau nicht auf den öffentlichen Bereich beschränkt bleiben. Zwar wollen Grundrechte traditionell Abwehr gegen eine womöglich übergriffige Staatsgewalt bieten. Auch das richterlich geschaffene Recht auf informationelle Selbstbestimmung entspringt dieser Abwehrkonstellation. Doch hat sich die Bedrohungslage geändert – genauer: aus der *einfachen* Beobachtung ist eine *dreifache* geworden. Nicht mehr nur staatliche Stellen sammeln Daten über die Bürgerinnen und Bürger, sondern auch private Stellen. Und schließlich überwachen sich die Datensubjekte mitunter selbst und arbeiten unbewusst den ebenfalls auf „Überwachung" ausgerichteten Unternehmen zu. Der Begriff ist dabei nicht zu verstehen im Sinne behördlicher Verfolgung oder unmittelbarer Kontrolle, eher im Sinne einer Informationssammlung. Die Motivation der drei Überwachungspole ist dabei unterschiedlich. Doch sind diese Unterschiede für das Ergebnis einer sektorübergreifenden Überwachungsgesamtrechnung langfristig von stark sinkender Relevanz.

Frederick Richter ist Ständiger Autor bei „Privacy in Germany". Seit Anfang 2013 leitet er die in Leipzig ansässige Bundesstiftung für Privatheit und Datenschutz. *(Foto: Lorenz Becker)*

Jedem sein Motiv für Überwachung

Die öffentliche Hand überwacht, um Gefahren von der Bevölkerung abzuwenden. Denn diese erwartet vom Staat in erster Linie Sicherheit. Die Politik möchte Handlungskraft zeigen und die Erwartungshaltung pro Sicherheit erfüllen (und mit dieser Erfüllung um Wahlstimmen werben). So trachten denn Innenpolitik und Behörden nach immer mehr Kontrollstruktur – von Kennzeichenerfassung bis Gesichtserkennung. Etwaige individuelle Ablehnungen von sicherheitsbezogenen Informationssammlungen werden einer – unterstellten oder tatsächlichen – sicherheitspolitischen Mehrheitsmeinung untergeordnet. Vorratsdatenspeicherung kennt kein Opt-Out.

1 Zuletzt im Rahmen der Verfassungsbeschwerde des Vereins gegen das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. 12. 2015 (Az. 1 BvR 2683/16).

2 Bieker, F./Bremert, B./Hagendorff, T., Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf., in: Roßnagel, A./Friedewald, M./Hansen, M. (Hrsg.), Die Fortentwicklung des Datenschutzes, 2018.

3 BVerfG, 1 BvR 256/08 – Rn. 218; BVerfGE 125, 260.

Die Wirtschaft sucht mit Überwachung derer, die ihre digitalen Angebote nutzen, die Mehrung des Umsatzes – was in einer marktorientierten Wirtschaftsordnung normal ist. Dass diejenigen wirtschaftlichen Akteure, die ihre Kundschaft und deren Vorlieben besser kennen, bessere Umsatzchancen haben, liegt auf der Hand. Wenn jedoch einem solchen datenbasierten „Kennenlernen" keine rechtlichen Grenzen gesetzt würden, käme es zu immer mehr Durchleuchtung. Es blieben dann nur freiwillige Eigenverpflichtungen und unverbindliche Corporate Responsibility Kodizes. Deren Befolgung und Durchsetzung ist jedoch ohne rechtliche Bewehrung schwach. Es bedarf also gesetzlicher roter Linien. Ob diese Linienziehung langfristig eher Aufgabe des Zivilrechts oder des Datenschutzrechts sein sollte, darüber lassen sich erquickliche Grundsatzdebatten führen.

