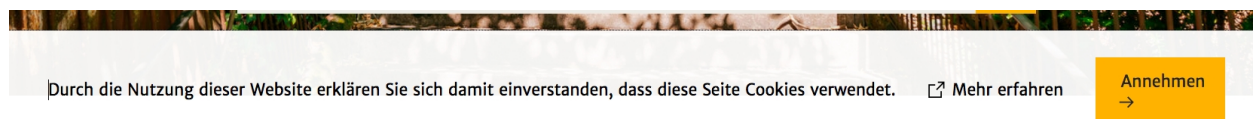


Zweierlei Recht

Im Internet scheint erlaubt, was in der Wirklichkeit verboten ist

Beim Öffnen vieler Internetseiten findet man einen Hinweis, dass man durch die weitere Benutzung der Seite zustimme, dass Cookies (kleine Textdateien) auf dem Rechner des Benutzers abgelegt werden dürfen. Hier zum Beispiel auf der Seite der Stadt Stuttgart:



Der Laie kann nicht erkennen, ob es sich dabei um Cookies handelt, die bestimmte Funktionen ermöglichen, etwa Waren, die man erwerben möchte, in einen virtuellen Einkaufswagen zu legen, oder ob es Cookies sind, die den Benutzer ausspionieren helfen, was man im Alltag als „Wanze“ bezeichnen würde.

Was man mit Hilfe von Cookies machen kann beschreibt die Telekom so:



„Ähnliche Technologien“ können z.B. Scripte sein, also Programme, die auf dem Rechner des Benutzers irgend etwas tun, wovon der Benutzer meist nichts merkt, wenn er nicht ein Programm wie „NoScript“ benutzt, das jeden Versuch Scripte auszuführen meldet und blockiert.

Man muss sich den obigen Text einmal in Ruhe betrachten und nachdenken, was das heißt:

Weitergabe Ihrer Daten an Drittanbieter. Die *Daten* werden für Analysen, Retargeting und zur Ausspielung von personalisierten Inhalten und Werbung auf Seiten der Telekom, sowie auf Drittanbieterseiten genutzt. Weitere

Was heißt das im Klartext?

1. Die Telekom sammelt Daten der Benutzer.
2. Die Telekom gibt diese Daten an Andere weiter.
3. Damit kann das Nutzerverhalten untersucht werden.
4. Dadurch können Benutzer gezielt angesprochen werden.
5. Den Benutzern kann dadurch Werbung, die auf sie zugeschnitten ist, gezeigt werden.
6. Und all das nicht nur auf den Seiten der Telekom, sondern bei allen anderen Anbietern, die Daten von der Telekom erhalten.

Dabei hat das Bundesverfassungsgericht 1983 fest gestellt, dass die Daten jedes Menschen geschützt sind. Wikipedia:

Das Recht auf **informationelle Selbstbestimmung** ist im Recht Deutschlands das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Es ist nach der Rechtsprechung des Bundesverfassungsgerichts ein **Datenschutz-Grundrecht**, das im Grundgesetz für die Bundesrepublik Deutschland nicht ausdrücklich erwähnt wird. Der Vorschlag, ein Datenschutz-Grundrecht in das Grundgesetz einzufügen, fand bisher nicht die erforderliche Mehrheit. Personenbezogene Daten sind jedoch nach Datenschutz-Grundverordnung und nach Art. 8 der EU-Grundrechtecharta geschützt.

Anschaulicher wird es, wenn man den Sachverhalt aus dem Internet in den Alltag überträgt:

Wenn es klingelt und man öffnet die Tür und der Besucher stellt den Fuß hinein, so dass man sie nicht mehr schließen kann, wäre das schon Hausfriedensbruch. Wikipedia:

Der **Hausfriedensbruch** ist die vorsätzliche Verletzung des verfassungsrechtlich geschützten Gutes der Unverletzlichkeit befriedeter Besitztümer. Der Hausfriedensbruch ist in Deutschland (...) ein Straftatbestand, der ausschließlich das individuelle Hausrecht schützt.

Für das Eindringen in einen Raum genügt bereits, dass der Täter unberechtigt einen Teil des Körpers in den befriedeten Bereich gelangen lässt. Ein Betreten mit dem gesamten Körper ist nicht notwendig; ausreichend ist schon der „Fuß in der Tür“.

Das grenzt dann schon an den Einbruch, der in Deutschland kein gesonderter Tatbestand ist, sondern stets mit weiteren Delikten, z.B. **Diebstahl** kombiniert wird. Wikipedia:

Ein **Einbruch** geschieht in der Regel mit dem Ziel, in den Besitz von Gegenständen und/oder Informationen zu gelangen.

