Jaschinski Biere Brexl

Rechtsanwälte

JBB . Rechtsanwälte . Christinenstraße 18/19 . 10119 Berlin

Bundesverfassungsgericht
2. Senat
Schloßbezirk 3

76131 Karlsruhe

Dr. Martin Jaschinski
Sebastian Biere*
Oliver Brexl*
Thorsten Feldmann, LL.M.
Dr. Till Jaeger
Thomas Nuthmann*
Julian Höppner , LL.M.
Dr. Markus Wiedemann
Dennis Gehnen, LL.M.

Christinenstraße 18/19
10119 Berlin

Telefon +49 30 . 443 765 0
Telefax +49 30 . 443 765 22

www.jbb.de
rae@jbb.de

*Fachanwalt für gewerblichen Rechtsschutz

Berlin, 30. Juli 2007

Unser Zeichen: 779/06
Sekretariat: Jacqueline Moderack

In dem Wahlprüfungsbeschwerdeverfahren

Dr. Ulrich Wiesner
Az.: 2 BvC 3/07

nehmen wir zu den Berichten

- der Physikalisch-Technischen Bundesanstalt vom 24. Mai 2007
- des Chaos Computer Club e.V. vom 28. Mai 2007
- des Bundesministeriums des Inneren vom 5. Juni 2007

Stellung. Weitere Berichte liegen dem Beschwerdeführer nicht vor, auch keine Zustimmungen zu der Begründung des BMI bzw. des Bundestages hinsichtlich der Zurückweisung des Einspruchs. Wir erlauben uns zunächst einige Korrekturen und Ergänzungen der vorgebrachten technischen Aspekte und sodann eine Bewertung der rechtlichen Argumente.

Berliner Volksbank
BLZ 100 900 00
Kto. 520 522 20 08

HypoVereinsbank München
BLZ 700 202 70
Kto. 658 706 373

Insgesamt haben die Stellungnahmen die Position des Beschwerdeführers gestützt. In den wesentlichen Aspekten wurde der tatsächliche und rechtliche Vortrag aus dem Beschwerdeschriftsatz vom 12. Februar 2007 bestätigt, die abweichenden Ansichten führen zu keiner anderen Bewertung hinsichtlich der Verfassungswidrigkeit des Einsatzes von Wahlcomputern.

A. Zu den Tatsachen

I. Manipulationsszenarien

Die Analyse des Chaos Computer Clubs e.V. („CCC“) hat in nachvollziehbarer und überzeugend dokumentierter Form belegt, dass nicht nur das Risiko einer Manipulation durch den Austausch der Firmware besteht, sondern dass auch durch Manipulation der verschiedenen, in den Wahlcomputer befindlichen Hardwareelemente Wahlfälschungen vorgenommen werden können, die nicht oder nur mit erheblichem Aufwand ermittelt werden können. In einigen Konstellationen kann ein nachträglicher Nachweis von Manipulationen vermieden werden. Dies gilt etwa für Eingriffe in den Prozessorchip, das Tastenfeld und die Stimmspeichermodule.

Die Physikalisch-Technische Bundesanstalt bestätigt die vom Beschwerdeführer vorgetragene und vom CCC demonstrierte Manipulierbarkeit der Nedap-Geräte (Stellungnahme der PTB, S. 22). Unwidersprochen bleibt die Feststellung des Beschwerdeführers, das Ergebnis einer Wahl mit den Nedap-Geräten sei nicht geräteunabhängig überprüfbar und entziehe sich damit einer effektiven Wahlprüfung.

Durch die Analyse des CCC wird die Feststellung des Beschwerdeführers bestätigt, dass die Manipulationsgefahr weniger während des Ablaufs der Wahlhandlung besteht, sondern im Vorfeld bei der Wahlvorbereitung oder sogar noch davor währen des Herstellungs- und Auslieferungsprozesses der Geräte.

II. Schutz durch organisatorische Maßnahmen

Die PTB behauptet in ihrer Stellungnahme, die Wahl mit den Nedap-Geräten sei durch organisatorische Maßnahmen und durch die Aufbewahrung der Geräte in einer geschützten Umgebung durch die Gemeinden ausreichend sicher (Stellungnahme der PTB, S. 14 f.). Diese organisatorischen Maßnahmen und auch die geschützte Aufbewahrung sind jedoch weder durch entsprechende Vorschriften geregelt, noch finden sie in der Praxis statt, wie auch die Ausführungen des Chaos Computer Clubs belegen (Stellungnahme des CCC, S. 38 f.).

Hersteller, BMI und PTB haben die betroffenen Gemeinden offenbar nicht über die Schutzbedürftigkeit der Geräte informiert. So behauptete der Wahlleiter der Stadt Dortmund, Ernst-Otto Sommerer, der auch Sprecher der Nedap-Anwendergemeinschaft ist, noch bei einer Podiumsdiskussion am 30. Mai 2007 in Münster, dass eine erfolgreiche Manipulation der Geräte nur erfolgen könne, wenn die Geräte schon von der Gemeinde für die nächste Wahl konfiguriert worden seinen.

> Audio-Mitschnitt der Veranstaltung im Internet abrufbar unter http://www.demokratie-und-recht.de/wahlcomputer.html

Auch die Firma HSG-Wahlgeräte GmbH hatte noch im Mai 2006 auf ihrer Anwendertagung die Meinung vertreten, eine besondere Sicherheitsverwahrung der Geräte sei nicht erforderlich.

> Mitteilung der HSG Wahlsysteme GmbH vom 31.05.2006 (S. 3), bereits beigefügt als
>
> **Anlage B 21**

Das Schutzziel der sicheren Geräteaufbewahrung kann nicht erreicht werden, wenn die dafür verantwortlichen Gemeinden die Gefährdungssituation und die Schutzziele ganz offensichtlich nicht verste-

hen und irrtümlich annehmen, die Geräte müssten nur für einen kurzen Zeitraum vor der Wahl sicher aufbewahrt werden.

