Die dunkle Seite der eGK

Diese Information soll dazu beitragen, dass sich mehr Menschen über die wirklichen Gefahren durch die eGK informieren können. Dafür wurden ausschließlich öffentlich zugängliche Quellen aus dem Internet benutzt und in dieser Form zusammengetragen, z. B. von Heise Online.

Nur wer informiert ist, kann nicht mehr belogen und manipuliert werden. ***Helfen Sie mit und geben Sie diese Dokumentation weiter.*** *Es bestehen gute Aussichten dieses Irrsinnsprojekt zu verhindern und unsere Freiheit und Selbstbestimmung zu erhalten. Wir wünschen Ihnen die besten Umstände.*

WICHTIGER HINWEIS

Wenn Sie diesen Text ganz oder teilweise für eine Klage betr. eGK verwenden, fragen Sie bitte VORHER Ihren Anwalt, denn er ist für eine Aufklärung und NICHT juristisch verfasst. Sonst werden sie mit der Klage ziemlich sicher scheitern, da die juristischen Formulierungen fehlen und zweimal wegen derselben Sache klagen können Sie nicht. Die Richter werden daraufhin bundesweit alle weiteren Klagen betr. eGK mit Hinweis auf diese gescheiterte Klage abschmettern.

Noch etwas: Wenn Sie klagen, dann bitte gegen die für die eGK geschaffene IT-Infrastruktur und die damit geplante zentrale Speicherung der Patientendaten und NICHT gegen die eGK. Diese Klagen werden nämlich alle abgewiesen mit der absurden Behauptung, dass die eGK nicht mehr Daten enthält als die bisherige KV-Karte und Sie also keine Nachteile durch die eGK hätten.

Also bitte fragen Sie zuerst Ihren Anwalt, wenn sie klagen wollen – vernetzen Sie sich möglichst vorher mit Gleichgesinnten, z. B. Hier:

http://stoppt-die-e-card.de/
http://ddrm.de/?p=4101#more-4101 (Die Datenschützer RheinMain)
http://www.kuhlsite.de/links.html (Kompetenter Anwalt, gute Seite mit Links)

Ansonsten soll und darf dieser Text hemmungslos weitergegeben werden.

Stand : 6. Juli 2015

Die Unmöglichkeit von Datensicherheit und ärztlicher Schweigepflicht bei der eGK ist übrigens hervorragend in dieser **Power Point Präsentation** zu erkennen: **(download)**
http://www.stoppt-die-e-card.de/index.php?
serendipity[subpage]=downloadmanager&thiscat=2&file=57
(Legen Sie die mal Ihrer Krankenkasse vor mit der Bitte um Stellungnahme)

Die dunkle Seite der eGK – eine Aufklärung

Vorneweg: *Es geht NICHT in erster Linie um die eGK, sondern um die dazugehörige, zentrale Speicherung aller Patientendaten durch eine eigene IT-Infrastruktur. Die eGK ist nur der Zugangsschlüssel dazu. Wo diese Server stehen sollen, wird hartnäckig verschwiegen. Diese können in Deutschland, aber auch in den USA oder anderen Ländern stehen und würden trotzdem immer nur als zentraler Speicherort bezeichnet werden. Tag und Nacht Zugriff hätten offiziell ca.2 Millionen Zugangsberechtigte. Die genaue Zahl lässt sich allerdings niemals ermitteln – siehe obiger Link – Power Point Präsentation: „eGK - INNENTÄTER, die unterschätzte Gefahr".*

Wussten Sie übrigens, dass:

- *Deutschland den USA und GB (wem noch?) seit 1945 die straffreie Spionage vertraglich garantiert? Seite 20, Punkt 3*
- *Dass bis heute ALLE ausgegebenen eGK illegal sind, da nicht identitätsgeprüfte Fotos verwendet werden? Seite 8 ff und Musterbrief am Schluss*
- *Dass selbst der **GKV-Spitzenverband** zugibt, dass es KEINE Datensicherheit bei der eGK gibt und geben kann? Seite 35-36*
- *Dass selbst das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** im Juni 2015 offiziell zugegeben hat, **dass es keine 100%-ige Daten-Sicherheit geben könne und Computersicherheit ein fortlaufender Prozess sei.** Seite 47*

Wir empfehlen Ihnen erst den ganzen Text zu lesen.
(Lassen Sie sich von der Seitenzahl bitte nicht abschrecken)

Inhaltsverzeichnis:

- **Geplanter Missbrauch** der eGK zur Medikamenten-rationierung….Seite 44
- Bundesamt für Sicherheit in der Informationstechnik **(BSI)** gibt zu, dass es **KEINE Datensicherheit** geben kann….Seite 47
- Dazu kommt noch eine ganz andere, **weit größere Gefahr** durch TTIP und TISA….Seite 49
- MASIVE Gefahr durch **lebenslang gültige Krankenversicherungsnummer** (glatter Rechtsbruch)….Seite 50
- **DER ultimative Beweis für die Lügen von Datensicherheit mit Patientendaten** (Seite 54)
- **Musterwiderspruch** zur Rücksendung der eGK…. Seite 54

Punkt 1: ***„Doch Anspruch auf Ersatzverfahren ab 1. 1. 2015“***

Die Aussage, dass ab dem 1. 1. 2015 nur noch die eGK gilt ist falsch. Schließlich gibt es ein entsprechendes Ersatzverfahren, wenn jemand keine gültige Versicherungskarte habe. **Auch das Bundesgesundheitsministerium bestätigt dies auf seiner Website:** *„Alternativ“,* heißt es dort, *„kann auch eine Einzelfallbestätigung der Krankenkasse, dass zum Zeitpunkt der Behandlung ein Leistungsanspruch bestand, vorgelegt werden.“* Nur wenn der Patient einen solchen Nachweis nicht innerhalb des Quartals vorlege, müsse er die Behandlungskosten privat bezahlen.

Der Anspruch auf ein Ersatzverfahren ergibt sich auch aus:

1. § 18 Absatz 8 Satz 3 Punkt 1 Bundesmantelvertrag – Ärzte (BMV-Ä). Dort ist *„...von einem anderen gültigen Anspruchsnachweis“* die Rede, ebenso im Punkt 9.
2. In der Anlage 4 a zum BMV-Ä vom 1. 9. 2014, Anhang 1 Nr. 2.1, Satz 1 ist ebenfalls von *„...einem anderen gültigen Anspruchsnachweis“* die Rede.
3. § 19 Absatz 1 und 3 BMV-Ä weist noch einmal auf das Ersatzverfahren in der Anlage 4 a hin.

Damit dürfte der Anspruch der Versicherten auf Quartalsnachweise wohl klar bestätigt sein. JEDE Einschränkung, z. B. papiergebundene Nachweise nur für den Tag des Arztbesuches auszustellen, oder die Leistung ganz zu verweigern oder zu verzögern usw. **sind klare Rechtsbrüche. Diese Schikanen verstoßen gegen § 17,**

Abs. 1 SGB I:

§ 17 Ausführung der Sozialleistungen

(1) Die Leistungsträger sind verpflichtet, darauf hinzuwirken, daß *jeder Berechtigte die ihm zustehenden Sozialleistungen in zeitgemäßer Weise, umfassend und zügig erhält."*

Keine Sanktionen durch fehlendes Lichtbild zulässig:

§ 291 SGB V bestimmt zwar, dass die Krankenkassen ab 01.01.1995 eine Krankenversichertenkarte mit Lichtbild des Versicherten ausstellen sollen. **Eine wie auch immer geartete Sanktionsregelung (Verwirkung von Leistungsansprüchen, Verhängung von Buß- oder Zwangsgeldern etc.) für Versicherte, die das dafür notwendige Lichtbild nicht zur Verfügung stellen, ist aber weder im SGB V noch im SGB I enthalten.**

§ 291a SGB V wiederum regelt, dass die Krankenkassen ab 01.01.2006 eine elektronische Gesundheitskarte (eGk) mit Lichtbild des Versicherten ausstellen sollen. **Aber auch hier fehlt eine wie auch immer geartete Sanktionsregelung für Versicherte, die das dafür notwendige Lichtbild nicht zur Verfügung stellen.**

Punkt 2: *„Das aktuelle (und absurde) Urteil des Bundessozialgerichts"*

Die Behauptung des **BSG** in seinem aktuellen Urteil v. 18. 11. 2014, (AZ: B 1 KR 35/13 R) dass *„das Recht bereits die betroffenen Daten vor unbefugtem Zugriff Dritter und vor missbräuchlicher Nutzung schützt"* kann man getrost als (juristischen) **GAU** bezeichnen: (**G**rößter **A**nzunehmender **U**nsinn). Nur weil der Missbrauch verboten und strafbar ist, (außer für Geheimdienste, die über dem Gesetz stehen), sind die Daten doch nicht sicher. Das zu erkennen, genügt ein Minimum an gesundem Menschenverstand und das dürfte den Richtern vom BSG durchaus bewusst sein. Trotzdem einige Beispiele:

1. Mord, Diebstahl und Terrorismus z. B. sind auch verboten, gibt es die jetzt nicht mehr?
2. Die Bundesregierung kauft für Millionen Steuergelder „Steuer-CDs", deren Daten

auf kriminelle Weise beschafft wurden, was nach der Definition des BSG eigentlich gar nicht möglich sein soll. (Sog. INNENTÄTER, die aus Geldgier, oder weil sie erpresst oder gekauft worden sind, Daten beschaffen)

3. Die Einführung der anlasslosen Vorratsdatenspeicherung wird ja von der Bundesregierung gerade mit dem Hinweis auf Verhinderung von Terrorismus begründet und setzt also voraus, dass ein ganzes Volk aus potentiellen Kriminellen besteht, die es zu überwachen gilt, damit sie keine (terroristischen) Straftaten begehen, die es nach der Definition des BSG aber gar nicht geben kann. Damit bestätigt die Bundesregierung indirekt, dass die obige Behauptung des BSG Unsinn ist.
4. Gleichzeitig erlaubt Sie aber per Geheimverträge (nicht nur) US-Firmen die Spionage in Deutschland und lässt sich von NSA-nahen Firmen wie z. B. Booz Allen Hamilton in Sachen Personalausweis und eGK „beraten“. In obiger Firma arbeiten hochrangige Mitglieder der amerikanischen Geheimdienste. (Quelle: Heise-online, später mehr dazu)
5. Die Datenskandale spätestens seit den Enthüllungen Edward Snowdens dürften klar belegen, dass es keine Datensicherheit geben kann und niemals geben wird – erst recht nicht bei 2 Millionen offizieller Zugriffsberechtigter bei der eGK und einer niemals zu ermittelnden Zahl inoffizieller Zugriffsberechtigter (nein, ausnahmsweise mal nicht die Geheimdienste) sondern Mitarbeiter externer Dienstleister, EDV-Wartungsfirmen, Betreiber der Server und jede Menge Mitarbeiter bei Ärzten, Behörden Instituten, einschl. kurzfristig eingestellter (und bald wieder entlassener) Zeitarbeiter.....

Die weitere Behauptung des BSG im aktuellen Urteil: *„...die Ausstellung einer eGK verletzt nicht sein Grundrecht auf informationelle Selbstbestimmung“* verstößt gegen Art. 1 Grundgesetz und verletzt das Recht auf freie Entfaltung der Persönlichkeit nach Art. 2 Grundgesetz. In diesem Zusammenhang sei hier verwiesen auf das Urteil des Bundesverfassungsgerichts mit seiner Entscheidung zur Volkszählung 1983 (BVerfGE 65, 1 – Seite 51)

Quelle:
http://www.humanistische-union.de/themen/datenschutz/steuer_id/detail/back/steuer-id/article/die-personenkennziffer-der-traum-von-der-datenzusammenfuehrung/

Weiter:

Die Datensicherheit der eGK bzw. der gesamten Telematikinfrastruktur konnte lt. aktuellen Urteil des BSG NICHT geprüft werden, da sich diese noch im Teststadium befindet. Inwiefern die Technik wirklich sicher ist, wurde in den Verfahren also gar nicht durch Expertengutachten untersucht. Daher konnte auch keine fundierte Interessenabwägung vorgenommen werden.

Das BSG hat also ausdrücklich KEIN Qualitätssiegel für die datenschutzrechtliche Unbedenklichkeit der Telematik-Infrastruktur vergeben.

Kein Patient wird seine persönlichen Daten einem ungeprüften und daher potentiell unsicheren EDV-System anvertrauen wollen, zumal es dafür auch gar keine gesetzliche Grundlage gibt. (Allein der Standort der Server ist ungeklärt. Diese könnten wie schon erwähnt auch z. B. in den USA stehen. Welche Art von Chip auf der Karte verwendet wird, ist ebenfalls ungeklärt.)
Erinnert sei in diesem Zusammenhang an dass das **BverfG,** das in seinem epochemachenden Urteil zur Volkszählung vom 15. Dezember 1983 mit bemerkenswerter Klarheit bestimmt hat, **dass ein (technisches) Verfahren, das erst noch entwickelt werden muss, NICHT zur Beurteilung herangezogen werden darf.**

Im Wortlaut:
“Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die [Daten-] Sammlung […] zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren.” (Dies als nähere Bestimmung zum ‘Verhältnismäßigkeitsgrundsatz’.) Quelle: (Urteil im Volltext; Absatz 161).
Das aktuelle Urteil des BSG hätte also vor den Augen der damaligen Richter des BVerfG keinen Bestand gehabt. Und es wäre nicht das erste Mal, dass ein BSG-Urteil vom BVerfG wieder kassiert wird.

Ferner kann nach diesseitiger Lesart nicht erkannt werden, dass das o. a. BSG-Urteil gem. des §291 (a) SGB V den Versicherten nunmehr gesetzlich verpflichtet ein Foto einzusenden.
Das Urteil hebt auch nicht die Regelungen auf, die in § 19, Absatz 1 und 3 des Bundes-

mantelvertrag Ärzte in Verb. mit Anlage 4a BMV-Ä, (Anhang 1, Abs. 2.1 und Abs. 3) zwischen dem Gesamtverband der gesetzlichen Krankenkassen (GKV) und der Kassenärztlichen Bundesvereinigung (KBV) getroffen wurden und die ausdrücklich einen „papiergebundenen Anspruchsnachweis“ als Grundlage für die Inanspruchnahme eines Kassenarztes und die Abrechnung dieser Leistungen mit der Krankenkasse ermöglichen. Vergleichbare Regelungen gibt es auch mit den Kassenzahnärzten.

Ferner stellt das BSG fest: *„Die freiwilligen, vom Einverständnis des Betroffenen abhängigen Anwendungen der eGK begegnen keinen verfassungsrechtlichen Bedenken.“* Da von „Freiwilligkeit“ ja wohl keine Rede sein kann, wenn dieses „Einverständnis“ gegen den erklärten Widerstand von hunderttausenden Versicherter und Ärzte erzwungen werden muss, ergeben sich im Umkehrschluss sehr wohl verfassungsrechtliche Bedenken. Dies verstößt nämlich gegen Art. 1 GG (Grundgesetz) und verletzt zugleich das Recht auf freie Entfaltung der Persönlichkeit nach Art. 2 Grundgesetz. (Das grenzt schon an den Straftatbestand der Erpressung nach § 253 StGB, denn es ist mehr als verwerflich Hunderttausende Zwangsversicherte zur Teilnahme am eGK-Verfahren trotz immenser technischer und rechtlicher Probleme zu zwingen.)

Zudem hängt der Versicherungsschutz keineswegs von der eGK ab, sondern davon, ob man die Beiträge gezahlt hat und alle notwendigen Angaben nach § 15 SGB V erteilt hat. Zu diesen gehört übrigens NICHT das Einreichen eines Fotos.

Punkt 3:

A) Das Verfahren der eGK und die zentrale Speicherung aller Patientendaten verletzt das Recht auf informationelle Selbstbestimmung, u. a. da eine Datensicherheit weder besteht, noch garantiert werden kann. Verwiesen sei auch hier auf das Urteil des Bundesverfassungsgerichts mit seiner Entscheidung zur Volkszählung 1983 (BVerfGE 65, 1).

B) Die Krankenkassen erfüllen NICHT Ihren gesetzlichen Auftrag, da sie bis heute keine identitätsgeprüften Lichtbilder verwenden. **Dadurch werden durch die Krankenkassen keine Identitätsnachweise ausgestellt, die den gesetzlichen Vorgaben entsprechen.“**

(Selbst für einen Angelschein muss man zum Einwohnermeldeamt, wo die Identität geprüft wird.)

Hier der Musterbrief eines Widerspruchs gegen die Aufforderung zur Einsendung eines Fotos:

„Die Anforderung des Lichtbildes stellt einen Verwaltungsakt dar, da in dem Schreiben – in Fettdruck hervorgehoben – auf die gesetzlich verankerte Pflicht der Versicherten zur Lichtbildbereitstellung hingewiesen wird. Da Ihr Aufforderungsschreiben dazu dient, die öffentlich-rechtliche Regelung in § 291 SGB V umzusetzen, liegt ungeachtet der äußeren Form des Schreibens ein öffentlich-rechtliches Handeln vor. Das Schreiben entfaltet für den Adressaten auch belastende Wirkung, da dieser ein Lichtbild anfertigen lassen muss und es anschließend übersenden muss. Hier der Text:

„Die Lichtbildanforderung ist nach hier vertretener Auffassung rechtswidrig. § 291 SGB V verlangt, dass auf der Krankenversichertenkarte „Lichtbild und Unterschrift des Versicherten“ aufgebracht werden. Sinn dieser Regelung ist es, Missbräuche dadurch zu verhindern, dass die eGK mittels Lichtbild und Unterschrift ähnlich dem Personalausweis oder Reisepass zu einem Ausweis- und Identifikationsdokument ausgestaltet wird. Dies ergibt sich auch klar aus Anlage 4a des BMV-Ä. Dort heißt es in Anhang 1 unter Ziffer 1.2..