Die Bürgerinnen und Bürger leisten zunehmender Datensammlung zu ihrer Person oft auch aus eigenem Antrieb Vorschub. Zwei Eigenschaften machen für freiwillige Überwachung empfänglich: Bequemlichkeit und Sparsamkeit – garstige Zeitgenossen mögen auch sprechen von Trägheit und Gier. So ist es bequem, sich von einem Versandhändler Warensendungen nicht vor, sondern hinter die Haustür stellen zu lassen und für diese Option die Erlaubnis zum Öffnen der „smart door" zu gestatten – und damit ohne Not ein Eindringen in die Privatsphäre.[4] Und sparsam ist es, einen Versicherungstarif zu wählen, der die Erlaubnis zur Kontrolle individueller Verkehrswege[5] oder zur Aufzeichnung individueller körperlicher Betätigung finanziell honoriert.[6] In derartigen Konstellationen werden Beobachtungen und Datensammlungen nicht etwa zähneknirschend und vermeintlich alternativlos hingenommen. Vielmehr wird das Überwachtwerden zum Tauschmittel: Zu verbergen hat man nichts, aber etwas zu verkaufen.

„Privat vor Staat"

Wer allein die Informationssammlungen der öffentlichen Hand kritisch sieht, sich aber im privaten Bereich noch vollkommen autonom wähnt, mag zwar weiterhin streng unterscheiden dürfen. Nicht zu unterschätzen ist jedoch der Gewöhnungseffekt. Auch insoweit dieser sich aus der nicht-öffentlichen Sphäre nährt, so relativiert doch auch er die Wahrnehmung öffentlicher Maßnahmen. In einer zukünftig komplett vernetzten Umgebung wird zwar die Frage des Zugriffs auf die Datensammlungen entscheidend bleiben. Doch die Wahrnehmung der Überwachung an sich, das Erleben des verfassungsgerichtlich gefürchteten „diffusen Gefühls des Beobachtetwerdens" wird sich entspannen. Wenn überall Kameras erfassen, wird der Zustand der Observation zur Normalität. Allein der konkrete Datenzugang und potentielle Datenmissbrauch wird dann noch viele interessieren, die bloße Datenerhebung aber nur mehr wenige. Beispiel ist die Stadt London, in der man das Beobachtetwerden geradezu erlernt, wenn man – Schätzungen zufolge – durchschnittlich 300mal am Tag von einer der bald 500.000 Kameras erfasst wird.

Aus dem privaten Sektor mögen zwei Beispiele aus den USA eine Idee vom Voranschreiten persönlicher Überwachung durch nicht-staatliche Stellen geben: Der Autohersteller Volvo wird dort bald alle Autos mit einer Kamera-Innenraumüberwachung ausstatten und die fahrende Person permanent beobachten – um feststellen zu können, ob es der gut geht oder ob sie abgelenkt ist.[7] Und der Händler Amazon hat sich Patente auf Armbänder erteilen lassen, mit denen sich jeder Griff des Personals im Warenlager überwachen lässt – inklusive Vibration bei falscher Handbewegung.[8]

Seien wir also ruhig etwas aufmerksamer, was eine schleichende Entwicklung angeht: Das Gleiten in die überwachte Gesellschaft.

4 Amazon is exploring ways to deliver items to your car trunk and the inside of your home; Bericht auf CNBC vom 22. 10. 2017; abrufbar unter: www.cnbc.com/2017/10/10/amazon-is-in-talks-with-phrame-and-is-working-on-a-smart-doorbell.html.

5 47 % der Autofahrer bereit, für günstigere Versicherungsprämie Fahr- und Fahrzeugdaten zur Verfügung zu stellen; PM der CosmosDirekt-Versicherung v. 15. 11. 2016; abrufbar unter: www.cosmosdirekt.de/veroeffentlichungen/telematik-195712.

6 Jeder Dritte würde Gesundheitsdaten an Versicherer geben; Bericht zu YouGov-Umfrage, abrufbar unter: www.cio.de/a/jeder-dritte-wuerde-gesundheitsdaten-an-versicherer-geben,3092361.

7 Pressemitteilung der Volvo Car USA vom 20. 03. 2019; abrufbar unter: www.media.volvocars.com/us/en-us/media/pressreleases/250015/volvo-cars-to-deploy-in-car-cameras-and-intervention-against-intoxication-distraction.

8 If Workers Slack Off, the Wristband Will Know; New York Times vom 01. 02. 2018; abrufbar unter: https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html.