Ohnehin sind die organisatorischen Schutzmaßnahmen, wenn Sie denn tatsächlich angewandt würden, nicht geeignet, eine Manipulation der Wahlgeräte durch Innentäter etwa beim Hersteller oder bei der Gemeinde, zu verhindern. Deshalb können Sie eine wirksame Kontrolle der Wahl durch die Öffentlichkeit und Wahlvorstände keinesfalls ersetzen.

III. Bedeutung der Gefahr von „Innentätern“

Die Ausführungen des BMI und der PTB zu der Frage der Manipulationssicherheit zielen im Wesentlichen auf die Problematik eines „Außentäters“, der eine Wahlfälschung herbeiführen will (vgl. Stellungnahme der PTB, S. 14 f., 24 f.). Unabhängig von der insoweit existierenden und durch den Bericht des CCC bestätigten Gefahren durch Außentäter besteht das wesentliche Risiko darin, dass ein Innentäter eine Manipulation vornimmt.

Hier verweist die PTB auf Hersteller-Audits, auf das „langjährig bewährte Prinzip der Baumusterprüfung“ und den wirtschaftlichen Interessen des Herstellers an einem baugleichem Nachbau der Wahlcomputer (Stellungnahme der PTB, S. 6). Diese Auffassung geht an der Realität eines Manipulationsrisikos vorbei. Denn weder Hersteller-Audits noch eine Baumusterprüfung sind geeignet, einen Innentäter von einer Manipulation abzuhalten und gerade wirtschaftliche Aspekte könnten ein Grund für die Vornahme einer Manipulation sein.

Dabei kommt es auch nicht auf die Vertrauenswürdigkeit des Herstellers NEDAP an. Denn letztlich würde es ausreichen, dass eine einzige beim Hersteller tätige oder mit dem Transport befasste Person unzuverlässig ist. Der durch das BMI vorgenommene Vergleich mit dem Druck von Geldscheinen und Ausweisdokumenten (Stellungnahme

des BMI, S. 11) vermag hier nicht zu überzeugen. Nicht nur, dass die Sicherheitsvorkehrungen bezüglich der Bundesdruckerei GmbH weit über die Sicherheitsvorkehrungen hinsichtlich der Firma NEDAP hinausgehen, wesentlich ist vor allem der Umstand, dass Manipulationen von Ausweisdokumenten und beim Geldscheindruck rückverfolgt werden können (etwa durch die Nummerierung der Banknoten oder dem Vergleich der Angaben in einem Ausweisdokument mit anderen Dokumenten wie Geburtsurkunden), während die Nachverfolgung bestimmter Formen der Manipulation von Wahlcomputern nachträglich verhindert werden kann (vgl. Stellungnahme des CCC, S. 33, 39).

IV. Zeitpunkt und Wirksamkeit einer Manipulation

Das BMI, das in seiner Stellungnahme vom 5. Juni 2007 „vollinhaltlich" auf die Stellungnahme vom 3. Mai 2006 verweist, behauptet, die Nedap-Geräte enthielten lediglich Informationen über das Bundestagswahlsystem. Eine wirksame Manipulation der Wahl erfordere deshalb die Kenntnis der Tastenbelegung des konfigurierten Wahlgerätes. Eine solche Manipulation sei deshalb nur möglich, wenn das Gerät bereits für die Wahl konfiguriert sei. Dann aber sei das Gerät verschlossen und würde besonders geschützt aufbewahrt. Eine Manipulation an den Wahlgeräten erscheine deshalb so unwahrscheinlich, dass es einer besonderen amtlichen Überprüfung der einzelnen Geräte nicht bedürfe (Stellungnahme des BMI vom 3. Mai 2006, S. 13 und S. 25). Eine Manipulation der Gerätesoftware sei ohne Zugriff auf deren Quellcode ohnehin nicht möglich. Dieser befinde sich jedoch lediglich beim Hersteller und der PTB (Stellungnahme des BMI vom 3. Mai 2006, S.13).

Diese Behauptungen zur Manipulierbarkeit sind durch die erfolgreiche Manipulation der Nedap-Geräte durch Gonggrijp et. al. und den Chaos Computer Club nachvollziehbar und überzeugend widerlegt (Stellungnahme des CCC, S. 13 f.). Sie waren auch zuvor schon als falsch erkennbar. Gegenteiliges wird auch von der PTB nicht vorgetragen. Richtig ist, dass eine Manipulation zu jedem beliebigen Zeitpunkt zwi-

schen zwei Wahlen erfolgen kann. Eine Kenntnis der Tastaturbelegung ist nicht erforderlich, weil diese von einer manipulierten Software ermittelt werden kann. Hierzu muss der manipulierten Software lediglich der Name der zu begünstigenden Partei oder des zu begünstigenden Kandidaten bekannt sein. Nach diesen kann die Software die Konfigurationsdaten der jeweiligen Wahl durchsuchen (Stellungnahme des CCC, S. 13 und Anlage B 8, S. 4 f.). Somit bietet auch die vollständige Versiegelung der Wahlgeräte vor der Wahl keinen zusätzlichen Schutz, weil ein Angreifer bereits im Vorfeld tätig werden kann. Eine solche Manipulation kann auch Folgewahlen greifen, ohne dass ein erneuter Eingriff erforderlich ist. Im Übrigen kann zur Bedeutung von Innentätern auf die Ausführungen oben verwiesen werden.