> ***Der Arzt ist verpflichtet, die Identität des Versicherten zu prüfen. ... Die Identität des Versicherten ist anhand der auf der elektronischen Gesundheitskarte aufgebrachten Identitätsdaten (Lichtbild, Unterschrift, Name, Vorname, Geburtsdatum) zu prüfen.“***

Eine solche Identitätsprüfung durch den Arzt ist aber nur möglich, wenn bereits bei der Herstellung der eGK ein identitätsgeprüftes Lichtbild verwendet worden ist, was bis heute definitiv NICHT der Fall ist. Ich verweise ergänzend auf eine im Internet veröffentlichte Broschüre des BMG mit der Bezeichnung „Die elektronische Gesundheitskarte“. Dort heißt es auf Seite 10: „Das aufgedruckte Foto weist einen Versicherten zweifelsfrei als Inhaberin oder Inhaber der Karte aus.“ Auch hat das BMG durch Frau Staatssekretärin Caspers-Merk auf eine Bundestagsanfrage mit der Arbeitsnummer 11/75, die die Notwendigkeit einer Identitätsprüfung durch die Krankenkassen bei Ausgabe der eGK betraf, im November 2008 dahingehend Stellung genommen, dass zwar die Ausgestaltung des Verfahrens in der Zuständigkeit der Krankenkassen liege, dabei aber Verfahren zu

bevorzugen seien, die eine Identitätsprüfung der Versicherten beinhalten.

Ohne eine solche Prüfung wird es also auch weiterhin Missbräuche gerade durch jene Personen geben, die auch bisher schon in betrügerischer Weise zum Schaden der Versicherten Leistungen der Krankenkasse erschlichen haben. Solange in dem Verfahren zur Ausgabe der eGK nicht sichergestellt ist, dass die eGKs auch tatsächlich mit einem Foto des Karteninhabers versandt werden, kann die eGK ihre gesetzlich vorgesehene Funktion nicht erfüllen. Insbesondere wäre es nicht möglich, die eGK in der im BMV-Ä vorgesehenen Art und Weise zu verwenden." (Ende des Musterbriefes)

Quelle:
https://diedatenschuetzerrheinmain.files.wordpress.com/2012/11/musterschreiben-wg-foto-egk.pdf

Der Arzt kann also die Identität gar nicht überprüfen und macht sich somit evtl. strafbar nach § 203 StGB (Ärztliche Schweigepflicht), wenn er sich auf die Daten der eGK verlässt und vielleicht auch noch Patientendaten per Internet überträgt (VSDM, Versichertenstammdatenmanagement). Dies bestätigt auch ein **Gutachten der Freien Ärzteschaft:** (Auszug)
"Um als Arzt nicht Gefahr zu laufen, selbst gegen die Regelungen des §203 StGB zu verstoßen, kann der Arzt nur durch die Nichtbeteiligung am VSD (Versichertenstammdatendienst) wegen der immanenten rechtlichen Mängel seine eigene Strafbarkeit – sei es als Täter oder Teilnehmer – sicher vermeiden. Schon die Bereitstellung einer unsicheren IT-Infrastruktur kann einen Verstoß i. S. v. § 203 StGB darstellen."

Pikanterweise darf der Arzt aber gar keine Identität überprüfen, denn er gehört nicht dem Personenkreis an, der lt. **§ 17 Personalausweisgesetz** dazu berechtigt ist. Will er die Identität nun feststellen/überprüfen, verstößt er also gegen § 17 Personalausweisgesetz und macht sich evtl. gleichzeitig lt. **§ 132 Strafgesetzbuch** der **Amtsanmaßung** schuldig. Der äußere Anschein genügt dazu lt. Aktueller richterlicher Rechtsprechung.
(Soll er jetzt gegen **§ 291 SGB V, § 203 StGB** und der **Anlage 4a, Anhang 1 BMV-Ä,** (Bundesmantelvertrag Ärzte) verstoßen, indem er die Identität nicht prüft oder gegen **§ 17 Personalausweisgesetz** und evtl. gegen **§ 132 Strafgesetzbuch,** indem er die Identität doch prüft???)
Quelle: http://strafverteidigung-hamburg.com/1951/amtsanmassung-§-132-stgb/

Wider besseren Wissens halten die Krankenkassen weiterhin an ihrer Praxis der nicht

identitätsgeprüften Fotos fest, obwohl feststeht, daß sie damit ihren gesetzlichen Auftrag gar nicht erfüllen können und auch bis heute nicht erfüllt haben.

Die hier vertretene Rechtsauffassung wurde durch das jetzt bekannt gewordene Gutachten der Kassenärztlichen Bundesvereinigung (KBV) bestätigt.

Quellen:
http://www.abendblatt.de/politik/article124533905/Hamburger-Senat-muss-Fragen-zu-Gesundheitskarte-beantworten.html
und
http://www.abendblatt.de/politik/article124502451/Gutachten-Die-elektronische-Gesundheitskarte-ist-illegal.html

Nach dem Abendblatt-Bericht über das bislang unter Verschluss gehaltene Gutachten der Kassenärztlichen Bundesvereinigung (KBV) ist die eGK rechtswidrig. Das Foto auf der Gesundheitskarte ist nicht identitätsgeprüft. Die Karte kann laut juristischer Expertise nicht eingesetzt werden wie geplant und verhindert deshalb auch nicht den Missbrauch.

Es gibt übrigens bis heute KEINE verlässlichen Daten über sog. „Missbrauch", der immer für diesen immensen Aufwand zur Einführung der eGK angeführt wird.

C) Es gibt bis heute keinen einzigen belegbaren *medizinischen* Grund für die eGK.

a) Das vielzitierte „Argument" der elektronischen Notfalldaten kommt:

1. einer Aufforderung zum Rechtsbruch gleich und
2. einer Aufforderung an den Notarzt, seinen geleisteten Eid des Hippokrates zu brechen. Im akuten Notfall spielt es keine Rolle, ob Sie z.B. an einer Penicillinallergie leiden oder welche Blutgruppe Sie haben. *Der Notarzt hat gar keine Zeit, um auf eine Computerverbindung zu warten und ein Bewusstloser oder ein geschocktes Unfallopfer wird kaum seine PIN-Nr. mitteilen können* und diese Informationen spielen für das Handeln des Notarztes auch keine wesentliche Rolle. Im akuten Notfall geht es darum, Herz, Kreislauf und Atmung zu stabilisieren. Eine Blutübertragung wird im lebensbedrohlichen Notfall mit einer „Standardblutgruppe" durchgeführt, erst im Krankenhaus wird die richtige Blutgruppe getestet, usw. **Ein Arzt, der anders handelt, wird ganz schnell vor Gericht landen.**

b) Gefährdung der Patientengesundheit:
(Patienten)- Daten müssen ständig aktualisiert werden. Krankheiten müssen EDV-tauglich werden. Komplexe, nicht vollständig verstandene Krankheitsbilder werden auf eine ICD-Nummer verkürzt. **So entsteht die Illusion, diagnostische Befunde und therapeutisch-präventive Behandlungsarten seien eindeutig.** Patienten müssen nicht mehr gefragt werden. Individuelle Unterschiede können in diesem allgemeinen und riesigen Informationssystem gar nicht berücksichtigt werden.
Das erhöht massiv die Gefahr für ärztliche Fehlleistungen, was Patienten mit ihrer Gesundheit und/oder mit ihrem Leben bezahlen müssen **und wäre ein krasser Verstoß gegen die ärztliche Sorgfaltspflicht und den Eid des Hippokrates, den jeder Arzt geschworen hat.**

Es ist bisher also KEIN praktischer *medizinischer* Nutzen erkennbar, in allen Test auf Praktikabilität im Alltag hat sich das Milliardenprojekt bisher als unbrauchbar herausgestellt.

D) Die sonstigen üblichen Argumente für die eGK sind ebenfalls nichtig, z. B.:

„Die neue Karte helfe den Ärzten, Sie besser zu behandeln. Ärzte hätten dadurch mehr Zeit für Sie und seien besser informiert“.
Das Gegenteil ist der Fall. Bei den Tests in den Testregionen stellte sich heraus: Die neue Karte raubt den Ärzten die Zeit. Das Einlesen der Daten, wenn der Patient in die Praxis kommt, das Erstellen von „elektronischen Rezepten“ und das Erstellen der „Notfalldatensätze“ kostet viel mehr Zeit als bisher. So haben ihre Ärzte weniger Zeit für Ihre Behandlung. Von Ihrem Haus- oder Facharzt können Sie die Unterlagen als Kopie bekommen, wenn Sie diese für einen Krankenhausaufenthalt oder Untersuchung bei anderen Ärzten benötigen. Nicht nur für Auslandsaufenthalte gibt es Notfallausweise auf Papier, sogar in viele Sprachen übersetzt. Die Daten können auch auf speziellen USB-Sticks gespeichert werden. Arztpraxen und Krankenhäuser können sich regional vernetzen. Alle diese Möglichkeiten wurden gar nicht geprüft.

Verwechslungsgefahr für Patienten in Krankenhäusern:
In der klinischen Routine löst die Elektronische Gesundheitskarte keinerlei Verwechslungsprobleme zwischen der Aufnahme und der Entlassung, da Lesegeräte für die Elektroni-

sche Gesundheitskarte innerhalb der Stationen gar nicht vorgesehen sind.

Quelle: eGk www.gen-ethisches-netzwerk.de - Patientendaten auf dem Präsentierteller

E) fehlende Kosten/Nutzen-Rechnung; explodierende Kosten bei fehlendem Nutzen.

1. Sollten die Kosten im Jahre 2004 offiziell noch bei 700 Mio € liegen, sind nunmehr **1,6 Mrd. €** veranschlagt. Neben Ärzten, Kliniken und Apothekern sollen die Krankenkassen den größten Teil davon bezahlen.
2. 2006 veröffentlichte der Chaos Computer Club ein Whistleblower-Dokument der Gematik, wonach die Gesamtkosten mehrere Milliarden betragen, ein Nutzen aber nur bei Annahme günstigster Bedingungen erkennbar sei. Dies hat sich inzwischen bestätigt.
3. 2009 analysierte dieselbe Strategieberatung wie 2006, Booz Allen Hamilton, Kosten zwischen **2,8 und 5,4 Milliarden €** für die Einführung der eGK. Erst die Nutzung möglichst vieler dieser bisher freiwilligen Funktionen durch möglichst viele Versicherte macht das Gesamtsystem profitabel. Dies ergab eine von der Gematik in Auftrag gegebene Studie der Düsseldorfer Unternehmensberatung Booz-Allen-Hamilton. Danach sind während der ersten fünf Jahre nach Ausgabe der eGK, sofern den Versicherten nur die weniger heiklen gesetzlich vorgeschriebenen Basisfunktionen zur Verfügung stehen, "sämtliche Anwendungen defizitär". **Erst nach der Einführung der „freiwilligen“ Anwendungen, elektronische Patientenakte und elektronischer Arztbrief werde der Nutzen höher sein als die Gesamtkosten und auch nur, wenn alle mitmachen.**
4. Ebenfalls 2009 berichtete das ARD-Magazin Monitor von Kosten bis zu **14 Milliarden Euro** im ungünstigsten Fall.
5. Die Kosten für die technische Ausstattung sind immens. Ebenso die erwartbaren bürokratisch-technischen Irrtümer. Diese fallen nicht nur einmalig, sie fallen fortlaufend an. Die Geräte und ihre Software sind jeweils auf dem neuesten Stand zu halten, ebenso die Patientendaten. Dies bedeutet u. a. permanente Fortbildung aller Mitarbeiter und ständige Systempflege aller EDV-Anlagen – **Zeit, die für die Behandlung der Patienten fehlt.**

Die kostenlose und sichere Alternative, dass die bisherige Versichertenkarte (ohne

Foto) nur in Verbindung mit einem Personalausweis zusammen gültig ist, wurde gar nicht geprüft, (90 % der Patienten wären sogar bereit dazu), **die Speicherung auf patienteneigenen USB – Sticks ebenfalls nicht.** Die USB-Stick-Lösung würde keine zentralen Server benötigen und die gespeicherten Daten bei den Patientinnen und Patienten lassen.

F) Die Datensicherheit der eGK ist NICHT gewährleistet und zwar:

1. Datenunsicherheit durch der Karte selbst

Bereits am 30. 12. 2013 wurde durch den Chaos-Computer-Club (CCC) in Hamburg öffentlich demonstriert, **wie Speicherkarten manipulierbar sind**.

Quelle: http://www.heise.de/newsticker/meldung/30C3-Trau-niemals-einer-Speicherkarte-2072906.html

Damit konnten:

1. Daten auf der Karte selbst **beliebig verändert und neu geschrieben** werden
2. Die manipulierte Karte erlaubte daraufhin **vielfältige Angriffe auf Rechner,** sobald der Nutzer eine umprogrammierte Karte in den Computer steckt. (u. a. sind damit „Man in the Middle-Attacken“ möglich).

Dazu kommen Mängel aller Art:

1. **Schwachstelle Verbindungsaufbau zu den diversen Servern im Internet**. Für den Zugriff zum Beispiel auf die Pflichtanwendung "Stammdaten-Management" ist eine Internetverbindung erforderlich. Überlange Laufzeiten sorgen für Wartezeiten und erhöhte Arbeitsbelastung in den Arztpraxen.
2. **Schwachstelle PIN**, die zum Zugriff auf die direkt auf der eGK gespeicherten Daten nötig ist. Nicht jeder kann sich, wie Kanzlerin Merkel hofft, auch noch eine weitere merken. (Schon gar keine 6-stellige)
3. **In Testregionen wurden zwischen 30 und 75 Prozent der Versichertenkarten** und auch der Heilberufskarten **durch falsche Eingabe** der initialen 6-stelligen PIN **dauerhaft gesperrt.** Bereits eine einfache Anwendung wie das elektronische Rezept ergab im „10.000er Feldtest“ 2008 Probleme. Die Arztsoftware (zugelassen durch die Kassenärztliche Bundesvereinigung) war mangelhaft. An all dem hat sich bis heute nichts geändert.

4. Professor Oliver Kalthoff (Universität Heidelberg und Hochschule Heilbronn) führte in einem sehr detaillierten und technischen Vortrag in die neue Gesundheitskarte ein.

Die Bedenken bzgl. der Sicherheit der auf der Karte gespeicherten Daten wurden dann experimentell eindrucksvoll von dem Informatiker aufgezeigt. **Mit Hilfe eines handelsüblichen Auslesegerätes** zeigte Herr Kalthoff, **wie einfach Daten aus der Gesundheitskarte extrahiert werden können.** Dabei ging es nicht nur um die Stammdaten wie Name und Geburtsdatum. Mit wenigen Operationen gelang es ihm grundsätzlich auch, mögliche Rezepte auszulesen.
Auch wies Kalthoff darauf hin, dass die Daten nicht alle auf der Karte gespeichert werden können, **sondern auf externen Servern abgelegt werden müssen.** Insofern ist die Sicherheit der Karte selbst, auf die sich die Diskussion im Moment konzentriert, nur ein Teil der relevanten Debatte um den möglichen Missbrauch.

Quelle: http://www.humanistische-union.de/nc/aktuelles/aktuelles_detail/back/aktuelles/article/baden-wuerttemberg-risiken-der-elektronischen-gesundheitskarte-praktisch-demonstriert/

Dazu kommen noch offene Fragen:

1. Um die Daten auf der eGK selbst zu ändern, benötigt jede(r) ein Lesegerät oder Zugang zu einem eKiosk.
2. Unklar ist, wer alles Daten auf den zentralen Servern ändern oder wer sie alles einsehen kann. Unklar ist auch, in welchem Land diese Server stehen sollen.
3. Andererseits haben nicht nur Ärzte, Apotheker oder Kassen Zugriff auf Daten, sondern nicht zuletzt die Gematik (also das BMfG) und ihre Dienstleister, wie IBM und eine bisher unbekannte und auch niemals genau zu ermittelnde Anzahl anderer. (Mögliche INNENTÄTER)
   Quelle: http://www.flegel-g.de/INNENTAETER%20%20-%20unterschaetzte%20Gefahr%20-%20eCard.pdf – S E H R L E S E N S W E R T
   Die Gematik wurde übrigens am 11. Jan. 2005 u. a. vom Bundesministerium für Gesundheit gegründet. Also ganz egal, was die Gematik sagt, es kommt immer vom BmfG!!!

In diesem Zusammenhang ist die Äußerung des **Geschäftsführers der Gematik**, Arno

Elmer interessant. Elmer überraschte Anfang 2013 in einer Diskussion betr. eGK mit der skeptischen Sichtweise: **"Wir bauen nur die Autobahn. Wenn der Gesetzgeber die Daten haben will, dann ändert er die Gesetze und holt sie sich."**

Quelle: http://www.heise.de/newsticker/meldung/Piratenpartei-diskutiert-elektronische-Gesundheitskarte-1797054.html

Weiterhin ist auch sehr interessant in diesem Zusammenhang die folgende Äußerung von Frau **Merkel am 5. 7. 2009** auf dem 60-jährigen Jubiläum der CDU: **"...denn wir haben wahrlich keinen Rechtsanspruch auf Demokratie und soziale Marktwirtschaft in alle Ewigkeit."** (Klingt das demokratisch???)

4. Für den Fall, dass die eGK mit dem geheimen Schlüssel abhandenkommt, **gibt es für die Gematik die Möglichkeit, den geheimen Schlüssel für die Patienten-daten wiederherzustellen.** Zwar verfügt die Gematik nicht selbst über die **"Nach-schlüssel",** sondern die damit beauftragte "Informationstechnische Servicestelle der gesetzlichen Krankenversicherung GmbH". Diese ist jedoch nicht ausreichend organisatorisch getrennt gehalten, um einen Zugriff durch Behörden oder Krankenversicherungen auf die Patientenakten mit absoluter Sicherheit ausschließen zu können.

Es gibt also Möglichkeiten ohne Wissen der Patienten auf die Daten der eGK zuzugreifen.