Wobei sich Diebstahl interessanter Weise vor allem gegen das Vermögen einer Person richtet. Das Wort „vermögen“ bezeichnet aber nicht nur Besitz, sondern auch die Fähigkeit etwas zu tun. Das hat das Bundesverfassungsgericht klar erkannt und deshalb 1983 geschrieben:

Die Selbstbestimmung bei der freien Entfaltung der Persönlichkeit werde gefährdet durch die Bedingungen der modernen Datenverarbeitung. Wer nicht wisse oder beeinflussen könne, welche Informationen bezüglich seines Verhaltens gespeichert und vorrätig gehalten werden, werde aus Vorsicht sein Verhalten anpassen (siehe auch: Panoptismus¹). Dies beeinträchtigt nicht nur die individuelle Handlungsfreiheit, sondern auch das Gemeinwohl, da ein freiheitlich demokratisches Gemeinwesen der selbstbestimmten Mitwirkung seiner Bürger bedürfe. „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“

Hinterhältiger Weise sind viele Browser zum Betrachten von Webseiten so eingestellt, dass sie solche Zugriffe von Webseiten-Anbietern erlauben, ohne den Benutzer zu fragen. Das wird dem Benutzer aber als Erleichterung verkauft, weil er sich um Vieles nicht mehr kümmern müsse. Man darf daher annehmen, dass sowohl die Hersteller der Geräte, als auch die Anbieter von Webseiten unter einer Decke stecken, wenn es darum geht aus dem Benutzer einen „Gläsernen Bürger“ zu machen, nur nicht im Interesse und im Auftrag des Staates, sondern im Interesse der Wirtschaftsunternehmen, die daran verdienen. Die Daten, die Nutzer Facebook im Monat überlassen, sollen im Schnitt 5 Euro wert sein. Das Internet und seine Nutzung sind also nicht kostenlos. Genau gegen die sozusagen ungefragt erteilte Zustimmung hat sich der Europäische Gerichtshof 2019 ausgesprochen: Meldung des Deutschlandfunks Oktober 2019:

Internetnutzer müssen nach einem Urteil des Europäischen Gerichtshofs beim Besuch von Webseiten einer Speicherung sogenannter Cookies aktiv zustimmen.

Eine voreingestellte Zustimmung sei unzulässig, urteilten die Richter in Luxemburg. Der Nutzer solle vor jedem Eingriff in seine Privatsphäre geschützt werden. Hintergrund ist ein Online-Gewinnspiel eines deutschen Anbieters. Der Betreiber hatte bei der Einwilligung zur Benutzung von Cookies ein Ankreuzkästchen mit einem voreingestellten Häkchen verwendet. Dagegen hatte der Bundesverband der Verbraucherzentralen geklagt.

Cookies speichern beim Surfen Daten auf der Festplatte des Nutzers und werden auch zur Werbung genutzt.

(Rechtssache C-673/17)

¹ Dieser Begriff von Michel Foucault geht auf das kreisrunde Gefängnis von Bentham zurück, bei dem ein Wächter in einem Turm in der Mitte des Hofes in alle Zellen sehen konnte, die nur zum Hof hin Fenster hatten. Der Begriff meint, dass durch Kontrolle die Macht erhalten und die Menschen diszipliniert werden könnten.

Zurück zum Alltagsbeispiel:

Wenn jemand, den man in die Wohnung lässt, etwa einen Handwerker oder eine Putzfirma, und ein Mitarbeiter dort den Schreibtisch durchstöbert und Kopien von Daten anfertigt, z.B. durch Fotografieren, dann ist das selbstverständlich **Diebstahl von Daten**.

Warum soll das anders sein, wenn man eine Webseite besucht und der Anbieter dieser Seite sich offenbar große Mühe gibt, um Daten des Benutzers zu stehlen? Je nach Seite findet man manchmal eine ganze Reihe von Programmen, die Daten erheben. Beliebte sind zum Beispiel Programme (Tracker), die verfolgen von welcher Seite der Benutzer kam und zu welchen Seiten er weiter geht. Das wäre was man im Alltag „Stalking“ nennt. Wikipedia:

Stalking beschreibt das willentliche und wiederholte (beharrliche) Verfolgen oder Belästigen einer Person, deren physische oder psychische Unversehrtheit dadurch unmittelbar, mittelbar oder langfristig bedroht und geschädigt werden kann. Stalking wird im deutschen Strafgesetzbuch als Straftatbestand der Nachstellung geahndet und ist in vielen Staaten Thema kriminologischer und psychologischer Untersuchungen. Der Begriff ist in den 1990er-Jahren im US-amerikanischen und britischen Raum aufgekommen und hat sich im deutschsprachigen Raum vor allem in der Umgangssprache verbreitet.

2017 hat der Gesetzgeber das Gesetz zur Verbesserung des Schutzes gegen Nachstellungen verschärft. Wikipedia:

Das bedeutet, dass der Täter also von nun an nicht nur dann bestraft werden kann, wenn er durch unbefugtes Nachstellen in Form der beharrlichen Vornahme ausdrücklich angeführter Tatvarianten eine schwerwiegende Beeinträchtigung der Lebensgestaltung verursacht hat, es reicht nunmehr aus, dass die Handlungen zu einer solchen Beeinträchtigung geeignet waren.

Ist das **Ausspionieren der Webseiten-Besucher** durch Tracker (Programme die sie verfolgen) oder entsprechende Dienste etwa kein unbefugtes Nachstellen? Warum?