V. Überprüfbarkeit des Ergebnisses

Das BMI behauptet weiterhin, durch Gegenüberstellung der Stimmabgabevermerke im Wählerverzeichnis mit der vom Gerät registrierten Stimmenzahl ließe sich überprüfen, ob das Gerät alle Stimmabgaben korrekt erfasst und addiert habe (Stellungnahme des BMI vom 3. Mai 2006, S. 21). Zudem werde jede Stimme mehrfach redundant gespeichert. Die gespeicherten Stimmen ließen sich auch zu einem späteren Zeitpunkt noch nachzählen und mit der Anwendungssoftware sogar als markierte Stimmzettel ausdrucken und per Hand nachzählen (Stellungnahme des BMI vom 3. Mai 2006, S. 22).

Der Abgleich der vom Gerät ausgegebenen Stimmenzahl mit den den Stimmabgabevermerken im Wählerverzeichnis bietet keinerlei Gewähr für die Richtigkeit des Wahlergebnisses. Mit einem solchen Abgleich kann lediglich bei Abweichungen bezüglich der Zahl der abgegebenen Stimmen ein falsches Ergebnis erkannt werden, nicht jedoch bei Übereinstimmung die Richtigkeit eines Ergebnisses verifiziert werden. Insbesondere kann mit einem solchen Abgleich nicht erkannt werden, ob Stimmen durch eine fehlerhafte oder manipulierte Software entgegen dem Wählerwillen falsch abgespeichert werden. Sol-

che falsch abgespeicherten Stimmen lassen sich auch durch wiederholtes elektronisches oder manuelles Nachzählen nicht mehr entdecken.

VI. Überprüfung durch Gemeinde und Wahlvorstand

Das BMI behauptet, die Gemeindebehörden würde im Rahmen der Wahlvorbereitung die Unversehrtheit der Siegel überprüfen, die vom Hersteller an der Geräteelektronik angebracht werden (Stellungnahme des BMI vom 3. Mai 2006, S. 4 und S. 8). Ferner wird behauptet, der Wahlvorstand vergleiche die Hard- und Softwareversionsnummern und Prüfsummen auf dem Prüfausdruck mit der Baugleichheitserklärung (Stellungnahme des BMI vom 3. Mai 2006, S. 8, S. 11).

Die Prüfschritte der Gemeinde sind in § 7 BWahlGV geregelt, der auf die Bedienungsanleitung des Herstellers verweist. § 10 BWahlGV regelt die Inbetriebnahme des Wahlgerätes durch den Wahlvorstand. Weder die BWahlGV noch die Bedienungsanleitung des Herstellers fordern die beiden erwähnten Prüfschritte. Sie finden daher in der Praxis offenbar auch nicht statt (Stellungnahme des CCC, S. 18). Die zahlreichen weiteren vom BMI aufgezählten Prüfschritte erwecken zwar den Eindruck einer umfassenden Prüfung, sie dienen jedoch in erster Linie dem Erkennen menschlicher und technischer Fehler. Sie laufen bei der Manipulation durch einen Innentäter ins Leere und können zudem die Integrität der Wahl nicht sicherstellen.

VII. Identifizierbarkeit der Software

Der Begriff Identität (von lat. idem, derselbe) bedeutet im wörtlichen Sinne „Übereinstimmung“ oder „Gleichheit“; Identifikation bedeutet entsprechend die Feststellung einer Übereinstimmung oder Gleichheit. Die Behauptung der PTB, mit der Forderung der Richtlinien für die Bauart von Wahlgeräten nach der eindeutigen Identifikation der

Software sei lediglich die eindeutige Bezeichnung der Software gemeint, ist deshalb weder umgangs- noch fachsprachlich haltbar. Die Gleichheit der in einem Nedap-Geräte installierten Software mit der Software des Baumusters ist, wie auch die PTB einräumt, anhand der angezeigten Prüfsummen nicht verifizierbar. Damit ist die Nedap-Software nicht, wie von der BWahlGV gefordert, eindeutig identifizierbar.

Der Prüfbericht der PTB vom 12. Mai 2004 (Anlage B 24 zur Wahlprüfungsbeschwerde, S. 21, Lfd. Nr. 6) belegt im Übrigen unmissverständlich, dass die PTB zum Zeitpunkt der Zertifizierung in den Prüfsummen einen ausreichenden Schutz vor der Manipulation der Software durch unbefugte Dritte gesehen hat. Dies ist jedoch, wie durch den CCC belegt (Stellungnahme des CCC, S. 18 f.), nicht der Fall.

VIII. Begriffe „Wahlcomputer“ und „Wahlgerät“

Die PTB vertritt die Auffassung, der von einem Beschwerdeführer verwendete Begriff „Wahlcomputer“ sei irreführend (Stellungnahme der PTB, S. 3). Dies trifft nicht zu. Mit dem Begriff „Computer“ bezeichnet man im allgemeinen Geräte, die Informationen mithilfe einer programmierbaren Rechenvorschrift verarbeiten. Dieser Begriff ist deshalb auch für softwaregesteuerte Wahlgeräte sachlich zutreffend. Denn bei solchen Geräten ist letztendlich durch das installierte Computerprogramm determiniert, wie die abgegebenen Stimmen gespeichert und gezählt werden. Dass der Begriff Computer auch für die Nedap-Geräte zutreffend ist, hat der CCC mit der Installation eines Schachprogramms belegt. Im Übrigen hat selbst die Firma Nedap ihre Geräte zunächst „Stemcomputer“ genannt.

Der Beschwerdeführer wendet sich in seiner Beschwerde gegen den Einsatz von Wahlcomputer im speziellen und nicht gegen Wahlgeräte im allgemeinen, weil gerade der Einsatz von softwaregesteuerten Geräten zu den monierten Transparenz- und Sicherheitsmängeln führt. Bei der Bundestagswahl 2005 sind laut Erfahrungsbericht des BMI (Anlage B 1 zur Wahlprüfungsbeschwerde) insgesamt 25 Wahlgeräte zum Einsatz gekommen, die keine Wahlcomputer waren. Sie sind nicht Gegenstand dieser Wahlprüfungsbeschwerde.