Quelle: http://www.ccc.de/de/elektronische-gesundheitskarte

5. **Ärzte im Ausland akzeptieren die Karte nicht.** Dies geht aus einer Umfrage der AOK Bayern und der Oberösterreichischen Gebietskrankenkasse hervor.
   Quelle: http://durchblick-gesundheit.de/content/red.otx/1175,85304,0.html

Dass die Gematik mit dem Betrieb der eGK-Dateninfrastruktur unter anderem ausgerechnet die Telekom-Tochter T-Systems beauftragt hat, weckte nach diversen Telekom-Datenskandalen zusätzliches Misstrauen. Dies bestätigen auch andere. **Wer im Angesicht von zwei Millionen Zugangsberechtigten glaube, so etwa Hartmut Pohl, Professor für Informatik, dass er einen Missbrauch der Daten ausschließen kann, „handelt naiv, fahrlässig oder will absichtsvoll täuschen".**

Quelle: eGk www.gen-ethisches-netzwerk.de - Patientendaten auf dem Präsentierteller

Selbst die **Gesellschaft für Informatik** warnt vor den Gefahren der zentralen Speicherung durch die eGK. **Eine sichere Speicherung der Daten im Internet sei nicht möglich.** Zitat der Gesellschaft für Informatik (GI): **„Die GI lehnt eine Speicherung von Gesundheitsdaten im Internet nachdrücklich ab“, ließ die IT-Fachgesellschaft schon 2009 verlauten. Denn „angesichts der Vielzahl Zugriffsberechtigter von etwa 80 Millionen dürfte eine hinreichend sichere Zugriffskontrolle überhaupt nicht machbar sein.“**
Quelle: http://www.freie-aerzteschaft.de/content/articles/1021/1022/index.html?catid=1022&artid=152603&topid=1021&nosum=1

Mit anderen Teilen der eGK-Infrastruktur hat die Gematik die Firma Atos Worldline betraut, die damit wirbt, dass sie "die gesamte Wertschöpfungskette der eGK-Mehrwertanwendungen abdecken" könne. **Peinlich nur, dass Atos Worldline als jenes Unternehmen Schlagzeilen machte, das Zehntausende abhanden gekommener unverschlüsselter Kreditkartendaten der Landesbank Berlin bearbeitet hatte.**

Das Interesse der Ärzte an einer lückenlosen Dokumentation und das Interesse der Patienten an informationeller Selbstbestimmung sind nicht zu vereinbaren. **Eine nutzbringende und rechtlich korrekte zentrale medizinische Akte ist daher nicht möglich.**

2. Datenunsicherheit bei einer zentralen Speicherung durch:

a) INNENTÄTER (die weitaus größere Gefahr) und
b) AUSSENTÄTER

Zu 2 a) INNENTÄTER (die unterschätzte Gefahr)
Nach den aktuellen IBM-Sicherheitsstudien (Juni 2015) sind NICHT professionelle Hacker die größte Gefahr für die Unternehmens-IT, sondern Insider. Von Outsidern ohne Zugriffsrechte kommt nur weniger als die Hälfte aller Attacken (45 Prozent).
Quelle: http://www.heise.de/newsticker/meldung/IBM-Sicherheitsstudien-Cyberattacken-aus-den-eigenen-Reihen-am-haeufigsten-2715977.html

1. **Die genaue Anzahl der Personen**, die tatsächlich, ob berechtigt oder nicht, Zugriff auf die zentralen Daten haben, ist **nicht bekannt** und **kann auch niemals korrekt ermittelt werden. U. a. sorgt der Gesetzgeber mit § 291 a, Abs. 4, 5 und 5a Satz 1 selbst dafür.** Dort heißt es sinngemäß: „Inhaber von Heilberufs- oder Berufsausweis

dürfen folgenden Personen den Zugriff auf Patientendaten erlauben: **berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätige Personen, (z. B. Angestellte, Praktikanten, Zeitarbeiter),** *„soweit dies im Rahmen der von ihnen zulässigerweise zu erledigenden Tätigkeiten erforderlich ist und der Zugriff unter Aufsicht der Ausweisinhaber erfolgt:“* In der Praxis sieht das dann so aus, daß einmalig eine Erlaubnis auf unbestimmte Zeit erteilt wird, da obige Personen nicht ständig vom Arzt beaufsichtigt werden können. Anders ist ein ärztlicher Betriebsablauf auch gar nicht möglich. **Nach § 291 a, Absatz 5a, Satz 2 Nr. 1 und 2 darf sogar OHNE EINWILLIGUNG der Versicherten auf deren Daten zugegriffen werden.** (Wird dann „versehentlich“ aus einem Organspendeverweigerer ein Organspender?)

2. **Die ärztliche Schweigepflicht wird durch die zentrale Speicherung praktisch aufgehoben**

Quelle: http://www.stoppt-die-e-card.de/index.php?serendipity[subpage]=downloadmanager&thiscat=2&file=57
(S E H R L E S E N S W E R T)

3. **Dem Patienten entstehen persönliche Nachteile:**

a) bei der Arbeitsplatzsuche, wenn z. B. künftige Arbeitgeber im Bewerbungsgespräch vom Bewerber verlangen, „mal eben freizuschalten“ („Machtmissbrauch“) und der Personalchef schweigend einen Eintrag als nachteilig beurteilt, kann das Gespräch für den Bewerber schon beendet sein – bei seiner Weigerung sowieso.

b) Sind dann meine Daten durch Missbrauch, menschliches Versagen oder technische Fehler verändert, kann das eine künftige Anstellung ebenfalls verhindern. (Sollte der Arbeitgeber z. B. ein Konzern o. ä. sein, muss der Bewerber auch noch mit einer internen „schwarzen Liste“ rechnen und wird von allen konzernzugehörigen Firmen abgelehnt.

Quelle:http://www.stoppt-die-e-card.de/index.php?serendipity[subpage]=downloadmanager&thiscat=2&file=57 – Seite 14 – 16

c) Gefahr für Leib und Leben, wenn zentral gespeicherte Daten nachträglich manipuliert werden, z. B. Zwangseinweisung in die Psychiatrie oder Tod durch falsche Medikamente usw.

Quelle: http://www.stoppt-die-e-card.de/index.php?serendipity[subpage]=downloadmanager&thiscat=2&file=57 – Seite 14 – 16

d) Nachteile bei der (Kranken-) Versicherungssuche, z. B. Ablehnung, weil angeblich ein um 2 % höheres Risiko besteht, einer teuren Krankheit zum Opfer zu fallen, eben weil die Vergleichsgruppe in den Datensätzen dieses aussagt – bzw. der Algorithmus, der von irgendwelchen Programmierern nach irgendwelchen unbekannten Vorgaben mit einer nicht näher bekannten Fehleranfälligkeit implementiert wurde.

4. Gefahr für die öffentliche Sicherheit und Ordnung durch Missbrauch zentral gespeicherter Patientendaten.

Mitglieder der Regierung, Opposition, Justiz, Polizei, Verwaltung, Behörde usw. könnten mit der Drohung der Veröffentlichung der (gefälschten) Patientendaten erpresst werden. *(So ein Minister, Präsident, Direktor, etc. wird sicher schnell gefügig, wenn er erst mal überzeugt wurde, dass er demnächst über seine psychoneurotischen Reaktionen (F 48.9), Verlust der Kontrolle Anus (R 15), Verwirrtheit (F 23.9), Pädophilie (F 54.4) oder Alkoholabhängigkeit (F10.2) etc. in der Zeitung, bzw. Internet lesen kann oder gefälschte Gesundheitsdaten zum Verlust seiner lieben Angehörigen führen können)*

Quelle: http://www.stoppt-die-e-card.de/index.php?
serendipity[subpage]=downloadmanager&thiscat=2&file=57 – Seite 14 – 16

In England war es fast soweit: (Nach heftigen Protesten vorerst wieder aufgegeben)
Die englische Zeitung „The Guardian“ verkündete am 20. 1. 2014: **die Patientendaten aller Briten werden verkauft.** Versicherungsunternehmen, Pharmakonzerne u. a. sollen künftig Patientendaten der gesamten britischen Bevölkerung kaufen können.
Eine einfache Gesetzesänderung genügt, und hier in Deutschland passiert dasselbe, sobald die Daten zentral gespeichert sind. (Nachdem diverse Regierungen seit Bestehen das Grundgesetz **56 mal** geändert haben, dürfte diese Änderung eine Kleinigkeit sein. Dies hat der Geschäftsführer der Gematik, Arno Elmer Anfang 2013 ja schon angedeutet.
Bei Heise-onine ist übrigens zu lesen, dass die britische Regierung das englisches Modell der e-GK inzwischen gestoppt hat, obwohl bereits 12,7 Milliarden englische Pfund (14,5 Milliarden €) in dieses Projekt investiert wurden und noch weitere Zahlungen trotz Stopp zu erwarten sind.

Quellen: http://www.heise.de/newsticker/meldung/Grossbritannien-will-Patientendaten-sammeln-und-weiterverkaufen-2090164.html
und

http://www.heise.de/newsticker/meldung/Britischer-Gesundheitsdienst-kippt-milliardenschweres-IT-Projekt-1349236.html

Zu 2 b: AUSSENTÄTER:

Die Speicherung von Patientendaten soll nicht auf der EGK erfolgen, sondern in der Telematik-Infrastruktur, d.h. auf Rechnern, die über das Internet miteinander verbunden sind, verschlüsselt natürlich. Endlose Skandale (nicht nur) im Bankbereich (CDs mit Schweizer Schwarzgeldkonten) zeigen, dass eine sichere, zentrale Speicherung von Massendaten nicht möglich ist, auch nicht unter Androhung langjähriger Gefängnisstrafen. Die Enthüllungen durch Edward Snowden haben zudem deutlich gezeigt, dass es keine Datensicherheit mehr gibt, auch keine sichere Verschlüsselung. (Sogar die Telefone von Angela Merkel und Gerhard Schröder wurden abgehört.)

Quelle: http://www.heise.de/newsticker/meldung/NSA-Ueberwachungsskandal-Lauschangriff-auf-Gerhard-Schroeder-2105599.html

Weder die Bundesregierung, noch sonst jemand kann Datensicherheit garantieren:

1. **In ihrer Regierungserklärung vom Jan 2014 hat Frau Merkel erklärt, sie hätte keinen Hebel um die Geheimdienstpraktiken der USA gegen Deutschland zu beenden.** Sie hat damit zugegeben, dass sie als Kanzlerin nicht in der Lage ist, die Spionage der USA gegen Deutschland zu beenden. (Verträge können gekündigt werden, falls man die Souveränität besitzt - was für Deutschland aber nicht zutrifft.)
2. **Bestätigt wurde ihre Aussage** durch die von **Herrn Schäuble**, der vor dem europäischen Bankenkongress 2011 in Frankfurt folgendes aussagte: *„Die Souveränität der europäischen Nationalstaaten sei ohnehin nur ein Relikt der Vergangenheit.“* Und er sprach etwas aus, woran Deutsche selten erinnert werden: **„Und wir in Deutschland sind seit dem 8. Mai 1945 zu keinem Zeitpunkt mehr voll souverän gewesen!“**
   Quelle: http://www.theintelligence.de/index.php/politik/eu-europaeische-union/3592-schaeuble-deutschland-ist-kein-souveraener-staat.html
3. **Bestätigt werden obige Aussagen** weiterhin durch den Freiburger Historiker Josef Foschepoth. Er hat durch **Dokumente aus dem Bundesarchiv** in Koblenz nachgewiesen, **dass den 4 Siegermächten** des 2. Weltkrieges in Geheimverhandlungen **die Spionage erlaubt wurde**. Adenauer hat 1955 durch „Vorbehaltsrechte“ garantiert, dass die ausländischen Geheimdienste vor der Strafverfolgung geschützt sind.

(Siehe auch Forschepoths Buch: *„Überwachtes Deutschland“*). **Straffreie Spionage in Deutschland (politisch, wirtschaftlich und militärisch) wird also den Geheimdiensten der USA und England (wem noch?) vertraglich garantiert** und die Bevölkerung darf ausspioniert werden.

Quelle: http://www.heise.de/newsticker/meldung/30C3-Die-ueberwachte-Bundesrepublik-2072768.html

4. **Bestätigt werden obige Aussagen indirekt durch** den früheren Präsidenten des Bundesverfassungsgerichts Hans-Jürgen Papier. *„Wenn der Staat seine umfangreichen Schutzpflichten gegen anlasslose Massenüberwachung der Bürger durch Geheimdienste nicht erfüllt, müssen die Rechtsgarantien gerichtlich einklagbar sein.“ (*Das Bundesverfassungsgericht hat Papier zufolge bereits angedeutet, *"dass Unterlassungen von Schutzpflichten einklagbar sein können"*.)
   Quelle: http://www.heise.de/newsticker/meldung/Ex-Verfassungsrichter-Schutz-vor-Massenueberwachung-notfalls-einklagen-2480212.html
5. **Bestätigt werden obige Aussagen durch** das ZDF-Magarzin **„Frontal“.**
   Nach Recherchen von Frontal21 erlaubte das Auswärtige Amt in den Jahren 2011 und 2012 über 110 US-Firmen die nachrichtendienstliche Auswertung von Datennetzen, darunter auch **Booz Allen Hamilton,** die die Bundesregierung zum Personalausweis und der eGK „berät“. **Aktuell** (Okt. 2014) **sollen in Deutschland 44 Verträge mit Geheimdienstfirmen bestehen – Spionage legal? Es dürfte wohl nur eine Frage der Zeit sein, bis so ein Vertrag auch für die zentral gespeicherten Patientendaten durch die eGK den Mißbrauch „legalisiert“ – ohne das Parlament damit zu behelligen.** (Falls er nicht schon existiert.)
   Quellen: http://www.zdf.de/frontal-21/auf-horchposten-in-deutschland-bundesregierung-duldet-us-spione-35515148.html
   und
   http://www.heise.de/newsticker/meldung/NSA-Skandal-US-Unternehmen-duerfen-in-Deutschland-ueberwachen-2428984.html

   Nachdem die Bundesregierung (nicht nur) US-Firmen per Vertrag die Datenspionage in Deutschland erlaubt hat, ist jede Beteuerung, daß die zentral gespeicherten Patientendaten sicher sind, mehr als unglaubwürdig.

   Quelle: http://www.heise.de/newsticker/meldung/NSA-Skandal-US-Unternehmen-duerfen-in-Deutschland-ueberwachen-2428984.html

6. **Bestätigt werden obige Aussagen durch den US amerikanischen Präsidenten Barack Obama am** 5. Juni 2009 während eines Besuchs auf dem US-Luftwaffen-

stützpunkt Ramstein. Er sagte dort vor amerikanischen Soldaten: ***"Deutschland ist ein besetztes Land und wird es auch bleiben".*** **Weiterhin sagte er dort:** *"Es ist wichtig zu verstehen, man kann nicht 100 Prozent Sicherheit und gleichzeitig 100 Prozent Privatsphäre haben."* ***„Der Staat muss alles über jeden wissen*****, fügte er hinzu, speziell was über das Internet abläuft...“**

7. **Antispy-Abkommen gescheitert.** Nach einem Bericht der New York Times (Dez. 2013) verweigern die USA übrigens den Abschluss eines Anti-Spionage-Abkommens mit Deutschland. (US-Sicherheitsberaterin Susan Rice bei Gesprächen in Berlin) ***(Anti-Spy-Abkommen: „Die NSA verspricht auch ganz lieb zu sein“)***
   Quelle: http://www.heise.de/newsticker/meldung/USA-verweigern-offenbar-Anti-Spionage-Abkommen-mit-Deutschland-2067078.html

8. **Bestätigt werden obige Aussagen indirekt:**
   Zum Thema eGK läßt sich die Bundesregierung von Firmen beraten, die mehr als ungeeignet sind dafür, darunter auch sehr NSA-nahe!
   Quelle: http://www.iknews.de/2013/12/19/egk-und-medizinische-daten-freie-fahrt-fuer-die-nsa-und-bertelsmann/

   Zum Einen die Booz & Company – einer Abspaltung aus Booz Allen Hamilton, einem führendem Unternehmen im Bereich der militärischen Dienstleistungen für das US-Verteidigungsministerium – des weiteren Arvato.

Zu Arvato gibt es einiges was, diametral den Interessen der Bürger und Patienten gegenübersteht und ein solches Unternehmen in derart sensible Bereich vordringen zu lassen, ist nahezu unglaublich. Einige kurze Zitate:

Über das Tochterunternehmen AZ Direct GmbH ist Arvato einer der bundesweit größten Anbieter im Adresshandel und Listbroking.
[...]
Parallel dazu hat der Mutterkonzern Bertelsmann SE & Co. KGaA ein Joint Venture mit der Deutschen Post AG, die Deutsche Post Adress GmbH & Co. KG. Über dieses Unternehmen werden u.a. die aus den Nachtsendeaufträgen der Deutschen Post AG stammenden Umzugsadressen vermarktet.
Mit dem Social Media Monitoring bietet Arvato online services Unternehmen an, die Kommunikation in relevanten Foren, Blogs und Communities zu beobachten und

über eine Beeinflussung zu beraten.

Die *Bundesregierung lässt sich von Booz beraten – kommt die NSA direkt in unsere kritische Infrastrukturen?* ***Der SPIEGEL*** *berichtet in seiner Ausgabe vom 18. 12. 2013,* ***dass das US-Beratungsunternehmen Booz jetzt unsere Bundesregierung „berät“:***

Für einen Auftragswert zwischen 16,5 Millionen und 19,5 Millionen Euro solle die Firma die Regierung bei „strategischen IT-Grundsatzentscheidungen und deren Umsetzung in die Praxis unterstützen“.

Die Secartis AG, eine Tochter des internationalen Technologiekonzerns Giesecke & Devrient (G&D), wird in den kommenden drei Jahren für die eGovernment-Initiative BundOnline 2005 der Bundesregierung gemeinsam mit der Unternehmensberatung Booz Allen Hamilton Konzepte und Lösungen erarbeiten, um Behördengänge per Mausklick sicher zu gestalten.[2]

Einige Zeilen zu Booz Allen Hamilton:

Nähe zum amerikanischen Geheimdienst:
In der Firma arbeiten verschiedene hochrangige Mitglieder aus den amerikanischen Geheimdiensten, *unter anderem der ehemalige Gesamtleiter (Director of National Intelligence), John Michael McConnell und der ehemalige CIA-Leiter James Woolsey. Während der umstrittenen Weiterleitung von Bankdaten der SWIFT an die amerikanischen und europäischen Geheimdienste war die Firma als Kontrollorgan involviert.* ***Laut dem Autor Tim Shorrock arbeiten über 1000 ehemalige Geheimdienstbeamte bei Booz Allen.***
Von den mehr als 24.000 Mitarbeitern verfügen drei Viertel über eine Sicherheitsfreigabe (security clearance). Knapp die Hälfte haben eine Freigabe für die Geheimhaltungsstufe Top Secret.[3]

Das ist das “who is who” der US-Geheimdienste. Von denen läßt sich die Bundesregierung „beraten“ zur „Datensicherheit“ bei Personalausweis und

eGK??? !!!