Um das zu klären, müsste man sich die Datenschutzbestimmungen der jeweiligen Seite anschauen. Im Falle der Stadt Stuttgart, wäre das aber zugleich die Zustimmung zur Nutzung von Cookies, denn anders als durch Benutzung der Seite, kommt man eben nicht zu den Datenschutzbestimmungen. Außerdem müsste der Internetbenutzer, wenn er vor unangenehmen Überraschungen sicher sein wollte, bei jeder Seite zunächst die Datenschutzbestimmungen lesen, was vor allem bei Seiten in fremden Sprachen zu erheblichem Aufwand führen würde. Da man aber in der Regeln nur die Möglichkeit hat die Vorgaben des Anbieters zu akzeptieren, ersparen sich sogar Rechtsanwälte, die die Texte vielleicht verstehen würden, die Lektüre. Ein Konzertveranstalter verlangte daher mal im Kleingedruckten, dass jeder Veranstaltungs-Besucher auch das Klo putzen müsse. Es dauerte eine Weile bis das jemand auffiel.

Auch hier hilft wieder der Vergleich mit der Wirklichkeit: Wenn man irgend wo in der Wohnung, etwa auf dem Klo, einen Hinweis anbringt, dass jeder, der die Wohnung betritt 100 Euro bezahlen muss, dann kann diesen Hinweis nur jemand lesen, der die Wohnung bereits betreten hat. Das ist selbstverständlich nicht fair, denn ein Vertrag kann eigentlich nur dann zustande kommen, wenn beide Vertragsparteien vorher die Vertragsbedingungen kennen und

sich wissentlich und willentlich auf diesen Vertrag einlassen können. Ist das nicht der Fall, dürfte der Vertrag anfechtbar, wenn nicht sogar nichtig sein. Schon die Ausnutzung der Notlage eines Vertragspartners gilt als Wucher. Wikipedia:

Wucher bezeichnet das Angebot einer Leistung zu einer deutlich überhöhten Gegenleistung unter Ausnutzung einer Schwächesituation eines Vertragspartners. Ursachen können zum Beispiel in einer Notlage oder in einer asymmetrischen Informationsverteilung zu Lasten eines Vertragspartners liegen. An Wucher können zivil- und strafrechtliche Folgen geknüpft sein.

Es ist also im Internet üblich Dinge zu tun, die im Alltag als Verstöße gegen das **informationelle Selbstbestimmungsrecht** gelten würden, als **Hausfriedensbruch**, als **Einbruch, Diebstahl, Stalking** und **Wucher**.

Aber während man das in der Wirklichkeit meist mit den Sinnen wahrnehmen würde, ist das in der virtuellen Scheinwelt des Internets kaum möglich. Das erklärt vielleicht, weshalb sich kaum jemand gegen diese Zumutungen wehrt, aber auch, weil man davon als Laie in der Regel nicht viel mit bekommt, geschweige denn versteht, was da gespielt wird.

Die Süddeutsche Zeitung hat in einem Experiment ein Smart-Phone so präpariert, dass es alle seine Tätigkeiten protokollierte. Ergebnis: Es verband sich – meist ohne Auftrag und ohne den Benutzer zu fragen – in 24 Stunden 7300 mal mit 636 Servern (Rechnern die Inhalte anbieten, verarbeiten oder sammeln), also ungefähr 5 mal in der Minute. Nun muss sich jedes Mobiltelefon in der Funkzelle melden, in der es sich befindet, damit Gespräche zu ihm durchgestellt werden können. Aber im Grunde genügt es, wenn es das tut, sobald es aus einer Zelle in die nächste wechselt. Die hohe Zahl der Kontaktaufnahmen, auch während des Schlafes der Testperson, lässt nur den Schluss zu das derartige Geräte von vorn herein so eingestellt sind, dass sie ihre Besitzer ausspionieren. Wer das verhindern will, muss rund hundert Einstellungen zu mehr Datenschutz verändern. Das überfordert die meisten Laien.

Was man aber vielleicht machen könnte, wäre jeden Webseiten-Betreiber aufzufordern alle über einen selbst gespeicherten Daten zu übermitteln. Der Aufwand für einen selbst wäre zwar erheblich, aber der für die Anbieter noch viel mehr.

Solange aber im Internet und in der Wirklichkeit des Alltag mit zweierlei Maß gemessen wird und Rechte im Internet ausgehebelt werden, muss sich niemand wundern, wenn das Vertrauen in die Anbieter sinkt und der Ärger wächst. Irgend wann wird der Gesetzgeber reagieren müssen, wenn er Rechtssicherheit gewährleisten will. Die Datenschutz-Verordnung ist ein erster Schritt.

Dass aber die Anbieter aus Bequemlichkeit, Geldgier oder Dummheit die nützlichen Seiten des Internets ruinieren und hoffen, es werde schon niemand merken, geschweige denn klagen, entspricht dem Niveau von kleinen Kindern, die Dinge ausprobieren, um ihre Grenzen kennen zu lernen. Erwachsene sollten dieses Stadium längst hinter sich haben und wissen, was man tun darf und was nicht, um der Gesellschaft keinen Schaden zuzufügen.

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“

Knapp 40 Jahre nach diesem Urteil des Bundesverfassungsgerichts, sind wir längst so weit.