Mechanische Wahlgeräte und Wahlcomputer funktionieren grundsätzlich verschieden und sind auch hinsichtlich der Manipulationsgefahr und der Vorverlagerung von Risiken nicht vergleichbar. Daher ist es nicht nachvollziehbar, wenn das BMI (Stellungnahme des BMI, S. 2) und die PTB von einer bloß irrelevanten Weiterentwicklung vorbestehender Wahlgeräte ausgehen und die Risiken von mechanischen Wahlgeräten und Wahlcomputern als vergleichbar ansehen. Bei mechanischen Wahlgeräten sind Manipulationen an dem Gerät reproduzierbar, so dass die Öffentlichkeit im Vorfeld der Wahl nicht gleichem Maße betroffen ist.

IX. Prüfverfahren und Prüferfahrung der PTB

Die PTB geht in ihrer Stellungnahme ausführlich auf das Prüfverfahren und die langjährige Erfahrung im Umgang auch mit mechanischen und elektromechanischen Wahlgeräten ein. Das aufwändige Verfahren erfordere in der Regel mehrmaliges Nachbessern durch den Hersteller (Stellungnahme der PTB, S. 8) und habe in der Vergangenheit

verschiedene Wahlgerätehersteller von einer Zertifizierung ihrer Geräte abgehalten (Stellungnahme der PTB, S. 12). Darauf kommt es jedoch nicht an. Relevant ist ausschließlich, ob das Prüf- und Zulassungsverfahren im Ergebnis dazu führt, dass nur Wahlgeräte zugelassen werden, die in ihren funktionalen und technischen Merkmalen die sichere Durchführung von demokratischen Wahlen unter Einhaltung der Wahlrechtsgrundsätze erlauben. Dies ist derzeit offensichtlich nicht der Fall, denn die zugelassenen Wahlgeräte erfüllen nicht einmal die von der PTB mitentwickelten, einfach-rechtlichen Vorschriften der Richtlinien für die Bauart von Wahlgeräten, insbesondere hinsichtlich dem allgemeinen Stand der Technik für Anwendungen hoher Kritikalität, der Erkennbarkeit von Software-Manipulationen und der eindeutigen Identifizierbarkeit der Software (s.u. Abschnitt B.I.).

Der Umstand, dass auch das öffentliche Bekanntwerden sicherheits- und konstruktionstechnischen Mängel nicht zu einer Rücknahme oder wenigstens vorübergehenden Suspendierung der Bauartzulassung für die Nedap-Geräte geführt hat, zeigt zudem, dass systematische Regelungslücken im Umgang mit solchen Ereignissen existieren. Im Ergebnis führt dies dazu, dass die Nedap-Geräte trotz ihrer bekannten Mängel weiterhin eingesetzt werden. Zunächst ist dies bei Landtags- und Kommunalwahlen der Fall, weil einige Bundesländer auf ein eigenes Zulassungsverfahren verzichten oder eine Bauart dann zulassen, wenn diese für Bundestag- und Europawahlen zugelassen ist. Entsprechende landesrechtliche Regelungen bestehen etwa in Hessen (§ 1 Abs. 2 WahlGV), Rheinland-Pfalz (§2 Abs. 2 LWgVO) und Sachsen Anhalt (§ 2 Abs. 1 LWGer-VO und § 2 Abs. 1 KWGer-VO).

X. Beachtete Sicherheitsnormen

Die PTB versucht durch die Aufzählung zahlreicher technischer Normen zu belegen, die Geräte seien besonders sorgfältig geprüft und durch der Anwendung einschlägiger Software-Qualitätsstandards besonders sicher (Stellungnahme der PTB, S. 9 und S. 26). Dabei werden

die Normen IEC 61508 und ITSEC im Bezug auf die Sicherheit herausgestellt, ohne dass die PTB weiter ausführt, wie durch Anwendung dieser Normen Sicherheit gewährleistet wird.

Die erste Norm (IEC 61508, „Functional safety of electrical/ electronic/ programmable electronic safety-related systems“) regelt Anforderungen an die Ausfallsicherheit sicherheitsrelevanter Systeme. Sie soll gewährleisten, dass z.B. alterungsbedingte Hardware-Defekte durch rechtzeitige Diagnose oder redundante Auslegung des Systems nicht zum Versagen der Sicherheitsfunktionalität führen. Dass sich diese Norm mit Sicherheit im Sinne von „safety“ und nicht im Sinne von „security“ beschäftigt, geht schon aus ihrem Namen hervor. Der Beschwerdeführer hat die Ausfallsicherheit der eingesetzten Wahlgeräte nicht bemängelt, der Vortrag der PTB ist deshalb in diesem Zusammenhang sachlich irrelevant.

Die zweite im Zusammenhang mit Software-Sicherheit erwähnte Norm (ITSEC, „Information Technology Security Evaluation Criteria“) definiert tatsächlich Anforderungen an die Vertrauenswürdigkeit von Computersystemen. Diese Norm gibt keine bestimmten Sicherheitsanforderungen vor, sondern definiert einen formalenProzess, in dem die Sicherheitsanforderungen eines Systems zu definieren und anschließend zu validieren sind.