Nach einem Bericht im „Guardian“, der sich auf Daten Edward Snowdens beruft, hat **Microsoft der NSA Zugriff gewährt für seine Email-Dienste**, z. B. „Outlook.com, Hotmail und Live.“ **Microsoft hat das bestätigt**. **Außerdem hat Microsoft zugegeben, dem FBI Zugriff auf den Internettelefoniedienst Skipe ermöglicht zu haben**. **Lt. Snowden sei Skype bereits 2011 an Prism angeschlossen.**

Quelle: http://www.welt.de/politik/ausland/article117971277/Microsoft-soll-Zugriff-auf-Outlook-ermoeglicht-haben.html

Das die Datenspione der NSA mit an Sicherheit grenzender Wahrscheinlichkeit bereits illegalen Zugang zu allen Windows-Betriebssystemen haben, gibt Microsoft indirekt selbst zu. **Microsoft habe erstmals bestätigt, dass es bei der Softwareentwicklung mit dem US-Geheimdienst NSA kooperiert habe,** wolle aber keine Details nennen. Dem Bericht nach hatte das Redmonder Unternehmen bereits vor vier Jahren die NSA um Gutachten für Windows XP und Windows Server 2003 ersucht. Microsoft habe auch mit anderen, nationalen wie internationalen Behörden und Organisationen einschließlich der NATO kooperiert, wird ein Microsoft-Mitarbeiter zitiert.

Quelle: http://www.heise.de/newsticker/meldung/Bericht-NSA-half-Microsoft-bei-der-Vista-Entwicklung-132473.html

Obige Aussagen werden indirekt bestätigt durch den **NSA-Key in der Registry von Windows**. Nach den Enthüllungen von Edward Snowden kann es allerdings als gesichert gelten, dass die NSA einen geheimen Zugang zu Windows-Systemen hat und somit jede Verschlüsselung umgehen kann.

Quelle: http://www.pcwelt.de/news/Skandalumwittert-Der-NSA-Key-in-Windows-322794.html

Weiterhin sollte folgendes zu denken geben:

Das ein weltweit genutztes Betriebssystem von Microsoft in Zeiten der Überwachung ein "gefundenes Fressen" für allerlei Spionage und Überwachungstätigkeiten ist, sollte jedem klar sein. Wer z. B. beim Betriebssystem von Microsoft 'Vista' die Lizenzvereinbarungen anklickt und damit auch rechtswirksam akzeptiert, sollte doch etwas vorsichtig sein.

Hier ein paar Auszüge aus dieser Lizenzvereinbarung:

"Der Benutzer stimmt zu, daß sich Vista regelmäßig mit Microsoft verbindet, ohne im Einzelfall den Benutzer auch nur davon zu unterrichten und Informationen über den PC und die installierte Software zu übermitteln." (und was sonst noch???)

(EULA=Endbenutzer-Lizenzvertrag, Punkt 7)

"Bei Vista soll der Benutzer nicht mehr nur auf Updates verzichten, falls die "Überprüfung" fehlschlägt. ***Microsoft behält sich vielmehr vor, das Betriebssystem bis hin zu Unbenutzbarkeit zu deaktivieren, wenn der Prozess scheitert "*** **(EULA, Punkt 5).**
"Mit der Benutzung von Windows Vista stimmt man zu, dass Microsoft via "Windows Defender" ohne jede Nachfrage "potenziell unerwünschte Software" vom Rechner entfernt, auch wenn dadurch andere Software auf dem Computer nicht mehr funktioniert oder deren Lizenzbestimmungen verletzt werden." Das kann durchaus auch Software betreffen, die vom Benutzer gar nicht unerwünscht ist, räumt Microsoft unumwunden ein.(vgl.*www.linux-user.de*) Dies gilt auch für Windows 7 und 8. (Und was tut Microsoft noch alles ohne Wissen der Benutzer???)

Lt. der Tageszeitung Washington Post **gibt Microsoft erstmals zu, dass es bei der Softwareentwicklung mit dem US-Geheimdienst kooperiert habe. Microsoft habe auch mit anderen, nationalen wie internationalen Behörden und Organisationen einschließlich der NATO kooperiert,** wird ein Microsoft Mitarbeiter zitiert.
Quelle: http://initiative.cc/Artikel/2007_06_19_Kurz_notiert.htm

Wie lächerlich einfach heute schon Datenmissbrauch mit Patientendaten (auch mit der eGK) möglich ist, belegen allein diese beiden Beispiele:

1. **Mit einem Anruf und einem Brief** war es möglich, sich im Internet Zugang zu Patientendaten eines gesetzlich Versicherten zu verschaffen.
   Quelle: http://www.rp-online.de/wirtschaft/unternehmen/so-wird-meine-krankenversicherung-gekapert-aid-1.4341498

Beim Anruf bei einer bekannten Hamburger gesetzlichen Krankenkasse (bzw. deren Callcenter) reicht der Hinweis, dass die Versichertennummer gerade nicht zur Hand ist. **Dann genügt das Geburtsdatum für die Auskunft !!!**

Dasselbe Ergebnis kam bei einem **Test Juni 2015** heraus. Nach Recherchen des **ZDF-heute-journals** sind sensible Patientendaten von Millionen Deutschen nicht sicher. Die AOK bzw. deren Callcenter prüfte NICHT die Identität des Anrufers. Mit diesem Ergebnis konfrontiert, antwortete die AOK: "(…) ***Im Sinne kundenorientierter Prozesse müssten***

Krankenkassen im Rahmen einer vertrauensvollen Kundenbeziehung Postadressen grundsätzlich als wahr annehmen können (…)“. **???!!!**

Quelle: http://www.heute.de/massive-datenschutzluecke-bei-elektronischer-gesundheitskarte-38542206.html

2. **Eine gesetzliche Krankenkasse, die BKK VBU stellte eine ECHTE eGK mit dem Bild des Krümelmonsters aus der Sesamstraße aus !!! Die Echtheit wurde bestätigt!**

   Quelle: https://diedatenschuetzerrheinmain.wordpress.com/2014/04/17/bkk-vbu-stellt-elektronische-gesundheitskarte-mit-foto-des-krumelmonsters-her/

D I E S E K A R T E I S T E C H T !!!

Weitere Belege für die Unsicherheit zentraler Daten:

Dass Verantwortliche (nicht nur aus der Politik) oft gar nicht wissen, wovon sie reden, und damit eine direkte Gefahr für jede Datensicherheit sind, belegen folgende Beispiele:

1. **Windows XP noch auf Dreiviertel der Rechner im Bundestag !!!**

   Viele Bundestagsabgeordnete müssen vom 9. April 2014 an die Computer in

ihren Büros in Berlin oder den Wahlkreisen voraussichtlich mit einem *erhöhten* Sicherheitsrisiko betreiben.

Quelle: http://www.heise.de/newsticker/meldung/Windows-XP-noch-auf-Dreiviertel-der-Rechner-im-Bundestag-2104836.html

Wie ein Sprecher der Bundestagsverwaltung Heise-online (4. 2. 2014) mitteilte, laufen von den ihr unterstehenden Rechnern noch 75 Prozent unter Windows XP. Microsoft wird den Support für das 2001 eingeführte Betriebssystem ab 9. 4. 2014 endgültig einstellen.

Immerhin ist seit 2003 (!) bekannt, dass es für XP ab dann keine Sicherheits-updates mehr geben wird – Heute, 1 Jahr später hat sich nichts geändert.

Die Berliner Verwaltung hat mit Microsoft für **300.000 €** einen verlängerten Support vereinbart. **Dieser lief am 14. April 2015 aus.** Lt. Berliner Senat sollen im März 2015 noch 28.477 Rechner mit XP laufen, jetzt OHNE Support. Wieviele Rechner es wirklich sind, ist nicht bekannt !!! ...und **300.000 € Steuergelder, die z. B. dringend für die Renovierung von Schulen gebraucht wurden, sind verschleudert.**

Quelle: *http://www.heise.de/newsticker/meldung/Datenschuetzer-Dix-Behoerden-Pcs-mit-Windows-XP-sofort-abschalten-2600693.html*

Solche Leute reden von „Datensicherheit“ bei der eGK!

2. **Datenklau im Gesundheitsministerium** (INNENTÄTER)

Nach einem Bericht des Spiegel (Dez. 2012) hat ein externer IT-Mitarbeiter des Bundesgesundheitsministeriums **über mehrere Jahre hochsensible und vertrauliche Informationen gestohlen** – darunter sollen sich auch E-Mails der Minister Philipp Rösler und Daniel Bahr sowie ihrer engsten Mitarbeiter und Staatssekretäre befinden. Dreh- und Angelpunkt des Datenklaus soll ein freiberuflicher Lobbyist der Apothekerschaft sein, der so Beschlüsse, Gesetzesentwürfe und andere Daten für Gegenstrategien der Apothekenlobby nutzen konnte.

Er arbeitete für ein externes Unternehmen, dass für die IT-Struktur des Ministeriums zuständig ist. (INNENTÄTER)

Quelle : http://www.heise.de/newsticker/meldung/Datenklau-im-Gesundheitsministerium-1766905.html

Der damalige **Gesundheitsminister** Daniel Bahr (FDP) hatte Ende 2012 berichtet, interne Informationen aus seinem Haus, die ihn selbst noch gar nicht erreicht hätten, seien bereits im Internet zum Download angeboten worden.

Quelle : http://www.heise.de/newsticker/meldung/Datenklau-im-Gesundheitsministerium-1766905.html

Solche Leute reden von „Datensicherheit“ bei der eGK!

3. **Auch Ministerien vom massenhaften Passwortklau betroffen.**
   Nach einem Bericht des Spiegel Ende Jan. 2014 sind auch der Bundestag und alle Ministerien betroffen.

   Quelle: http://www.heise.de/newsticker/meldung/Bericht-Auch-Ministerien-von-massenhaftem-Passwortklau-betroffen-2104085.html

   Das BSI, die oberste Behörde für die IT-Sicherheit in Deutschland, hatte am **21. Januar 2014** mitgeteilt, dass **16 Millionen Benutzerkonten gekapert** worden seien, **obwohl sie bereits seit August 2013 davon wusste.**

   Solche Leute reden von „Datensicherheit“ bei der eGK!

4. **Systemadministrator stiehlt Patientendaten.** (INNENTÄTER)
   Jahrelang hat der Systemadministrator eines externen Datendienstleisters sensible Patientendaten auf private Festplatten kopiert. In dem Rechenzentrum werden zahlreiche Daten niedergelassener Ärzte, medizinischer Versorgungszentren und Apotheken verarbeitet. (Nov. 2013)

   Quelle: http://www.hna.de/lokales/northeim/systemadministrator-entwendete-patientendaten-staatsanwalt-ermittelt-3246933.html

   Soviel zur „Datensicherheit“ bei der eGK!

5. **95 % aller Geldautomaten laufen unter XP.**

   Anfang April 2014 ist nun endgültig "End of Life" für das bald 13 Jahre alte Betriebssystem und das bedeutet, es wird keine Systemaktualisierungen oder Hot-Fixes für Sicherheitslücken mehr geben.

   Ein Heise-Online vorliegendes Dokument der Deutschen Kreditwirtschaft über die zugelassenen Geldautomaten (Stand Ende November 2013) legt den Schluss nahe, dass praktisch alle Automaten in Deutschland mit Windows 2000 oder

Windows XP betrieben werden. Soviel zur „Datensicherheit.“!

Quelle: http://www.heise.de/newsticker/meldung/95-Prozent-aller-Geldautomaten-laufen-mit-Windows-XP-2088583.html

6. **Gefahr für die Unabhängigkeit der Justiz (und aller anderen Behörden) durch externe Dienstleister, z. B. Dataport.**

   Aus der Antwort des Justizministeriums Schleswig Holsteins (Jan. 2014) geht hervor, daß durch IT-Störungen der Geschäftsbetrieb erschwert und in den betroffenen Bereichen lahmgelegt wurde. Die Auslagerung birgt auch die Gefahren für die Unabhängigkeit der Justiz von Außeneingriffen und -einsicht. (Mögliche INNENTÄTER) Wenn das Land Regress wegen irgendetwas von Dataport gerichtlich einfordern würde – Dataport hätte Zugriff auf sämtliche Daten des Landes und der Justiz, aber auf die der Justiz hat sie ihn ohnehin.

   Quelle: http://www.heise.de/newsticker/meldung/Piraten-Abgeordneter-ruegt-IT-Stoerungen-bei-Schleswig-Holsteins-Justiz-2098458.html

   Solche Leute reden von „Datensicherheit“ bei der eGK!

7. **Karten mit Nullstellen-PIN.**

   Zwei Millionen Karten wurden an Versicherte von 55 Krankenkassen mit einer sogenannten Nullstellen-PIN vergeben, die auch Unberechtigten Einblick in alle Daten der Versicherten erlaubt**.** Sie mussten jetzt ausgetauscht werden.

   Quelle: http://www.golem.de/news/egk-klage-gegen-elektronische-gesundheitskarte-gescheitert-1206-92831.html

   Soviel zur „Datensicherheit“ bei der eGK.

8. **Patientendaten unverschlüsselt verkauft.**

   Nach einem Bericht des „Spiegel“ hat das Apothekenabrechenzentrum VSA **Patientendaten in unzureichend verschlüsselter Form u. a. an den US-Konzern IMS-Health verkauft, darunter 42 Milionen aus Deutschland.** Ebenso sei dabei allenfalls eine Pseudoanonymisierung erfolgt. Der Datenschutzbeauftragte Thilo Weichert hat das überprüft und bestätigt. (INNENTÄTER)

   Quellen: http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/rund-1-5-cent-je-rezeptdatensatz-rechenzentren-der-apotheken-verkaufen-patientendaten-

12536882.html
und
apothekenrechenzentrum-in-der-kritik-a-993106.html
Soviel zur „Datensicherheit“ bei der eGK!

9. **Callcentermitarbeiter speichern Patientendaten auf privaten Rechnern.**

   Das **ARD-Magazun „Kontraste“** hat ein Datenleck bei der BKK Gesundheit ans Licht gebracht, Deutschlands größter Betriebskrankenkasse. Sie gewährte Callcentermitarbeitern Zugriff auf intime Daten ihrer 1,5 Millionen Versicherten. Das externe Unternehmen hat wiederum einen anderen Dienstleister angeheuert, „Value Health Care“. **Deren Mitarbeiter hatten Zugriff auf intimste Daten und konnten diese sogar auf ihren privaten Rechnern abspeichern, wo sie die Daten auch bearbeitet haben (!)** (Mögliche INNENTÄTER)

   Quelle: http://www.durchblick-gesundheit.de/content/red.otx/1177,92716,0.html

   Soviel zur „Datensicherheit“ bei der eGK!

10. **Psychiatrieakten problemlos im Internet einsehbar.**

    Durch eine Panne waren April 2011 in Schleswig Holstein über einen längeren Zeitraum **ca. 4000 psychiatrische Patientenakten problemlos im Internet einsehbar. Gespeichert waren sie auf einem Server des IT- Dienstleisters Rebus GmbH.** (Mögliche INNENTÄTER)

    Quelle: http://www.freitag.de/autoren/philou-pfab/patientendaten-fuer-die-geheimdienste
    Soviel zur „Datensicherheit“ bei der eGK!

11. **Schengen-Informationssystem gehackt.**
    Beim Angriff durch 2 Hacker auf das Schengen-Informationssystem Ende 2013 wurden auch **272.606 Datensätze aus Deutschland gestohlen**. Die beiden hatten es nicht einmal auf die Schengendaten abgesehen, sondern einfach mit runtergeladen, weil sie „zufällig“ auf den Servern lagen. Die Behörden hätten davon nicht einmal etwas bemerkt, wenn sie nicht die Daten auf dem Rechner der Hacker gefunden hätten.

    Quelle: http://www.heise.de/newsticker/meldung/Angriff-auf-Schengen-Informationssystem-

272-606-Datensaetze-aus-Deutschland-betroffen-2088169.html

Solche Leute reden von Datensicherheit!

12. **DAK verkauft Patientendaten OHNE Einverständnis der Patienten.**

Bereits 2008 hat das ARD-Magazin „Report“ aufgedeckt, daß die DAK rund **200.00 Datensätze** mit vertraulichen Patientendaten an die Privatfirma „Healthways“ weitergegeben hat. Die betreffenden Patienten wurden anschließend von einem Callcenter in der Nähe Berlins „medizinisch beraten.“ **Die Firma „Healtsways“ sagte aus, dass die Daten ohne Einverständnis der Patienten an sie weitergegeben wurden. (**INNENTÄTER)

Quelle: http://www.focus.de/finanzen/versicherungen/krankenversicherung/krankenkasse-dak-gibt-patientendaten-weiter_aid_325837.html

Soviel zur „Datensicherheit“ bei der eGK!

Schutz der Versichertendaten bei Krankenkassen: Häufig mangelhaft bis ungenügend

Das Bundesversicherungsamt (BVA) – die Aufsichtsbehörde für die über die bundesunmittelbaren Träger der gesetzlichen Kranken-, Renten- und Unfallversicherung sowie der sozialen Pflegeversicherung – veröffentlicht jährlich einen Bericht über die Ergebnisse seiner Prüfungen. Vor wenigen Tagen (April 2015) erschien der Tätigkeitsbericht des BVA für 2013. **Was darin an Mängeln festgestellt wird, hat häufig die Note 5 (mangelhaft) oder gar die Note 6 (ungenügend)** verdient.

Quelle: http://ddrm.de/?p=4082

Soviel zur „Datensicherheit“ bei der eGK!

13. **Künftige Gesetzesänderung**

Niemand kann garantieren, dass ein künftiger Gesetzgeber irgendwann den Datenschutz aufweicht (das hat er früher auch schon getan, z. B. beim umstrittenen BKA-Gesetz), oder von der EU dazu „gezwungen“ wird. (Dass dies möglicherweise geplant ist, ergibt sich aus der Aussage des Geschäftsführers der Gematik, Arno Elmer, der in einer Diskussion Anfang 2013 sagte: ***"Wir bauen nur die Autobahn. Wenn der Gesetzgeber die Daten haben will, dann ändert er die Gesetze und holt sie sich.“***

Quelle: http://www.heise.de/newsticker/meldung/Piratenpartei-diskutiert-elektronische-

Gesundheitskarte-1797054.html

Und wie sagte doch Frau Merkel am 5. 7. 2009: ***„...denn wir haben wahrlich keinen Rechtsanspruch auf Demokratie und soziale Marktwirtschaftlich in alle Ewigkeit.“***

14. **Wenn etwa** nach einem Gewaltverbrechen an einem Kind (angebliche oder tatsächliche) Tatortspuren auf eine seltene Krankheit (oder ähnliches) des Täters hinweisen sollten, wird es ganz schnell eine Diskussion über einen Zugriff auf die entsprechenden Daten zur Strafverfolgung geben. Dabei wird niemand prüfen (können), ob die Behauptung auch stimmt oder nur als Vorwand dient. Und wenn erst einmal eine Behörde auf die Daten zugreifen kann, werden andere bald folgen.