Die Norm unterscheidet u.a. bestimmte Funktionalitätsklassen (z.B. hinsichtlich der Ausfallsicherheit und Zugriffskontrolle), die Mindeststärke bestimmter Schutzstärken und Evaluationsstufen hinsichtlich deren Validierung. Die tatsächlichen Anhaltspunkte sprechen dagegen, dass einem solchen Zertifizierungsprozess gemäß ITSEC tatsächlich gefolgt wird. So fehlt es schon an der formalen Definition des geforderten Schutzes. Eine solche Definition wird weder im Prüfkonzept der PTB vom 11. April 2006 aufgeführt (Anlage B 25 zur Wahlprüfungsbeschwerde), noch im Prüfbericht vom 12. Mai 2004 dokumentiert (Anlage B 24). Die Definition solcher Anforderungen wird von der PTB auch nicht behauptet. Zudem sind weder IEC 61508 noch ITSEC

unter den etwa 30 Normen zu finden, die im Prüfkonzept der PTB aufgezählt werden. Es ist schwer vorstellbar, dass die PTB systematisch gegen bestimmte Normen prüft, diese aber bei der Dokumentation des Prüfkonzeptes und der Prüfergebnisse nicht aufführt.

XI. Übertragbarkeit der Ergebnisse der Manipulation von niederländischen Geräten auf die bei der Bundestagswahl verwendeten Geräte

Die PTB behauptet, die Ergebnisse der Stiftung *Wij vertrouwen stemcomputers niet* seien nicht auf die deutschen Geräte übertragbar . Die deutschen Geräte seien von den niederländischen Geräten signifikant verschieden, ein gegenteiliges Gutachten der niederländischen Prüfbehörde TNO sei nicht in diesem Sinne zu verstehen (Stellungnahme der PTB, S. 21 f.). Im Übrigen könne die PTB die Hardwaredifferenzen zwischen der niederländischen Bauart ES3B und der deutschen Bauart ESD1 nicht bewerten, weil die genaue Identifikation der Bauart im TNO-Gutachten fehle (Stellungnahme der PTB,, S. 21 f.). Die fünf in Deutschland zugelassenen Bauarten unterschieden sich zum Teil stark (Stellungnahme der PTB, S. 7).

Das Gutachten der TNO stammt vom 12. Februar 2002. Zu diesem Zeitpunkt (und darüber hinaus bis Mitte 2004) waren in Deutschland ausschließlich Bauarten der Baureihe ESD1 mit Hardwareversion 1.02 zugelassen (Gesamtliste der PTB-Prüfberichte vom 30. August 2006, Anlage B 28 zur Wahlprüfungsbeschwerde). Da für den Einsatz in den Niederlanden die Software ausgetauscht wird (durch Ersetzen der EPROMS, ebenso wie bei der Manipulation der Geräte durch den Chaos Computer Club), spielen die verschiedenen Softwareversionen für den Vergleich der Baureihen keine Rolle.

Geräte dieser Hardwareversion sind u.a. von den Städten Köln und Dortmund angeschafft worden. Schon wegen den hohen Stückzahlen

in diesen beiden Städten sind diese Hardwareversionen bei der Bundestagswahl 2005 am häufigsten zum Einsatz gekommen.

Bei der niederländischen Parlamentswahl im November 2006 hat die Stadt Dortmund ihre Geräte in die Niederlande ausgeliehen, weil dort nach dem Widerruf der Bauartzulassung für Wahlgeräte eines anderen Herstellers die Wahldurchführung gefährdet war (Bericht von Heise-Online vom 21.11.2006, Anlage B 23). Für den Einsatz in den Niederlanden sind die Geräte vom Hersteller mit einer niederländischen Gerätesoftware ausgestattet worden. Damit hat der Hersteller in der Praxis demonstriert, dass die Erkenntnisse des Hacks der niederländischen Geräte auch auf deutsche Geräte übertragbar sind, nämlich dass sich die Geräte durch Austausch der Software entgegen ihrer ursprünglichen Bestimmung verwenden lassen.

Der Aussage der PTB, die fünf in Deutschland zugelassenen Bauarten würden sich zum Teil erheblich unterscheiden, wird in der Stellungnahme der PTB nicht weiter substantiiert. Die Unterschiede der Bauarten sind für die vom Beschwerdeführer vorgetragenen Monita allerdings auch nicht relevant. Alle fünf Bauarten weisen die selben Mängel hinsichtlich der Transparenz des Wahlgeschäfts und der Stimmenauszählung sowie hinsichtlich der Überprüfbarkeit des Wahlergebnisses auf. Auch unterscheiden Sie sich nicht in ihrem Schutz vor Manipulationen der eingesetzten Software und gegen die anderen vom CCC dargestellten Angriffsmöglichkeiten.

Die in Deutschland für Bundestagswahlen zugelassenen fünf Bauarten sind sich immerhin ähnlich genug, dass die Version 3.08 der Gerätesoftware auf drei der vier Hardware-Versionen (ESD1 1.03 und 1.04 sowie ESD2 1.01) zum Einsatz kommt. Es ist nicht einsichtig, warum sich die Geräte dann ausgerechnet in ihrer Sicherheit vor Softwaremanipulationen unterscheiden sollten.

Die Unterschiede der Hardwareversionen ESD1 1.03 und 1.04 zur Hardwareversion ESD1 1.02 sind im Prüfbericht der PTB vom 12. Mai

2004 beschrieben (Anlage B 24 zur Wahlprüfbeschwerde, S. 6). Demnach verfügen die neuen Hardware-Versionen über eine verbesserten Schutz gegen Unterbrechungen der Stromversorgung. Außerdem finden in den Speichermodulen nun elektronische Bauelemente unterschiedlicher Bauart Verwendung, ohne dass dies Einfluss auf Funktionalität oder die logische Verschaltung hätte. Zudem sei die feste Taste zur ungültigen Stimmabgabe entfallen und müsse nun auf dem Gerätestimmzettel programmiert werden.

Die Unterschiede der Softwareversion 3.08 zu den Softwareversionen 2.02 und 2.07 sind im selben Prüfbericht beschrieben (S. 6 f.). Demnach kann die neue Software nun auch Wahlen mit Kumulieren und Panaschieren mit bis zu drei Stimmen, Wahlen nach dem Mitbestimmungsgesetz und Umfragen darstellen. Außerdem kann die Stimmabgabe und -korrektur nun auch über frei definierbare Tasten auf dem Gerätestimmzettel erfolgen. Auch verfügt die Software über eine verbesserte Selbstdiagnose.

Sowohl für die Unterschiede der Hardware als auch die der Software gilt: die Unterschiede sind für die vorgetragenen Monita allesamt irrelevant. Allen Bauarten fehlt gleichermaßen ein ausreichender Manipulationsschutz, die Geräte entsprechen mindestens in dieser Hinsicht nicht dem Stand der Technik. Keine der Bauarten ermöglicht eine Eindeutige Identifikation der installierten Software oder ein Erkennen von Softwaremanipulationen.

XII. Bewertung des Berichts der irischen Kommission

Es wurde bereits ausführlich auf die unzutreffende Interpretation des irischen Kommisionsberichtes durch die PTB eingegangen (Wahlprüfungsbeschwerde, Anlage B 5). Es wird vorliegend nicht bestritten, dass die zentrale Auszählung der Stimmen in Irland mit zusätzlichen Risiken verbunden ist, die in Deutschland nicht bestehen. Dies bedeu-

tet jedoch nicht, dass die negative Bewertung übertragbarer Aspekte deshalb vernachlässigbar wäre.

Zahlreiche in den Niederlanden identifizierte Mängel und vom CCC diskutierten Manipulationsmöglichkeiten finden sich bereits im ersten Bericht der irischen Kommission für elektronische Wahlen:

- Verwendung des unzureichenden Design-Konzeptes Security by Obscurity (First Report of the CEV, 2004, S. 129)
- Mangelnder Schutz gegen einen Austausch der Gerätesoftware durch eine manipulierte Version und die Möglichkeit der Durchführung einer solchen Manipulation innerhalb von zwei Minuten (CEV 2004, S. 139, S. 189)
- Unzureichende Schutzwirkung der Herstellerversiegelung an der Geräteelektronik (CEV 2004, S. 140)
- Unzureichender Schutz der Stimmenspeicher gegen Veränderung der Stimmen nach der Wahl (CEV 2004, S. 141)
- Möglichkeit des Austauschens der Elektronik des Stimmenspeichers vor der Wahl, um eine falsche Speicherung der Stimmen zu erzielen (CEV 2004, S. 164f, S. 189)
- Möglichkeit des Vorhandenseins von „Hintertüren“ in der Software (CEV 2004, S 148)

Diese Mängel bestehen ganz unabhängig davon, ob eine zentrale Auszählung der Stimmen stattfindet oder nicht.

B. Zu den Rechtsfragen

Das BMI hat bestätigt, dass der Grundsatz der Öffentlichkeit der Wahl eine Grundvoraussetzung für die demokratische und rechtsstaatliche Willensbildung ist (Stellungnahme des BMI, S. 3). Insofern besteht – soweit ersichtlich – allgemeine Einigkeit. Abweichende Auffassungen bestehen hingegen hinsichtlich der Bedeutung dieses Verfassungsgrundsatzes für das einfache Recht und seinen rechtlichen Grenzen sowie hinsichtlich der Auslegung des einfachen Rechts. Nachfolgend

wird dazu ebenso Stellung genommen (I.) wie zum Grundsatz der Öffentlichkeit der Wahl (II.) und zur Mandatsrelevanz (III.).

I. Verstoß gegen einfaches Recht

Die technische Analyse des CCC hat deutlich gemacht, dass allen Bauarten der Nedap-Wahlcomputer gleichermaßen ein ausreichender Manipulationsschutz fehlt. Die Geräte entsprechen zumindest in dieser Hinsicht bei weitem nicht dem Stand der Technik und verstoßen gegen B 2.1 der Anlage 1 zur BWahlGV. Dort heißt es:

„Das Wahlgerät entspricht in seiner Konstruktion dem allgemeinen Stand der Technik und ist unter Beachtung der für Systeme mit schwerwiegenden Schadensfolgen bei Fehlverhalten (hohe Kritikalität) anerkannten Regeln der Technik aufgebaut.
Das Wahlgerät ist so konstruiert, daß eine Veränderung des technischen Aufbaus und bei rechnergesteuerten Geräten auch der installierten Software durch unbefugte Dritte nicht unbemerkt bleibt."

Auch die Anforderung zur Identifizierbarkeit (*„Eindeutige Identifikation der installierten Software bei rechnergesteuertem Wahlgerät"*, B 1 der Anlage 1 zur BWahlGV) wird durch die bei der Bundestagswahl eingesetzten Geräte nicht erfüllt.

Für die Details kann auf die Stellungnahme des CCC verwiesen werden.

II. Grundsatz der Öffentlichkeit der Wahl

Weder die Regelungen des einfachen Rechts noch deren praktische Umsetzung genügt dem Grundsatz der Öffentlichkeit der Wahl. Anders als das BMI glaubt, stellen die vom Beschwerdeführer geltend

gemacht Bedenken keine „Überspannung“ des Öffentlichkeitsprinzips dar, sondern ergeben sich aus den technischen Tatsachen.

1. Verhältnis des Grundsatzes der Öffentlichkeit der Wahl zum einfachen Recht

Das BMI ist der Auffassung, dass der Grundsatz der Öffentlichkeit der Wahl beachtet worden sei, weil keine Verletzung der einfachgesetzlichen Vorgaben der §§ 10 und 31 BWG vorliege (Stellungnahme des BMI, S. 3, 6). Der Grundsatz der Öffentlichkeit gelte „nach dem Gesetzeswortlaut“ nicht für die Arbeit der anderen an der Vor- und Nachbereitung der Wahl beteiligten Institutionen (Stellungnahme des BMI, S. 4 a.E.).