15. **Wieder massive Cyberspionage nachgewiesen.**

    Nach einem Bericht in Heise-online vom 14. 1. 2013 hat das Sicherheitsunternehmen Kaspersky massive Cyberspionage nachgewiesen. **Danach werden seit 5 Jahren Rechnernetzwerke von diplomatischen Vertretungen, Regierungs- und Handelsorganisationen, Energiekonzerne, sowie Einrichtungen der Forschung, der Luftfahrt und des Militärs infiltriert.** Über eine ausgeklügelte Infrastruktur konnten die unbekannten Hacker vermutlich Terabyte an geopolitischen Informationen und Daten höchster Vertraulichkeit erbeuten. **Das System soll derzeit noch aktiv sein und Daten an die C&C-Server senden.**

    Quelle: http://www.heise.de/newsticker/meldung/Operation-Roter-Oktober-Massive-Cyberspionage-aufgedeckt-1783457.html

Die Liste läßt sich bis heute beliebig fortsetzen mit hunderten ähnlicher massiver Datenpannen und -skandalen. Jede Woche tauchen neue auf.

Hier noch einige aufgedeckte Beispiele für massive und gezielte Datenspionage, wie sie heutzutage i. d. R. von Geheimdiensten angewandt werden: (Das sind nur die bekannten**!**)

1. **„Stuxnet-Virus“ -** wurde und wird verwendet um hochgesicherte Industrie-komplexe, wie z. B. Atomkraftwerke oder Wasserwerke usw. gezielt zu sabotieren.
   Quelle: http://www.heise.de/security/meldung/Das-Stuxnet-Duo-Boesartige-Geschwister-2053847.html

2. **„Roter Oktober“ -** zur gezielten Infiltrierung von diplomatischen Vertretungen, Regierungs- und Handelsorganisationen, Energie-Konzernen sowie Einrichtungen der Forschung, der Luftfahrt und des Militärs .

   Quelle: http://www.heise.de/newsticker/meldung/Operation-Roter-Oktober-Massive-Cyberspionage-aufgedeckt-1783457.html

3. **„MiniDuke“ -** zielt gegen Regierungen, um in den Besitz vertraulicher politischer Informationen zu gelangen. **MiniDuke überwindet erstmals auch modernste Sicherheitsverfahren, wie z. B. die „Sandbox“ -**

   Quelle: http://info.kopp-verlag.de/hintergruende/deutschland/redaktion/miniduke-neue-cyberangriffe-zielen-gegen-regierungen-um-in-den-besitz-vertraulicher-politischer-in.html

4. **„Regin“ -** bisher *"am schwersten zu fassenden und ausgefeilte Spyware“* zur Überwachung von Mobilfunknetzen, Regierungseinrichtungen sowie internationale politische Gremien, Providern, Forschungsorganisationen, Finanzinstitute sowie Individuen in verschiedenen Ländern. Regin ist offensichtlich auch heute noch aktiv.

   Quellen: http://www.heise.de/newsticker/meldung/GCHQ-und-NSA-stecken-angeblich-hinter-ausgefeilter-Spyware-Regin-2463042.html

Weitere bekannte Methoden der NSA für Datenspionage: (Die richtig fiesen kommen zum Schluss - Sollte also jemand meinen, hier bei „uns im Haus“ passiert sowas nicht...)

1. **Injizieren von Schadcode über WLANs aus mehreren Kilometer Entfernung** (Projekt "Nightstand")
2. **Abfischen von Bildschirm- und Tastaturdaten per Radar** (Tempest-Verfahren, Projekt "Ragemaster")
3. **Abfischen von Tastatureingaben per Radar** (Projekt "Surlyspawn")
4. **Eingebaute „Hintertür“ in iPhones**

   Quelle für Nr. 1 – 4: http://www.heise.de/newsticker/meldung/30C3-Neue-tiefe-Einblicke-ins-Schreckenskabinett-der-NSA-2073078.html

5. **Abgreifen von PIN- und Tastatureingaben an der Steckdose !!!**

   Quelle: http://www.heise.de/ix/meldung/Black-Hat-PIN-an-der-Steckdose-abgreifen-748865.html

6. **Manipulierte Computermäuse** (auch in Originalverpackung)

Quelle: http://www.heise.de/newsticker/meldung/Angriff-der-Computer-Maus-1269684.html

7. Die **NSA** fängt "manchmal" Server, Router und andere Netzwerkgeräte ab, die aus den USA verschickt werden, **öffnet die Pakete und installiert Spyware, bevor sie per Post weitergeschickt werden.** Dies geht aus Ausschnitten von NSA-Dokumenten hervor, die diesen Eingriff in den Postversand erläutern.

   Quelle: http://www.heise.de/newsticker/meldung/NSA-manipuliert-per-Post-versandte-US-Netzwerktechnik-2187858.html

8. Neuen Dokumenten von Edward Snowden zufolge greifen NSA-Agenten nicht nur in den USA Postsendungen ab, um sie zu manipulieren, sondern wohl auch in Deutschland. Zur Sprache kommt unter anderem **ein Programm namens "TAREX"** zu dem auch der **"Eingriff in Lieferketten"** gehört. **Die NSA hat offenbar auch in Deutschland Agenten stationiert, die beispielsweise Postsendungen abfangen und darin enthaltene Netzwerktechnik manipulieren,** bevor sie an ihr eigentliches Ziel weitergeleitet wird. Die Enthüllung lässt einen Wechsel auf vermeintlich sichere Technik, etwa aus Deutschland, in einem anderen Licht erscheinen. (Wissen SIE, ob Ihre EDV garantiert „NSA-freie“ Bauteile enthält??? Nein, das können weder SIE noch sonst jemand.)

   Quelle: http://www.heise.de/newsticker/meldung/NSA-sabotiert-offenbar-auch-direkt-in-Deutschland-2415559.html

9. Das **NSA-Programm "Sentry Eagle"** ("Wachadler") umfasst auch **Undercover-Agenten der NSA** bei US-amerikanischen und eventuell auch ausländischen Unternehmen. Dabei handle es sich um Angestellte, von denen niemand im Unternehmen wisse, dass sie eigentlich für den Staat/NSA arbeiten. **Die könnten etwa an besonders vertrauliche Daten gelangen wie z. B. zentral gespeicherte Patientendaten oder private Kryptographie-Schlüssel.**

   Quellen: http://www.heise.de/newsticker/meldung/NSA-sabotiert-offenbar-auch-direkt-in-Deutschland-2415559.html und
   https://tarnkappe.info/sentry-eagle-nsa-sabotiert-gezielt-deutschland/

10. Zu "Sentry Eagle" gehöre auch ein **Programm namens "Sentry Raven"** („Wachrabe"). Laut der Beschreibung arbeitet die NSA dabei mit "bestimmten US-Konzernen zusammen, **um Kryptographie-Systeme aus den USA für die Überwachung nutzbar zu machen".** (Der Konzern RSA hat in diesem Zusammenhang Geld er-

halten, um ein Verschlüsselungsprogramm zu schwächen. **Er bestätigt gleichzeitig, daß Verschlüsselungssystemen aus den USA nicht vertraut werden kann.**

Quelle: http://www.heise.de/newsticker/meldung/NSA-sabotiert-offenbar-auch-direkt-in-Deutschland-2415559.html

Aber auch in Fällen, wo die NSA nicht weiterkomme oder ihr rechtliche Grenzen gesetzt seien wie etwa bei Gmail, blieben keine überwachungsfreien Zonen. Den Dokumenten von Edward Snowden zufolge **übernehme dann ihr britischer Partner GCHQ und übermittle im Erfolgsfall die gewünschten Daten zurück an den großen Bruder in den USA.**

Nach einer Allensbach-Umfrage 2011 hatten übrigens 2 von 3 deutschen Unternehmen schon Hackerbesuch.

Quelle: http://www.heise.de/newsticker/meldung/Zwei-von-drei-deutschen-Unternehmen-hatten-Hackerbesuch-1345208.html

Sogar die Server der Bundespolizei wurden gehackt, über ein Jahr lang unentdeckt. Dort waren 44 (!) Trojaner installiert.

Quelle: http://www.heise.de/security/meldung/Server-der-Bundespolizei-ausspioniert-1276055.html

Lt. Definition des BSG in seinem aktuellen Urteil vom Nov. 2014 hätte es so etwas doch gar nicht geben dürfen, da es ja lt. Gesetz verboten ist.

Auch zukünftige Verfahren sind heute schon unsicher:

Update – Dez. 2014 – Selbst Fingerabdrücke und Iriserkennung sind leicht zu umgehen.

Der Hacker Starbug zeigte auf dem Hackerkongress, wie man mit einer normalen Digitalkamera bei öffentlichen Veranstaltungen an Fingerabdrücke Dritter gelangen kann, um biometrische Authentifizierungssysteme zu überwinden. **Dazu reiche dafür schon die Aufnahme eines Fotos mit einer gängigen Digitalkamera aus einem Abstand einiger Meter aus.** Dies gilt sowohl für den Fingerabdruck wie auch für die Irisaufnahme.

Quelle: http://www.heise.de/newsticker/meldung/31C3-CCC-Tueftler-hackt-Merkels-Iris-und-von-der-Leyens-Fingerabdruck-2506929.html

Update – 20. Januar 2015 – GKV-Spitzenverband gibt öffentlich zu, daß es KEINE Datensicherheit gibt!

Am 20. 1. 2015 hat das ZDF in der Sendung **Frontal 21** beim GKV-Spitzenverband zum Thema Datenschutz bei der eGK nachgefragt: (Ab Minute 8.32 Uhr)

Frage:
„Wie wollen die Krankenkassen Datenmissbrauch mit der neuen Karte verhindern?“

Antwort des Sprechers, Florian Lenz:

„Wir wissen, dass in der Vergangenheit Fehler gemacht worden sind, dass nicht korrekt mit Daten umgegangen worden ist...

(Und ab Min. 8.50)

„Wir können nicht völlig ausschließen, dass an irgendeiner Stelle irgendwo jemand aus Versehen oder mit Absicht etwas mit Daten falsch macht.“

(Eine bemerkenswert ehrliche und außerdem die einzig richtige Antwort auf obige Frage)

Quellen:

http://www.stoppt-die-e-card.de/exit.php?url_id=706&entry_id=288

und

https://www.youtube.com/watch?v=WlEpaP-TY9g

Was für eine „Datensicherheit“ soll denn das sein, wenn sogar die Befürworter der eGK öffentlich zugeben, daß es gar keine Datensicherheit gibt und geben kann ???

Sollte also jemand an Ihre persönlichen Gesundheitsdaten gelangen, kommt das einem Identitätsdiebstahl gleich. Das kann bei kriminellem Ausnutzen existenzvernichtende Folgen haben.

Update 23. 2. 2015 – Firmware von Festplatten bekannter Hersteller manipuliert.

Vor einem Jahr haben SPIEGEL und SPIEGEL ONLINE über geheime NSA-Schadsoftware berichtet, die sich in der Firmware von Festplatten einnistet. Jetzt haben Experten solche Programme auf Hunderten Rechnern gefunden.

Die acht Schadprogramme sollen alle aus einer Hand stammen, die der **Equation-Gruppe. Wahrscheinlich seit 2001, vielleicht schon seit 1996 wurden dem Bericht zufolge von der Equation-Gruppe Tausende bis Zehntausende Computer infiltriert.**

Quelle: http://www.spiegel.de/netzwelt/web/equation-group-kaspersky-warnt-vor-manipulierter-festplatten-firmware-a-1018852.html

Diese Malware überlebt eine Formatierung der Festplatte oder Neuinstallation des Betriebssystems und sei nicht zu entdecken. Die einzige Methode, die Malware loszuwerden, sei die physische Zerstörung der Festplatte.

Zu den Opfern gehörten Regierungen und diplomatische Institutionen, Rüstungskonzerne, Forschungseinrichtungen, Massenmedien sowie Kryptographieentwickler.

Quelle: http://www.heise.de/newsticker/meldung/Equation-Group-Hoechstentwickelte-Hacker-der-Welt-infizieren-u-a-Festplatten-Firmware-2550779.html

Update 22. 2. 2015 –

Geheimdienste unterwandern SIM- und Kreditkarten und Sicherheitsvorkehrungen der Chipkarten-Hersteller ausgehebelt

Seit Jahren kopieren NSA und GCHQ bei den Herstellern von SIM-Karten und Smart Cards die zugehörigen Schlüssel ab. Damit können sie die übertragenen Informationen mitlesen und manipulieren.

Der Bericht von „The Intercept" konzentriert sich auf Gemalto, Weltmarktführer bei Chips für SIM-Karten und Zahlkarten. ***"GEMALTO – Erfolgreich mehrere Maschinen implantiert und wir glauben, dass wir ihr gesamtes Netzwerk haben",*** **frohlockte GCHQ schon 2010 in einer geheimen Präsentation.**

Übrigens manipulieren die Schnüffler auch die Abrechnungs-Server der Netzbetreiber. So können sie Daten und SMS zu und von fremden Endgeräten übermitteln, ohne dass es in den Rechnungsdaten erscheint. Weder Kunde noch Netzbetreiber merken, wie die Zielperson ausspioniert oder ihr Gerät aus der Ferne bearbeitet wird.

Warum Verschlüsselungen knacken, wenn man den Schlüssel hat?!

Marktführer Gemalto gilt also seit 2010 als gehackt.

Quelle: http://www.heise.de/newsticker/meldung/Geheimdienste-unterwandern-SIM-und-Kreditkarten-2555685.html

2012 hat Gemalto trotzdem weitere15 Millionen eGK für die AOK ausgegeben.

Quelle: http://www.pressebox.de/pressemitteilung/gemalto-gmbh/Gemalto-liefert-2012-weitere-15-Millionen-elektronische-Gesundheitskarten-fuer-AOK-Versicherte-aus/boxid/493440

Auch Gemaltos deutscher Mitbewerber *Giesecke & Devrient* (eGK) wird als Angriffsziel erwähnt, und es darf angenommen werden, dass in den vergangenen Jahren auch andere Hersteller dazugekommen sind.

Wenn nun Geheimdienste seit Jahren das gesamte Netz Gemaltos "pwnen", liegt es nahe, dass sie auch die dazu gehörenden Algorithmen und Schlüssel kopiert, **sowie Schwachstellen und Hintertüren eingebaut** haben.

Quelle: http://www.heise.de/newsticker/meldung/SIM-Karten-Hack-Die-Kompromittierung-der-Mobilfunknetze-durch-NSA-GCHQ-2555714.html

Dass der britische Geheimdienst GCHQ und die US-amerikanische NSA schon vor Jahren die Sicherheitsvorkehrungen der Chipkarten-Hersteller ausgehebelt haben, hat weitere Konsequenzen. Die gemeinsamen Einheit von GCHQ und NSA namens Mobile Handset Exploitation Team (MHET) soll Schwachstellen in Mobiltelefonen finden und auszunutzen sowie die internen Netzwerke der großen SIM-Karten-Hersteller, der großen Endgerätehersteller und vieler Netzbetreiber kompromittiert haben, wie der Intercept berichtet. **Mit einem Schlüssel kann auch die Übertragung gefälscht und verfälscht werden.**

Den Geheimdiensten erwachsen durch das Abfangen der elektronischen Schlüssel (Zertifikate), die auf jeder SIM-Karte fixiert sind, ungeahnte Möglichkeiten – dies reiht sich ein in die vor kurzem bekannt gewordenen Methoden der mit den Geheimdiensten in Verbindung gebrachten so genannten Equation-Group, (s. o.) die unter anderem Firmware von Festplatten manipuliert.

"Wenn bis heute dieses Datenleck den Betreibern der Firma nicht aufgefallen ist, bedeutet das, dass interne Kontrollen völlig versagt haben müssen. Es gibt also KEINE Sicherheit mit den jetzt ausgegebenen elektronischen Karten.“

"Der Nachweis dieser unbemerkten Angriffe ist der Super-GAU für das eGK-Projekt. Das zeigt, dass es die von der eGK-Betreibergesellschaft Gematik immer wieder behauptete Datensicherheit nicht gibt."

Aber es kommt noch schlimmer:

Update März 2015 – CSC (und damit NSA und GCHQ) in alle großen IT-Vorhaben der

Bundesregierung eingebunden.

Quelle: *https://netzpolitik.org/2014/interne-e-mails-csc-freut-sich-ueber-neue-vertraege-mit-behoerden-trotz-no-spy-erlass-und-medialen-anschuldigungen/*

Aus internen Mails der *CSC Deutschland Solutions GmbH* geht hervor, dass die Firma an allen großen IT-Vorhaben der Bundesregierung beteiligt ist. Philipp Müller, Public Affairs Director von CSC, hat telefonisch indirekt die Echtheit der E-Mails bestätigt:

> *„Wir finden, es gehört nicht zum guten Ton, interne E-Mails zu veröffentlichen."*
>
> Allein in den vergangenen vier Jahren der letzten Regierung unter Angela Merkel zwischen 2009 und 2013 bekam die CSC Deutschland **genau 100 Aufträge von zehn unterschiedlichen Ministerien und dem Bundeskanzleramt.**

Die Rahmenverträge zwischen der Bundesregierung und CSC enthalten eine *„No-Spy-Klausel"* (Auf deutsch: die Firma CSC hat unterschrieben ganz lieb zu sein).
Wenn alles ganz harmlos ist, warum verlangt das Innenministerium dann eine No-Spy-Klausel?

Dabei ist bekannt, daß diese Klausel unwirksam ist. Das bestimmt der PATRIOT Act.