Das BMI begeht hier einen unzulässigen Zirkelschluss. Der Umfang des Grundsatzes der Öffentlichkeit ergibt sich nicht aus dem einfachen Recht, sondern aus dem Verfassungsrecht. Dem entsprechend besagt die Einhaltung der einfachrechtlichen Vorschriften auch nichts über die Verfassungsmäßigkeit des Wahlablaufs bei der Bundestagswahl 2005. Wie nachfolgend nochmals dargelegt wird, ergibt sich aus dem Einsatz von Wahlcomputer eine Verschiebung der Kontrollmöglichkeiten, die zwingend eine Anwendung des Grundsatzes der Öffentlichkeit auf Handlungen im Vorfeld der eigentlichen Wahl erfordert.

2. Bedeutung des Grundsatzes der Öffentlichkeit der Wahl für die Wahlvorbereitung

Wie bereits dargestellt wurde, handelt es sich bei Wahlcomputern nicht bloß um eine weitere Entwicklungsstufe mechanischer Wahlgeräte, sondern um eine neue Art der Stimmabgabe, die zu neuen Gefährdungen geführt hat. Da das wesentliche Risiko eben nicht bei Manipulationen während der Wahlhandlung liegt, sondern bei Manipulationen im Vorfeld, führt eine bloße Beachtung der bestehenden Vor-

schriften zur Öffentlichkeit während der Wahlhandlung zu keinem Schutz vor Wahlfälschungen und entsprechend auch nicht geeignet, das Vertrauen der Bürger in die Korrektheit der Wahl zu sichern. Denn wenn für die Wahlausschüsse und Wahlvorstände bzw. die während der Wahlhandlung anwesenden Bürger keine Möglichkeit besteht, etwaige Manipulationen zu erkennen, verkommt der Öffentlichkeitsgrundsatz zur Farce, ist inhaltlich entleerte Hülle. Der Zweck des Grundsatzes der Öffentlichkeit, wie ihn auch das BMI annimmt, kann nicht erfüllt werden.

Die vom CCC nachvollziehbar uns überzeugend dargelegten Angriffszenarien sind während des Zeitraums, für den bislang die Öffentlichkeit gewährleistet ist, nicht aufzudecken. Nur eine Nachvollziehbarkeit und Überprüfbarkeit des gesamten Herstellungsprozesses durch die Öffentlichkeit würde zusammen mit einer Identitätsüberprüfung jedes einzelnen Geräts einen hinreichenden Schutz gewähren.

Hier liegt auch der wesentliche Unterschied zu anderen Handlungen der Wahlvorbereitung. Während beim Druck von Wahlbenachrichtigungen und Stimmzetteln keine Wahlfälschungen vorbereitet werden können, die während des Wahlvorgangs nicht mehr aufdeckbar wären, kann bei einer Manipulation von Wahlcomputern eine unentdeckbare Wahlfälschung vorgenommen werden.

3. Eignung der Öffentlichkeit zur Erreichung der damit bezweckten Ziele

Das BMI merkt richtig an, dass eine Offenlegung des Quellcodes der verwendeten Software nur eine Spezialistenöffentlichkeit herstellen würde, da nur Fachleute in der Lage wären, den Quellcode zu verstehen (Stellungnahme des BMI, S. 6). Dem ist ebenso zuzustimmen wie der Auffassung des CCC, dass ein höheres technisches Schutzniveau zwangsläufig zu komplexeren Systemen führt, die von noch weniger Menschen verifiziert werden können (Stellungnahme des CCC, S. 54).

Aus diesen zutreffenden Prämissen müssen jedoch die verfassungsrechtlich richtigen Folgerungen gezogen werden. Anders als das BMI meint, kann dies nicht zu dem Schluss führen, dass dann eben überhaupt keine öffentliche Kontrolle zuzulassen ist. Denn damit würde der Grundsatz der Öffentlichkeit insgesamt entwertet. Solange ein hinreichender technischer Schutz von Wahlcomputern vor Manipulationen und eine allgemeine Überprüfbarkeit durch jedermann nicht nebeneinander möglich sind, kann dies nur bedeuten, dass Wahlcomputer überhaupt nicht in verfassungsrechtlich zulässiger Weise eingesetzt werden können.

4. Hinreichender Schutz von Manipulationen durch begleitende Maßnahmen?

Der Beschwerdeführer stimmt der Ansicht zu, dass auch die Urnenwahl nicht vollständig manipulationssicher ist und die Korrektheit der Wahl durch begleitende Maßnahmen sicherzustellen ist. Das BMI betont in diesem Zusammenhang ganz zu Recht die Bedeutung der dezentralen Organisation der Wahl (Stellungnahme des BMI, S. 10).

Allerdings ist die Bedeutung der dezentralen Organisation auf Manipulationsversuche während der Lagerung der Wahlgeräte und der Wahl selbst beschränkt. Unabhängig von den dort vorliegenden und vom CCC dokumentierten Problemen, läuft dieser Schutz durch begleitende Maßnahmen bei Innentätern und im Vorfeld der Wahl ins Leere. Gerade das Modell der Baugleichheitserklärung ist ein Element der *zentralen* Organisation und keineswegs geeignet einen zusätzlichen Schutz zur Öffentlichkeit zu gewährleisten.