„Die Bestimmungen des PATRIOT Act erlauben US-Behörden wie dem FBI, der NSA oder der CIA nicht nur den Zugriff ohne richterliche Anordnung auf die Server von US-Unternehmen. ***Auch ausländische Töchter sind nach dem US-Gesetz verpflichtet, Zugriff auf ihre Server zu gewähren; selbst dann, wenn lokale Gesetze dies untersagen."***

Quelle: http://de.wikipedia.org/wiki/USA_PATRIOT_Act#Auswirkungen_auf_den_Schutz_personenbezogener_Daten_und_geistigen_Eigentums

Lt. diversen amerikanischen Gerichtsurteilen dürfen Firmen noch nicht einmal zugeben von Geheimdiensten kontaktiert worden zu sein.

Die *CSC Deutschland Solutions GmbH* ist die Tochterfirma der *Computer Science Corporation (CSC).* Der CSC Konzern ist lt. Bundesgesetzblatt in Docper-AS-22-02 u. a. als Helfer *"bei nachrichtendienstlichen Analysen" für das US Militär* in Deutschland akkreditiert.

CSC ist einer der wichtigsten IT-Dienstleister des US-Geheimdienstes NSA

(praktisch die „EDV-Abteilung der NSA“), **u. a. an der Entwicklung von Späh-programen des US-Nachrichtendienstes beteiligt,** ebenso wie an Entführungen durch die CIA.

Quelle: http://www.sueddeutsche.de/digital/csc-deutschland-umstrittener-nsa-dienstleister-verliert-ausschreibung-1.2378310

Dieser Firma wird Zugang zu praktisch allen großen IT-Vorhaben der Bundes-regierung gewährt, auch zur eGK und neuem Personalausweis?!

„Und noch ein Hammer“ !!!

(„...aber das war ja zu erwarten“)

Update 9. 4. 2015 – Biotech-Verband will Daten der elektronischen Gesundheitskarte nutzen

Am 9. 4. 2015 war dazu bei heise.de und ddrm.de folgendes zu lesen:

BIO Deutschland e. V. ist kein Verein, der sich mit ökologisch erzeugten Lebensmitteln beschäftigt. Das wird deutlich, wenn der vollständige Name des Vereins genannt wird: **Biotechnologie-Industrie-Organisation Deutschland e.V.** Noch deutlicher wird der Zweck von BIO Deutschland e. V. beim Blick auf die Fördermitglieder des Vereins:

Der einzige Zweck dieser Unternehmen dürfte die Gewinnmaximierung sein. Die Verbesserung der Gesundheit des Menschen scheint nicht dazuzugehören (siehe auch **„Die Gesetze der Pharma-Industrie“** von Dr. Rath – **Quelle:** http://www4ger.dr-rath-foundation.org/GESCHAEFT_MIT_DER_KRANKHEIT/die_gesetze_der_pharma-industrie.html) (SEHR AUFSCHLUSSREICH)

Dieser Verband hat vor wenigen Tagen in einer Stellungnahme zum Entwurf für ein E-Health-Gesetz gefordert: *„Die Anwendungen der mit dem e-Health-Gesetz einzuführenden neuen elektronischen Gesundheitskarte beinhalten eine solche Datenbasis, die die forschenden Biotechnologie-Unternehmen effektiv unterstützen könnte. Nach der derzeitigen Ausgestaltung der elektronischen Gesundheitskarte ist den Unternehmen aber ein Zugriff auf diese Daten zu Forschungszwecken verwehrt…“* **Der Verein fordert deshalb erweiterte Zugriffsmöglichkeiten auf den durch die Telematik-Strukturen entstehenden Datenpool. Sie fordern aber auch für sich das Recht, unmittelbar in die Entscheidungsstrukturen der Gematik eingebunden zu werden**: *„Biotechnologie-Unternehmen müssen in die Entscheidungsprozesse im Hinblick auf die Telematikinfra-struktur und die elektronische Gesundheitskarte eingebunden werden, Einbeziehung von Bio-IT Experten bei der Erarbeitung von Interoperabilitätsstrukturen…“*

Ein unverhüllter Angriff auf die bisherigen Datenschutzregelungen im Sozialge-setzbuch!

Die Daten sind noch nicht einmal zentral gespeichert und schon will die Pharma-industrie sie nicht nur haben, sondern im Vorfeld schon mitbestimmen, wie das zu ihrem größten Vorteil zu geschehen hat.

Die in § 75 SGB X (Übermittlung von Sozialdaten für die Forschung und Planung) und § 287 SGB V (Forschungsvorhaben) enthaltenen Regelungen erscheinen den Firmen der Pharma- und Medizintechnik-Industrie als Hemmnis für ihre wirtschaftlichen Interessen. **Sie fordern mit Ihrer Stellungnahme von Bundesgesundheitsminister Gröhe einen unmittelbaren Zugriff auf die Gesundheits- und Behandlungsdaten der knapp 70 Mio. Menschen in der gesetzlichen Krankenversicherung.** Dieser Forderung muss entschieden entgegen getreten werden!

Die Patientenakte mag dem Arzt gehören, aber die Patientendaten gehören dem Patienten, niemand sonst !!!

ALLES andere hat KEINE Rechtsgrundlage!

Das Geld auf dem Konto gehört auch dem Kontoinhaber und nicht der Bank, und trotzdem ist das Geld auf der Bank und nicht beim Inhaber zu Hause. Die Pflicht der Bank ist es sein Geld sicher aufzubewahren und loyal dem Inhaber gegenüber damit umzugehen. In der Regel gilt: Jeder einzelne Mensch (und niemand anders) ist der Eigentümer seiner persönlichen Daten. Jeder andere (Unternehmen, Ärzte, etc etc) dürfen auf diese Daten nur mit der Erlaubnis jedes Einzelnen zugreifen und nutzen.

Bitte bedenken Sie:

- Die kostenlose (aber auch eine eventuelle kostenpflichtige) Bereitstellung von Patienten- und Gesundheitsdaten zum wirtschaftlichen Nutzen von Pharma- und anderen Unternehmen verletzt das Grundrecht auf informationelle Selbst-bestimmung und der freien Entfaltung der Persönlichkeit nach Art. 2 GG und auch gegen Art. 1 GG (Menschenwürde)
- Erfahrungen auch aus anderen Anwendungsbereichen machen deutlich: Auch anonymisierte oder pseudonymisierte Daten können – entsprechende Rechner-leistungen vorausgesetzt – leicht wieder re-anonymisiert werden.
- Und nicht zu vergessen: Bisher geht § 291a SGB V Elektronische Gesundheits-karte) davon aus, dass der Zugriff auf die Daten eines Patienten, die im telematischen System hinterlegt sind, in jedem Einzelfall (Notfalldaten ausgenommen) der vorherigen aktiven Zustimmung des betroffenen Menschen bedarf.

Wie lächerlich einfach Re-Anonymisierung ist, lesen Sie hier:
http://www.faz.net/aktuell/feuilleton/medien/metadaten-von-kreditkarten-keiner-bleibt-anonym-13398079.html

Weitere Interessenten werden mit Sicherheit folgen, offensichtlich oder heimlich, legal oder illegal. Stellen Sie sich mal die '"wunderbaren" Möglichkeiten mit zentral gespeicherten Patientendaten vor. **Durch gezielt manipulierte Gesundheits- und Behandlungsdaten** z. B. könnte:

1. JEDER (Entscheidungsträger) erpreßt werden, (z. B. mit dem Tod naher Angehöriger)
   - Polizisten, Zöllner, Bundesgrenzschützer, Offiziere,
   - Personenschützer,

- Staatsanwälte, Richter und Justiz-Mitarbeiter
- unsere Politiker,
- die Mitarbeiter des Bundeskanzleramtes,
- des Krisenstabs,
- der Generalstaatsanwaltschaft,
- des Bundesnachrichtendienstes,
- des Staatsschutzes und anderer Sicherheitsdienste usw.

2. Der Staat / Geheimdienste (auch ausländische) haben mit den Daten z. B. die Möglichkeit: (...um nur einige Möglichkeiten zu nennen)

- JEDEN potenziell unbequemen Menschen auf ewig in der Psychiatrie verschwinden zu lassen.oder die
- Risikolose Beseitigung (Ermordung) von Opposition, Regimekritikern o. a. missliebigen, „aufmüpfigen“ Personen (wer braucht denn dazu noch Drohnen, wie der Herr Obama?)
- Die Rentenkasse zu entlasten („Regulierung“ der Anzahl der Rentner nach unten), z. B. so: (das sind nur 3 Beispiele)

Nun stellen Sie sich einmal vor ...	**Bei (einzelnen oder missliebigen) Personen:**
richtig	falsch
Hypertonie (Bluthochdruck)	Hypotonie (Blutniederdruck)
Blutgruppe 0d (rh neg)	Blutgruppe AB (Rh pos.)
Diabetes-Allergie	Eintrag erscheint gar nicht

(So ähnlich könnten auch die Bevölkerung insgesamt oder Teile davon nach unten „reguliert“ werden)

3. Die Pharmaindustrie hätte wunderbare Möglichkeiten überteuerte Medikamente zu entwickeln ***und den Bedarf dafür gleich mit*** **!!!** Dazu kommt die kostenlose und massenhafte Testung von neuen Medikamenten. Dumm ist nur, daß die beteiligten Ärzte und Patienten gar nichts davon wissen – und auch sonst kein Außenstehender. *(Noch einmal: die Pharmaindustrie besteht aus gewinnorientierten Unternehmen, deren einziges Ziel die Gewinnmaximierung ist und nicht Ihre Gesundheit – siehe Seite 39 und 41)*

4. Die „Organindustrie“ hätte unbegrenzt Nachschub an lebendfrischen Organen. (Auch ohne IHR Einverständnis. Ärzte oder Angehörige werden dabei nicht beteiligt.)

5. Versicherungen und Arbeitgeber werden sowieso alles daran setzen, um an die Patientendaten zu gelangen, so wie der BioTech-Verband dies ja heute schon fordert.

6. Wann das organisierte Verbrechen an die Daten gelangt, dürfte nur eine Frage der Zeit sein. Die Folgen können sie sich selbst ausrechnen. (Oder auch nicht, weil diese so ungeheuerlich sind, dass sich der Verstand weigert.)

Dazu kommt noch, dass das alles und noch mehr passieren kann durch Versehen/ menschliches Versagen oder technische Fehler beim Übertragen o. Kopieren von Daten. Wer kann das denn verhindern???

Dies sind nur einige Möglichkeiten – denken Sie mal darüber nach.

Das alles ist hervorragend in folgender Power Point Dokumentation nachzulesen
(u. a. auch, warum die ärztliche Schweigepflicht dann nicht mehr existiert):
http://www.stoppt-die-e-card.de/index.php?serendipity[subpage]=downloadmanager&thiscat=2&file=57
(S E H R L E S E N S W E R T)

Geplanter Missbrauch: (Juni 2015)
Spitzenvertreter der Kassen planen offensichtlich, mit Hilfe der "Gesundheitskarte" **dass der Medizinische Dienst der Krankenkassen auf Grundlage der Patientenakten festlegt, welche Patienten welches Medikament bekommen oder nicht bekommen.** Es geht also **NICHT um medizinische Verbesserungen für Versicherte und Patienten,** sondern es wird ganz deutlich dass es um Sparmaßnahmen, Rationierung und durch Kassen gesteuerte Versorgung ("Managed-Care Medizin") **mit Hilfe von zentralisiert überwachten Medizindaten möglichst der gesamten Bevölkerung geht.**
Quelle: http://www.stoppt-die-e-card.de/index.php?/archives/312-Offene-medizinische-Rationierung-mit-Hilfe-der-Elektronischen-Gesundheitskarte.html

Update – 3. Mai 2015 – Bundesregierung vertuscht US-Spionage

Noch vor wenigen Tagen erklärte das Innenministerium dem Bundestag, nichts über NSA-Wirtschaftsspionage zu wissen. Offensichtlich stimmte das nicht und die Bundesregierung hat gegenüber dem Bundestag offenbar noch vor wenigen Wochen falsche Aussagen gemacht.

Dabei scheint inzwischen klar, dass der BND das zuständige Kanzleramt schon seit Jahren auf die Versuche der NSA hinweist, in Deutschland und Europa Wirtschafts-spionage zu veranlassen.

Vergangene Woche war erst bekannt geworden, dass die NSA jahrelang versucht hat, dem BND sogenannte Selektoren unterzujubeln, deren Überwachung gegen deutsche und europäische Interessen verstoßen würde. Weil die Informationen, um die es gehe, aber aus "geheimen" und "streng geheimen" Unterlagen stammten, sehe der „Bundesinnen-minister“ de Maizière sich außerstande, sich öffentlich zu äußern.

Das lassen Sie sich mal auf der Zunge zergehen: Ein sog. „Bundesinnenminister“ muss erst die Überwacher fragen, ob und was er öffentlich sagen darf ???!!!

Das kann man getrost auch als "Landesverrat auf Bundesebene" bezeichnen.

Und solche Leute reden von „Datensicherheit“ bei der eGK, weil die Ihre Gesund-heitsdaten haben wollen ?! Für wie glaubwürdig halten SIE denn die Aussagen solcher Politiker???!!!

Quelle: http://www.heise.de/newsticker/meldung/BND-Skandal-Bundesregierung-machte-falsche-Angaben-zur-NSA-Spionage-2627738.html

Doch nun weiter mit:

E-Health auf Deutsch: Die Regierung beschließt die Einführung einer flächendeckenden Technologie und schreibt dafür Paragraphen in das Sozialgesetzbuch, die nicht der Gesundheit dienen, sondern ausschließlich den Finanzmärkten und ihren Handlangern, der (meist börsennotierten) IT-Industrie. Nicht Diagnostik und Heilbehandlung – Ausbildung der Ärzte, Zeit für Gespräche mit der Ärztin oder dem Arzt oder bessere Personalausstattung in Kliniken – werden gestärkt, sondern die Lobbyisten haben gewonnen, die Signaturen, Chip-Karten und technische Infrastruktur verkaufen wollen.

Das Gesetz zwingt die Krankenkassen, die teure Infrastruktur zu finanzieren – und dies aus den Taschen der Beitragszahlenden. Also auf unser aller Kosten.

Das kommende „eHealth-Gesetz“ bedeutet das Umverteilen der Milliardenetats des Gesundheitssystems in die Taschen von börsennotierten Konzernen.
Quelle: https://bigbrotherawards.de/2015/verbraucherschutz-bundesministerium-fuer-gesundheit

Herrn Gröhe muss deutlich gemacht werden, dass die Versichertengemeinschaft eine Reduzierung der informationellen Selbstbestimmung über die eigenen Gesundheitsdaten nicht hinnehmen wird.

Quellen:
http://www.heise.de/newsticker/meldung/Biotech-Verband-will-Daten-der-elektronischen-Gesundheitskarte-nutzen-2597974.html
und
http://ddrm.de/?p=4101#more-4101

Ärzte lehnen übrigens den Anschluss an die zentrale e-Card Infrastruktur erneut ab

Am 27.2.2015 wurde bei der Vertreterversammlung der Kassenärztlichen Bundesvereinigung (also dem "Parlament" der KBV) folgender Beschluss mit großer Mehrheit gefasst. **Der hauptamtliche KBV Vorstand wurde aufgefordert**, sich im Gesetzgebungsverfahren des drohenden E-Health Gesetzes **konkret gegen die strategisch wichtige Funktion des e-Card Projektes "Online Versichertenstammdatenmanagement" (VSDM) einzusetzen.**

Mit der Einführung des VSDM, welches von Minister Hermann Gröhe mit Hilfe des neuen Gesetzes **auch mit Sanktionen erzwungen werden soll, hängen künftig alle Arztpraxen an dem von ARVATO (Bertelsmannkonzern) aufgebauten "zentralen Großnetz".**

Beschluss 27. 2. 2015: *"Aufforderung an den Vorstand der KBV zur Abschaffung der vorgesehenen Pflicht zum Versichertenstammdaten-Management“*

Quelle:
http://www.kbv.de/html/13975.php

Übrigens können ALLE eGK zurückgeschickt werden, denn sie genügen NICHT den gesetzlichen Vorgaben:

Die eGK OHNE Foto mit der Begründung:

Die mir zugeschickte eGK verstößt durch das fehlende Lichtbild gegen :

- § 291a Abs. 2 und 3 i. V. m. § 291 Abs. 2 und 2a SGB V
- § 3 Abs. 1 der Anlage 4 a zum BMV-Ä
- Anhang 1, Abs. 1.2 der Anlage 4 a zum BMV-Ä.

Selbst eine eGK *mit* Foto wäre rechtswidrig, da auch sie den gesetzlichen Anforderungen nicht entspricht, weil keine identitätsgeprüften Fotos verwendet wurden und werden, obwohl der § 291, Abs. 2 SGB V verlangt, dass auf der Krankenversichertenkarte u. a. „*Unterschrift und Lichtbild des Versicherten*“ aufgebracht werden. (siehe **Musterwiderspruch** Seite 7 und **Musterbrief** am Schluss.)

Schlusspunkt und Eingeständnis der Illusion von Datensicherheit:

Auf der Pressekonferenz Anfang Juni 2015 betr. Trojaner-Angriff auf Bundestag hat der Chef des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Michael Hange, folgendes offiziell zugegeben:

Mehrfach erklärte Hange auf Nachfragen der Journalisten, dass es keine 100%-ige Sicherheit geben könne und Computersicherheit ein fortlaufender Prozess sei. Ein Zustand, in dem das BSI sagen könnte "dieses Netz ist absolut sicher", könne es nicht geben, dazu habe heutige Software einfach zu viele Schwachstellen.

Damit wird also (wieder einmal) offiziell eingestanden, dass es niemals Datensicherheit gegeben hat und geben kann und die Bevölkerung in diesem Punkt bis heute ganz bewusst belogen wurde und wird.

Fazit:

Aus all dem bisher dargelegten ist wohl mehr als deutlich geworden, daß es keine Datensicherheit gibt und auch niemals geben kann, schon gar nicht in Deutschland.

Noch einmal: (nur einige Beispiele)

1. Durch Booz-Allen-Hamilton, CSC-Deutschland-Solutions GmbH, und Dataport sind die NSA und der britische Partnergeheimdienst *GCHQ* praktisch schon an allen großen IT-Vorhaben der Bundesregierung beteiligt.
2. Der **GKV-Spitzenverband** gibt öffentlich zu, daß es Datensicherheit niemals gab

und geben kann, das **Bundesamtes für Sicherheit in der Informationstechnik** (BSI) ebenfalls.

3. Straffreie Spionage in Deutschland (politisch, wirtschaftlich und militärisch) wird den Geheimdiensten der USA und England (wem noch?) vertraglich garantiert.
4. In ihrer Regierungserklärung vom Jan 2014 hat Frau Merkel erklärt, sie hätte keinen Hebel um die Geheimdienstpraktiken der USA gegen Deutschland zu beenden.
5. Die Firmen Gemalto und Giesecke & Devrient (eGK) gelten seit 2010 als gehackt. *(Warum Verschlüsselungen knacken, wenn man die Schlüssel hat?!)*

„Aber die Patientendaten sind ja sooo sicher ..."

Bei ca. 2 Millionen offiziell Zugriffsberechtigten und einer niemals genau zu ermittelnden Zahl nicht offiziell Zugriffsberechtigter (z. B. Personal in Versicherungen, EDV-Dienstleistern, Mitarbeiter der Serverfirmen, EDV-Wartungsfirmen, Subunternehmen, diverse kurzfristig eingestellte Zeitarbeiter usw. (mögliche INNENTÄTER) kann es auch gar keine Datensicherheit geben, von den äußerst hinterhältigen Geheimdienstmethoden mal ganz abgesehen.

Dabei ist es heute schon möglich, dass sich Ärzte gegenseitig eine sichere Mail (im eBriefumschlag mit eStempel, eUnterschrift und eBriefmarke) schicken können. Dazu genügt die Ende-zu-Ende-Verschlüsselung mittels PGP über die üblichen Mailversandstrukturen mit gegenseitig signierten Public Keys, so dass auch der Anscheinsbeweis einer Unterschrift gewährleistet ist. PGP gibt es schon seit 1991, ist kostenlos und hätte nur 0,001 Prozent der Kosten verschlungen, die bis dato in dieses größenwahnsinnige Technikprojekt gesteckt worden sind und seine Fortentwicklung als freie Software hätte allen Menschen genützt.
Bei allen Datenpannen der Vergangenheit hatten auch stets nur max. einige hundert Personen Zugriffsberechtigungen. Trotzdem kam es zu teils gröbsten Datenpannen und Datendiebstählen, bei denen persönliche Daten im Internet offen für alle zu sehen waren. Wie schnell wird das dann erst bei den erwarteten ca. 2 Millionen offiziell Zugriffsberechtigten und einer nicht bekannten Anzahl nicht Zugriffsberechtigten, die aber trotzdem zugreifen können, dazu kommen?

Mitarbeiter können erpresst oder gekauft werden, oder wollen einfach nur „ihr Gehalt

aufbessern“. (Bank-CD's aus der Schweiz...). **Die Bundesregierung ist sich übrigens nicht zu schade, mit solchen Daten-Kriminellen auf Kosten der Steuerzahler trotzdem Geschäfte zu machen,** was von einem geringen bis nicht vorhandenen Unrechtsbewusstsein zeugt. Bestätigt wird dies vom bisherigen Umgang der Regierung mit der eGK, besonders mit dem geplanten E-Health-Gesetz. Damit sollen trotz immenser datenschutzrechtlicher und technischer Probleme hunderttausende Ärzte und Versicherte gegen ihren Willen an der Teilnahme am eGK-Verfahren gezwungen werden. Es gibt übrigens noch ca. 2 Millionen Versicherte, die die eGK weiterhin verweigern. Wäre die eGK mit der dazu geplanten IT-Infrastruktur wirklich zum Wohl der Patienten, müsste es nicht gegen den Widerstand von Millionen Menschen brutal „durchgedrückt“ werden.

Aus dem bisher dargelegten geht klar hervor, dass die eGK für Patienten wie Ärzte NUR Nachteile hat, z. Teil gravierende bis tödliche und es gibt KEINEN einzigen medizinischen Grund für die eGK und auch nach inzwischen acht Jahren ist **kein einziger patientenorientierter Nutzen zu erkennen**. Wie auch, denn in den politischen Gremien sitzen keine Mediziner mehr, nur noch Politiker und Lobbyisten.

Dazu kommt noch eine ganz andere, weit größere Gefahr:
Es geht um CETA und TTIP und in dessen Gefolge um TISA. Und damit wird die eGK erst richtig interessant. Das bedeutet die **Privatisierung aller staatlichen Dienstleistungen.** Wenn CETA oder TTIP ratifiziert sind, können Unternehmen Staaten wegen ALLEM verklagen, was deren jetzige und zu erwartende künftige Gewinn schmälert, (sog. „Handelshemmnisse“) z. B. wegen Umweltschutz- oder Arbeitnehmerschutzgesetzen, Sozialstandards usw. (Staaten können übrigens KEINE Unternehmen verklagen !!!) und Sie werden zugeben, dass eine staatliche Gesundheitsversorgung ein echtes Handels-hemmnis ist. Im Sinne eines sogenannten Investorenschutzes **würden Regierungen dann für die Kosten haftbar gemacht, die ausländischen Unternehmen z. B. durch schärfere Umweltschutzregeln entstehen.** Diese Klagen würden unter Ausschluss der Öffentlichkeit vor geheimen Schiedsgerichten geführt. Also wird man klagen, gewinnen und plötzlich hat die eGK ganz erhebliche Schattenseiten vorzuweisen. Nun können nämlich die Daten der eGA dazu führen, dass die Beiträge in die Höhe schnellen, denn die Gesundheitsvorsorge ist nun kein Solidarsystem mehr, sondern ein profitorientiertes privates Unternehmen. (Dasselbe passiert dann mit der gesetzlichen Rentenversicherung, Sozialhilfe, Früh- und Erwerbsunfähigkeitsrente, Beamtenpensionen usw.)

Dann sind IHRE Gesundheitsdaten entscheidend, ob und zu welchen Konditionen Sie in eine Krankenversicherung aufgenommen werden. Die Privaten wollen schließlich wissen, ob ein Kunde ein Geschäft werden kann oder lediglich ein nicht erwünschter Kostenfaktor sein würde. **Wird langsam klar, worum es bei der eGK wirklich geht??? !!!**

Das ist übrigens keine Verschwörungstheorie, sondern drohende bittere Realität. Regierungen, die sich auf eine derartig folgenreiche Veränderung der Spielregeln einlassen, geben ohne Not ihre politische Gestaltungsfähigkeit aus der Hand und schränken die demokratische Willensbildung ihrer Bürger auf unzulässige Weise ein. Man kann auch sagen, dass sie die Bevölkerung den „Konzerngewinnen" ausliefert.

Dass diese Diskussion bisher nur in Gremien geführt wird, die es offiziell gar nicht gibt, zeigt, wie wichtig die anstehenden Entscheidungen für uns alle sind. ***Parlamentarier sind übrigens nicht beteiligt.*** *Sie dürfen auf Antrag nur die (derzeit 685 Seiten langen) Entwürfe einsehen, aber keine Kopien, Notizen oder Fotos machen. Die Verträge werden übrigens erst 5 Jahre nach Inkrafttreten veröffentlicht – das kommt einer Abschaffung der Demokratie gleich.*

...und beginnt schon hier und heute mit einem folgendem Rechtsbruch:
Damit obiges funktioniert, müssen Gesundheitsdaten nämlich eindeutig Ihrer Person zugeordnet werden können. Dazu hat der Gesetzgeber gegen geltendes Recht eine **lebenslang gültige Krankenversicherungsnummer** eingeführt. Praktischerweise kann die Bundesregierung sich die Gesetze ja selber machen, so wie sie die gerade braucht und hat dazu einfach den § 290 SGB V geändert. Bei dieser Versichertennummer handelt es sich jetzt um ein **unzulässiges Personenkennzeichen**, das dazu dient, einzelne Personen in den zunehmenden Datenmengen zu identifizieren.
Dies verstößt gegen Art. 1 Grundgesetz und verletzt das Recht auf freie Entfaltung der Persönlichkeit nach Art. 2 Grundgesetz, da ein Einzelner bei der heutigen Verknüpfung verschiedener Datenbanken nicht mehr überschauen kann, welche Konsequenzen sich daraus für das staatliche Handeln ergeben. Bei den deutschen Sicherheitsbehörden werden derzeit geschätzte 1000 Datenbanken geführt, in denen sich Angaben über mehrere Millionen Menschen finden. Allein in die aufgebaute Anti-Terror-Datei werden nach Angaben der Bundesregierung Informationen aus 845 verschiedenen Datenbanken eingespeist. Die geht aus einer Antwort der Bundesregierung auf die Kleine

Anfrage der Abgeordneten Ulla Jelpke und weiterer Abgeordneter der Fraktion DIE LINKE vom 6.10.2006, BT-Drucksache 16/2607 hervor.
Verwiesen sei hier nochmals auf das Urteil des Bundesverfassungsgerichts mit seiner Entscheidung zur Volkszählung 1983 (BVerfGE 65, 1).

In dem Urteil fand sich nicht nur die Begründung des Rechts auf informationelle Selbstbestimmung, wonach der Einzelne *„grundsätzlich selbst zu entscheiden [hat], wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden".* (Rdnr. 152)
Darüber hinaus erlegten die Verfassungsrichter dem Staat das Verbot auf, über seine Bürgerinnen und Bürger Persönlichkeitsprofile zu erstellen. Die Gefahr einer solchen Profilbildung sahen sie insbesondere in den informationstechnischen Möglichkeiten der Datenverarbeitung: Sie mache es leicht, verschiedene Datenbestände unterschiedlicher staatlicher Stellen miteinander zu verknüpfen (s. o.). Insbesondere diese Verknüpfungsmöglichkeiten können dazu führen, dass „ein für sich gesehen belangloses Datum einen neuen Stellenwert [bekommt]". (Rdnr. 158)

Quelle:
http://www.humanistische-union.de/themen/datenschutz/steuer_id/detail/back/steuer-id/article/die-personenkennziffer-der-traum-von-der-datenzusammenfuehrung/

Bundesgesundheitsminister Gröhe plant, die – nach seiner Zählung – mehr als 200 vd. Informationstechnischen Systeme im Gesundheitswesen zu vereinheitlichen und ihre Datenbestände für die Institutionen im Gesundheitswesen nutzbar zu machen. So begründete er bereits im August 2014 seine Pläne für ein **E-Health-Gesetz** (siehe http://www.bmg.bund.de/ministerium/presse/interviews/gelber-dienst-110814.html). Die lebenslange **Krankenversichertennummer stellt ein Suchkriterium dar,** mit der die **bislang verstreuten Informationen personenbezogen zugeordnet werden könnten.** Der **gläserne Patient** wäre endgültig Wirklichkeit geworden und **die ärztliche Schweigepflicht abgeschafft.** (Und so ganz nebenbei erhält der Staat von jedem Zwangsversicherten alle 5 Jahre ein aktuelles Foto)

*„**Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren**…".* Diesen Satz hat der Erste Senat des Bundesverfassungsgerichts in seiner Entscheidung vom 16.07.1969 (Aktenzeichen 1 BvL 19/63 – http://www.rechtsanwaltmoebius.de/urteil/bverfg_urteil_1-bvl-

19-63-mikrozensus.html) den politisch Handelnden in Exekutive und Legislative ins Stammbuch geschrieben.

Im Zeitalter elektronischer Datenverarbeitung scheint das bei den politisch Verantwortlichen in Vergessenheit geraten zu sein. Wie anders ist es erklärbar, dass jeder Mensch von Geburt an mit der **lebenslangen Steuer-ID** (Rechtsgrundlage: § 139 Abgabenordnung – http://www.gesetze-im-internet.de/ao_1977/__139b.html), der **lebenslangen Krankenversichertennummer** (Rechtsgrundlage: § 290 SGB V – http://dejure.org/gesetze/SGB_V/290.html) und spätestens mit Eintritt ins Berufsleben der **lebenslangen Sozialversicherungsnummer** (Rechtsgrundlage: §§ 18f – 18h SGB IV – http://dejure.org/gesetze/SGB_IV/18f.html) zum **gläsernen Staatsbürger** gemacht wird. Denn mit Hilfe dieser drei Identifikationsmerkmale lassen sich nahezu alle Aktivitäten eines Menschen außerhalb seines allerprivatesten und intimsten Lebensbereichs ihm zuordnen und auswerten.

Um noch einmal das Bundesverfassungsgericht zu Wort kommen zu lassen. Es hat in seiner Entscheidung vom 16.07.1969 auch festgestellt: *„In der Wertordnung des Grundgesetzes ist die Menschenwürde der oberste Wert… Damit gewährt das Grundgesetz dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist… Es widerspricht der menschlichen Würde, den Menschen zum bloßen Objekt im Staat zu machen… Ein solches Eindringen in den Persönlichkeitsbereich durch eine umfassende Einsichtnahme in die persönlichen Verhältnisse seiner Bürger ist dem Staat auch deshalb versagt, weil dem Einzelnen um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein ‚Innenraum' verbleiben muss, in dem er ‚sich selbst besitzt' und ‚in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt'…In diesen Bereich kann der Staat unter Umständen bereits durch eine – wenn auch bewertungsneutrale – Einsichtnahme eingreifen, die die freie Entfaltung der Persönlichkeit durch den psychischen Druck öffentlicher Anteilnahme zu hemmen vermag…"*

- Wenn diese Maßstäbe des Bundesverfassungsgerichts künftig nicht einmal bei den sensibelsten Daten der Menschen – ihren Gesundheits- bzw. Krankheitsdaten – Berücksichtigung finden,
- wenn die Pläne von Minister Gröhe mit seinem E-Health-Gesetz Wirklichkeit werden,

- wenn die Gesundheits- bzw. Krankheitsdaten der gesetzlich Versicherten Menschen in den Telematik-Strukturen gesammelt werden und zur Auswertung bereit stehen,

dann wird **George Orwells 1984** – seiner Phantasie von der Überwachung im fiktiven Staat Ozeanien – von der Realität in der Berliner Republik des Jahres 2015 übertroffen.

Fazit:

§ 139 Abgabenordnung ***(lebenslange Steuer-ID)****, die §§ 18f – 18h SGB IV* ***(lebenslange Sozialversicherungsnummer)*** *und vor allem der* ***§ 290 SGB V (lebenslange Kranken-versicherungsnummer) sind in ihrem derzeitigen Wortlaut definitiv verfassungs-widrig.*** *Damit haben die Krankenkassen ohne gültige Rechtsgrundlage bzw. verfassungs-widrig eine neue, lebenslängliche Versicherungsnummer und damit ein unzulässiges Personenkennzeichen zugewiesen.*

Diese Aufklärung könnte noch endlos weitergeführt werden, jedenfalls solange dieses Irrsinnsprojekt besteht. Es dürfte aber genügen, um zu verstehen, worum es bei der eGK wirklich geht.

Solange es also das Projekt eGK mit seiner zentralen Speicherung von Patientendaten gibt, besteht also eine reale, massive Gefahr für JEDEN (Patienten) und die Demokratie und es wird weder eine Datensicherheit, noch sozialen Frieden geben.

Der Plan zur EGK wurde 2003 entwickelt, im Auftrag des Gesundheitsministeriums, vom Konsortium *„bit4health“*, ihm gehörten genau die Firmen an, die heute vom Projekt profitieren: *Sagem Orga, IBM, Siemens, Giesecke & Devrient, IntercomponentWare* und **an die bisher mehr als eine Milliarde Euro geflossen sind,** (Mai 2013) noch bevor die Infrastruktur in Wirkbetrieb ist. Dazu kommen noch die Hersteller von Plastikkarten, Anbieter von digitalen Signaturen, die Telematikindustrie (wie z.B. T-Systems und die Firma Arvato des Bertelsmann-Konzerns) und natürlich Unternehmen, die Kartenlese-geräte herstellen. Nach heutiger Einschätzung der Unternehmensberatung „Booz Allen Hamilton“ wird das wohl ca. 15 Milliarden Euro kosten.

Hauptsächlich obige 5 Firmen, besonders aber Giesecke & Devrient, profitieren von diesem Mammutprojekt und natürlich der Staat, der die Karte später auch sicher-heitspolitisch nutzen oder auch missbrauchen kann. (und dies mit an Sicherheit

grenzender Wahrscheinlichkeit auch tun wird.)

Durch eine einfache Gesetzesänderung wird ein Missbrauch dann „legal“.

DER ultimative Beweis für die Lügen von Datensicherheit mit Patientendaten:

Wenn Sie jetzt immer noch an die Märchen von Datensicherheit in Zusammenhang mit der eGK glauben, fragen Sie sich mal, warum diese zentral gespeicherten Patientendaten in ein **WELTWEIT LESBARES Austauschformat** umgewandelt werden und im **GLOBAL** angelegten Datenverarbeitungs- und Speichersystem landen sollen !!!

Quelle: http://www.ocmts.de/egk/xmlcontainer/index.html

(**Es wird empfohlen, die kurze, aber höchst interessante Quellenangabe unbedingt zu lesen.)**

Trotzdem sollte der Humor nicht zu kurz kommen:

Noch Fragen ???

Mit freundlichen Grüßen

<u>Hier aber noch der MUSTERBRIEF zur Rücksendung der eGK -</u> Stand: 6. Juli 2015

<u>Absender</u>

An die
Krankenkasse
Straße
Ort

Ort, Datum

eGK zurück– Vers.-Nr.:

Sehr geehrte Damen und Herren,

zunächst möchte ich meine Zufriedenheit mit den Leistungen der (Name der KK) äußern. Mein Schreiben richtet sich also <u>nicht</u> gegen die (Name der KK), sondern gegen das Vorhaben der Bundesregierung, angestoßen mit dem GMG Gesundheitsmodernisierungs-gesetz von 2005, eine Datenbasis mit allen relevanten Patientendaten zu schaffen, also ALLE Patientendaten <u>zentral</u> zu speichern. Das ist ein weiterer Schritt zum gläsernen Bürger und bedeutet die Abschaffung der ärztlichen Schweigepflicht. Beides bin ich nicht bereit mitzutragen.

Aus 2 Gründen muss ich Ihnen heute meine eGK zurückschicken:

- Die Karte ist ungültig, da gesetzliche Vorgaben nicht erfüllt sind.
- Der Datenschutz im Zusammenhang mit der eGk existiert NICHT und kann auch niemals existieren.

<u>Zu 1. – ungültige Karte:</u>
In meinem Schreiben vom 2. 2. 2015 habe ich <u>keineswegs eine eGK beantragt</u>, sondern lediglich um Zusendung einer neuen Versichertenkarte gebeten, da meine alte verlorengegangen ist.

Geschickt wurde mir aber eine <u>eGK,</u> die zudem noch ungültig ist:

- sie entspricht nicht den gesetzlichen Vorgaben.
- sie enthält ein **verfassungswidriges** und damit **unzulässiges Personenkennzeichen,** nämlich die lebenslang gültige Krankenversicherungsnummer (Mein Antrag vom 18. 1. 2015)
- Mein elektronisch verwendeter Name ist falsch geschrieben (Rückseite).

In Ihrem Schreiben vom 3. 3. 2014 haben Sie darauf hingewiesen, daß Sie keine Versichertenkarte ohne Lichtbild mehr erstellen dürfen, da es der Gesetzgeber im SGB V, § 291, Abs. 2 so vor-schreibt. Daran hat sich bis heute nichts geändert.

Die mir zugeschickte eGK verstößt durch das fehlende Lichtbild also gegen :

4. § 291a Abs. 2 und 3 i. V. m. § 291 Abs. 2 und 2a SGB V
5. § 3 Abs. 1 der Anlage 4 a zum BMV-Ä
6. Anhang 1, Abs. 1.2 der Anlage 4 a zum BMV-Ä.

Sie werden sicher nachvollziehen können, dass ich nicht die Abschaffung der ärztlichen Schweigepflicht durch Annahme einer (ungültigen) eGK unterstütze, denn nichts anderes bedeutet der derzeitige Aufbau der Telematik-Infrastruktur zur eGK, u. a. mit geplanten Anwendungen, die mit der eGK gar nichts zu tun haben – s. u. Begründung 2, e-health-Gesetzentwurf.

Der Titel "Elektronische Gesundheitskarte" ist übrigens eine Irreführung. In Wirklichkeit geht es nicht um die Karte, sondern der Kern des Projektes ist ein gigantisches, deutschlandweites IT-Netzwerk mit zentralen (bzw. funktionell zentralen) Großcomputern zur Patientendatenspeicherung. Wo diese Server stehen, wird bis heute verschwiegen. Diese könnten in Deutschland, aber auch in den USA oder anderen Ländern stehen.

Tatsächlich, im neuen System liegen Patientendaten nicht mehr im geschützten Raum Hausarztpraxis, sondern irgendwo auf einem **Zentralrechner,** auf den 120.000 Arztpraxen, 60.000 Zahnarztpraxen und Psychotherapiepraxen, 3.000 Krankenhäuser, 300 Krankenkassen und 22.000 Apotheken und deren Mitarbeiter Tag und Nacht potentiellen Zugriff haben müssen. Dazu kommen eine unbekannte Anzahl von EDV-Wartungsfirmen und die Betreiber der Server. (NSA und GCHQ sind übrigens schon „drin“ – später mehr dazu)

Selbst eine eGK *mit* Foto wäre rechtswidrig, da auch sie den gesetzlichen Anforderungen nicht entspricht, weil keine identitätsgeprüften Fotos verwendet wurden und werden, obwohl der § 291, Abs. 2 SGB V verlangt, dass auf der Krankenversichertenkarte u. a. „*Unterschrift und Lichtbild des Versicherten“* aufgebracht werden.

Der Arzt ist nach der **Anlage 4a des BMV-Ä, Anhang 1, Ziffer 1.2 verpflichtet die Identität des Versicherten zu prüfen.** Eine solche Identitätsprüfung durch den Arzt ist aber nur möglich, wenn bereits bei der Herstellung der eGK ein identitätsgeprüftes Lichtbild verwendet worden ist, was bis heute definitiv NICHT der Fall ist.

Der Arzt kann also die Identität gar nicht überprüfen und macht sich somit evtl. strafbar nach § 203 StGB (Ärztliche Schweigepflicht), wenn er sich auf die Daten der eGK verläßt und vielleicht auch noch Patientendaten per Internet überträgt (Versichertenstamm-datenmanagement).

Die hier vertretene Rechtsauffassung wurde durch das 2014 bekannt gewordene Gutachten der Kassenärztlichen Bundesvereinigung (KBV) bestätigt.

Zu 2. – nicht existierender Datenschutz der eGK:

Begründung 1)

Nach der heutigen Sachlage muß davon ausgegangen werden, dass die versprochene Datensicherheit

6. nicht existiert und
7. niemals existieren kann

Dies hat der **GKV-Spitzenverband** am 20. 1. 2015 in der ZDF-Sendung **Frontal 21** zum Thema Datenschutz bei der eGK selbst zugegeben.

Antwort des GKV-Verbandsprechers, Florian Lenz zur obigen Frage: (Ab Minute 8.30)
„Wir wissen, daß in der Vergangenheit Fehler gemacht worden sind, daß nicht korrekt mit Daten umgegangen worden ist...

Und weiter...(ab Minute 8.50)
„Wir können nicht völlig ausschließen, dass an irgendeiner Stelle irgendwo jemand aus Versehen oder mit Absicht etwas mit Daten falsch macht.“

Quellen:
http://www.stoppt-die-e-card.de/exit.php?url_id=706&entry_id=288 und
https://www.youtube.com/watch?v=WlEpaP-TY9g
Wie leichtfertig die Krankenkassen, leider auch die Securvita, mit Patientendaten heute schon umgehen, belegen der telefonische und der Online-Service. Beim Telefonat reichen auch schon der Name und das Geburtsdatum. So ist schon eine ECHTE *eGK mit dem Bild des „Krümelmonsters“* aus der Sesamstraße ausgestellt worden. (mein Schreiben vom 18. 1. 2015, Seite 2)

Der Verlust der KV-Karte kann also recht einfach zum Datenmissbrauch genutzt werden – und ist es auch schon, ein Telefonat genügt. (Mein Schreiben vom 18. 1. 2015) Sollte also jemand an meine persönlichen Gesundheitsdaten, bzw. heutzutage einfach nur an meine Versicherungsnummer gelangen, kommt das einem **Identitätsdiebstahl** gleich. Das kann bei kriminellem Ausnutzen existenzvernichtende Folgen haben.

Begründung 2)

Gemalto und Giesecke & Devrient, beide führend bei der Ausgabe der eGK, gelten seit 2010 als gehackt: *(Warum Verschlüsselung knacken, wenn man den Schlüssel hat?!)*

Meldung vom 20. Februar 2015: (netzpolitik.org)
Schon im Gründungsjahr von MHET, 2010, verkündete GCHQ stolz seinen Erfolg in

einer Präsentation:

> **„GEMALTO – Erfolgreich mehrere Maschinen verwanzt und wir glauben, dass wir ihr gesamtes Netzwerk haben.“**

Seit Jahren kopieren also NSA und GCHQ bei den Herstellern von SIM-Karten und Smart Cards die zugehörigen Schlüssel ab. Damit können sie die übertragenen Informationen mitlesen und manipulieren.

Übrigens manipulieren die Schnüffler auch die Abrechnungs-Server der Netzbetreiber. So können sie Daten und SMS zu und von fremden Endgeräten übermitteln, OHNE dass es in den Rechnungsdaten erscheint.

Auch Gemaltos deutscher Mitbewerber Giesecke & Devrient (eGK) wird als Angriffsziel erwähnt, und es darf angenommen werden, dass in den vergangenen Jahren noch andere Hersteller dazugekommen sind.

Quelle:
https://netzpolitik.org/2015/verschluesselung-knacken-wenn-man-den-schluessel-haben-kann-wie-nsa-und-gchq-sim-karten-keys-stehlen/

Der Einbruch in ein System der höchsten Sicherheitsstufe ist also gelungen.... und seit 2010 bis Februar 2015 völlig unentdeckt !!!

Vor ein paar Tagen noch komplett ahnungslos - und jetzt ist sich Gemalto sicher, dass nichts gestohlen wurde – für wie glaubwürdig halten Sie diese Aussage und wie stellt man eigentlich zweifelsfrei fest, daß Daten (seit 2010) niemals kopiert wurden?

Wenn bis heute dieses jahrelange Datenleck den Betreibern der Firma nicht aufgefallen ist, bedeutet das, dass interne Kontrollen völlig versagt haben müssen. Es gibt also KEINE Sicherheit mit den jetzt ausgegebenen elektronischen Karten.

Begründung 3)

Aus internen Mails der **CSC Deutschland Solutions GmbH** geht hervor, daß die Firma an allen großen IT-Vorhaben der Bundesregierung beteiligt ist. Die Mutterfirma **CSC** (USA) **ist einer der wichtigsten IT-Dienstleister des US-Geheimdienstes NSA** (praktisch die *„EDV-Abteilung der NSA“*), **u. a. an der Entwicklung von Spähprogramen des US-Nachrichtendienstes beteiligt.**

Philipp Müller, Public Affairs Director von CSC, hat telefonisch indirekt die Echtheit der E-Mails bestätigt:

> *„Wir finden, es gehört nicht zum guten Ton, interne E-Mails zu veröffentlichen.“*
>
> (Allein in den vergangenen vier Jahren der letzten Regierung unter Angela Merkel zwischen 2009 und 2013 bekam die CSC Deutschland genau 100 Aufträge von zehn unterschiedlichen Ministerien und dem Bundeskanzleramt.)

Nach den Bestimmungen des PATRIOT Act sind auch ausländische (US) Töchterfirmen

nach dem US-Gesetz verpflichtet, Zugriff auf ihre Server zu gewähren; selbst dann, wenn lokale Gesetze dies untersagen.

Die Firma *CSC Deutschland Solutions GmbH* ist bereits mehrfach durch ungefilterte illegale Datenweitergabe unangenehm aufgefallen und steht heftig in der Kritik.

Dieser Firma wird Zugang zu praktisch allen großen IT-Vorhaben der Bundesregierung gewährt?!

Quelle:
https://netzpolitik.org/2014/interne-e-mails-csc-freut-sich-ueber-neue-vertraege-mit-behoerden-trotz-no-spy-erlass-und-medialen-anschuldigungen/

Selbst so hochspezialisierte Firmen wie Google, Microsoft oder Sony konnten Datenklau nicht verhindern. Für wie hoch halten Sie die Wahrscheinlichkeit, dass dies einem halbstaatlichen Unternehmen mit ca. 2 Millionen (!) offiziell Zugriffsberechtigten und eine unbekannten Zahl nicht offiziell Zugriffsberechtigter gelingt?

Im **e-Health-Gesetzentwurf** ist derzeit folgendes zu lesen: (März 2015)

Der Austausch von Gesundheitsdaten – auch mit nicht-ärztlichen Leistungserbringern – soll so gestärkt werden. […] Die bisherige Regelung, wonach in der Telematikinfrastruktur der eGK gespeicherte Gesundheitsdaten ausschließlich zum Zweck der Versorgung der Patienten genutzt werden dürfen, würde durch die Hintertür abgeschafft.

Im Klartext:
Durch das geplante **e-Health-Gesetz** werden die (zentral gespeicherten) Patientendaten an Versicherungen, Pharmaindustrie, Behörden, Forschungs- und Entwicklungsprojekte, etc. weitergeleitet. (sämtliche Arbeitgeber dürften an den Daten brennend interessiert sein). Spätestens jetzt dürfte klar sein, **daß der Datenschutz bei der eGk durch das e-Healt-Gesetz aufgehoben** und der **gläserne Patient** Wirklichkeit wird.

In diesem Zusammenhang ist die Äußerung des **Geschäftsführers der Gematik**, Arno Elmer interessant. Elmer überraschte Anfang 2013 in einer Diskussion betr. eGK mit der skeptischen Sichtweise: **"Wir bauen nur die Autobahn. Wenn der Gesetzgeber die Daten haben will, dann ändert er die Gesetze und holt sie sich."** Klingelt's ?!

Es dürfte damit wohl klar sein, worum es bei der eGK WIRKLICH geht, oder?!

„Aber nun kommt der Hammer“ !!!

Biotech-Verband will Daten der elektronischen Gesundheitskarte nutzen

Am 9. 4. 2015 war dazu bei heise.de und ddrm.de folgendes zu lesen:

BIO Deutschland e. V. ist kein Verein, der sich mit ökologisch erzeugten Lebensmitteln beschäftigt. Das wird deutlich, wenn der vollständige Name des Vereins genannt wird: **Biotechnologie-Industrie-Organisation Deutschland e.V.** Noch deutlicher wird der Zweck von BIO Deutschland e. V. beim Blick auf die Fördermitglieder des Vereins:

Der einzige Zweck dieser Unternehmen dürfte die **Gewinnmaximierung** zu sein. Die Verbesserung der Gesundheit des Menschen scheint nicht dazuzugehören (siehe auch *„Die Gesetze der Pharma-Industrie“* von Dr. Rath – **Quelle:** http://www4ger.dr-rath-foundation.org/GESCHAEFT_MIT_DER_KRANKHEIT/die_gesetze_der_pharma-industrie.html)

Dieser Verband hat vor wenigen Tagen in einer Stellungnahme zum Entwurf für ein E-Health-Gesetz gefordert: *„Die Anwendungen der mit dem e-Health-Gesetz einzuführenden neuen elektronischen Gesundheitskarte beinhalten eine solche Datenbasis, die die forschenden Biotechnologie-Unternehmen effektiv unterstützen könnte. Nach der derzeitigen Ausgestaltung der elektronischen Gesundheitskarte ist den Unternehmen aber ein Zugriff auf diese Daten zu Forschungszwecken verwehrt…“* **Der Verein fordert deshalb erweiterte Zugriffsmöglichkeiten auf den durch die Telematik-Strukturen entstehenden Datenpool. Sie fordern aber auch für sich das Recht, unmittelbar in die Entscheidungsstrukturen der gematik eingebunden zu werden**: *„Biotechnologie-Unternehmen müssen in die Entscheidungsprozesse im Hinblick auf die Telematikinfrastruktur und die elektronische Gesundheitskarte eingebunden werden, Einbeziehung von Bio-IT Experten bei der Erarbeitung von Interoperabilitätsstrukturen…“*

Ein unverhüllter Angriff auf die bisherigen Datenschutzregelungen im Sozialgesetzbuch!

Die in § 75 SGB X (Übermittlung von Sozialdaten für die Forschung und Planung) und § 287 SGB V (Forschungsvorhaben) enthaltenen Regelungen erscheinen den Firmen der Pharma- und Medizintechnik-Industrie als Hemmnis für ihre wirtschaftlichen Interessen. **Sie fordern mit Ihrer Stellungnahme von Bundesgesundheitsminister Gröhe einen unmittelbaren Zugriff auf die Gesundheits- und Behandlungsdaten der knapp 70 Mio. Menschen in der gesetzlichen Krankenversicherung.** Dieser Forderung muss entschieden entgegen getreten werden!

Patientendaten gehören den Patienten! Niemand sonst!

ALLES andere hat KEINE Rechtsgrundlage!

- Die kostenlose (aber auch eine eventuelle kostenpflichtige) Bereitstellung von Patienten- und Gesundheitsdaten zum wirtschaftlichen Nutzen von Pharma- und anderen Unternehmen verletzt das Grundrecht auf informationelle Selbstbestimmung.
- Erfahrungen auch aus anderen Anwendungsbereichen machen deutlich: Auch anonymisierte oder pseudonymisierte Daten können – entsprechende Rechnerleistungen vorausgesetzt – wieder re-anonymisiert werden.
- Und nicht zu vergessen: Bisher geht § 291a SGB V Elektronische Gesundheitskarte) davon aus, dass der Zugriff auf die Daten eines Patienten, die im telematischen System hinterlegt sind, in jedem Einzelfall (Notfalldaten ausgenommen) der vorherigen aktiven Zustimmung des betroffenen Menschen bedarf.

Wie lächerlich einfach Re-Anonymisierung ist. Lesen Sie hier:
http://www.faz.net/aktuell/feuilleton/medien/metadaten-von-kreditkarten-keiner-bleibt-anonym-13398079.html

Herrn Gröhe muss deutlich gemacht werden, dass die Versichertengemeinschaft eine Reduzierung der informationellen Selbstbestimmung über die eigenen Gesundheitsdaten nicht hinnehmen wird.

Quellen:
http://www.heise.de/newsticker/meldung/Biotech-Verband-will-Daten-der-elektronischen-Gesundheitskarte-nutzen-2597974.html

und

http://ddrm.de/?p=4101#more-4101

Weitere Interessenten werden mit Sicherheit folgen, offensichtlich oder heimlich, legal oder illegal. Das das organisierte Verbrechen an die Daten gelangt, dürfte nur eine Frage der Zeit sein. Mit den Daten wird jeder (Entscheidungsträger) erpressbar oder kann durch gezielte (oder versehentliche) Verfälschung von Gesundheits- und Behandlungsdaten umgebracht werden.

Ärzte lehnen übrigens den Anschluss an die zentrale e-Card Infrastruktur erneut ab

Am 27.2.2015 wurde bei der Vertreterversammlung der Kassenärztlichen Bundesvereinigung (also dem "Parlament" der KBV) folgender Beschluss mit großer Mehrheit gefasst. **Der hauptamtliche KBV Vorstand wurde aufgefordert**, sich im Gesetzgebungsverfahren des drohenden E-Health Gesetzes **konkret gegen die strategisch wichtige Funktion des e-Card Projektes "Online Versichertenstammdatenmanagement" (VSDM) einzusetzen.**

Mit der Einführung des VSDM, welches von Minister Hermann Gröhe mit Hilfe des neuen Gesetzes **auch mit Sanktionen erzwungen werden soll, hängen künftig alle Arztpraxen an dem von ARVATO (Bertelsmannkonzern) aufgebauten "zentralen Großnetz".**

Beschluss 27. 2. 2015: *"Aufforderung an den Vorstand der KBV zur Abschaffung der*

vorgesehenen Pflicht zum Versichertenstammdaten-Management“

Quelle: http://www.kbv.de/html/13975.php

Wenn sie immer noch an die Märchen von Datensicherheit in Zusammenhang mit der eGK glauben, fragen Sie sich mal, warum diese zentral gespeicherten Patientendaten in ein **WELTWEIT LESBARES Austauschformat** umgewandelt werden und im **GLOBAL** angelegten Datenverarbeitungs- und Speichersystem landen sollen !!!

Es wird empfohlen, die kurze, aber höchst interessante Quellenangabe unbedingt zu lesen.

Quelle: http://www.ocmts.de/egk/xmlcontainer/index.html

Mit freundlichen Grüßen