Weiterhin ist zu berücksichtigen, dass das Ausmaß einer Manipulation eine vollständig andere Dimension hätte, wenn bereits bei der Herstellung oder Auslieferung der Wahlcomputer eine Manipulation vorgenommen würde. Während eine Manipulation bei der Urnenwahl im

Regelfall nur ein Wahllokal betrifft, kann es durch Manipulationen an den Geräten zu einer wesentlich umfassenderen Fälschung kommen, die zudem nachträglich nicht nachweisbar ist, wenn etwa im Rahmen der Wartung oder bei der Entleihe für eine andere Wahl eine Softwareversion aufgespielt wird. So ist an den von der Stadt Dortmund an die Niederlande ausgeliehenen Geräten keine Wahlmanipulation nachweisbar.

Die PTB hat bei der Aufstellung der sicherheitsbezogenen Anforderungen vorausgesetzt, dass Wahlfälschungen strafbewehrt sind (Stellungnahme der PTB, S. 15). Durch die Vorverlagerung von Manipulationsrisiken ist es allerdings fraglich, ob etwa eine Manipulation beim Hersteller in den Niederlanden tatsächlich strafbar wäre. So wird die einschlägige Norm des § 107a StGB nicht im Katalog des § 5 StGB über Auslandstaten gegen inländische Rechtsgüter aufgeführt. Auch § 7 StGB führt zu keiner Strafbarkeit, wenn der Täter kein deutscher Staatsangehöriger wäre.

5. Begrenzungen des Grundsatzes der Öffentlichkeit

Die vom BMI vorgebrachten Argumente für eine Begrenzung des Grundsatzes der Öffentlichkeit der Wahl vermögen nicht zu überzeugen.

Dies gilt zunächst für Grundrechte beteiligter Unternehmen, etwa der Schutz von Betriebsgeheimnissen. Zutreffend ist die Auffassung des BMI, dass gegenwärtig keine Informationsansprüche von Bürgern gegen NEDAP oder andere betroffene Unternehmen bestehen. Dies betrifft insbesondere die Einsicht in den Quellcode. Dieser Befund bedeutet jedoch nicht, dass sich daraus eine Beschränkung von verfassungsrechtlichen Grundsätzen ergibt. Zunächst könnte die Bundeswahlgeräteverordnung durchaus so ausgestaltet sein, dass nur Wahlgeräte von Anbietern zuzulassen sind, für die auch jedermann Einsicht in den Quellcode und andere relevante Unterlagen gewährt wird.

Entscheidend ist aber der Gesichtspunkt, dass bei der Durchführung einer Urnenwahl überhaupt keine Betriebsgeheimnisse Dritter betroffen sind, die zur Verwirklichung des Grundsatzes der Öffentlichkeit beeinträchtigt werden müssten. Wenn der Grundsatz der Öffentlichkeit der Wahl wegen entgegenstehender Grundrechte Dritter nicht verwirklicht werden kann, dann folgt daraus nicht die Beschränkbarkeit des Verfassungsgrundsatzes, sondern die Erkenntnis, dass dann eine herkömmliche Urnenwahl anstatt der Verwendung von Wahlcomputern geboten ist. Dies gilt umso mehr, als mit dem Einsatz von Wahlcomputern keine Vorteile verbunden sind, die verfassungsrechtliche Beschränkungen rechtfertigen würden (vgl. Schriftsatz vom 12. Februar 2007, S. 78 ff.).

Auch der Verweis auf die Briefwahl verfängt nicht. Die beschränkte Überprüfbarkeit bei der Briefwahl ist nur vor dem Hintergrund entsprechender Vorteile für die Wahlbeteiligung zu rechtfertigen (vgl. BVerfGE 59, 119 (124)) und auch nur in beschränktem Rahmen. Da Wahlcomputer nicht als nachrangige Alternative, sondern als Substitut für die Urnenwahl eingesetzt werden, ist eine Vergleichbarkeit nicht gegeben.

Das BMI zeichnet ein falsches Bild, wenn die Verwirklichung des Grundsatzes der Öffentlichkeit im Vorfeld der Wahl mit dem Hinweis auf „eine sich selbst blockierende Demokratie“ abgelehnt wird. Allein entscheidend ist, dass der Zweck des Öffentlichkeitsprinzips hinreichend durch die Ausgestaltung des einfachen Wahlrechts verwirklicht wird. Wegen der Vorverlagerung des Manipulationsrisikos ist es eben nicht mehr ausreichend, dass die Wahlhandlung selbst öffentlich ist. Hier dürfen die Augen nicht davor verschlossen werden, dass sich die Gefährdungslage grundlegend geändert hat und die Wahlgesetze dies nicht ausreichend berücksichtigen.

II. Mandatsrelevanz

Ohne weitere Begründung hält es das BMI für irrelevant, dass die gerügten Wahlfehler die Möglichkeit beseitigt haben, Manipulationen konkret zu belegen. Wollte man dieser Auffassung folgen, würde dies nur zusätzlich die Annahme bestärken, dass Wahlcomputer gänzlich ungeeignet sind für eine demokratische Wahl. Ansonsten würde man bewusst die Möglichkeit aufgeben, Wahlfälschungen aufzudecken und manipulierte Wahlen nachträglich zu korrigieren. Die gesamte Wahlprüfung nach Art. 41 GG wäre Makulatur.

Bei richtigem Verständnis dient das Merkmal Mandatsrelevanz dazu, die Wirksamkeit der Wahl zu bewahren, wenn der Wahlfehler für das Ergebnis irrelevant war. Dann mangelt es aber einer Mandatsrelevanz nur in dem Fall, dass der Wahlfehler wegen der Stimmenverteilung oder wegen des Umfangs einer Manipulation keine Auswirkungen hat. Sofern sich Wahlfehler jedoch derart auswirken, dass Auswirkungen auf die Stimmverteilung zumindest möglich sind, besteht auch die erforderliche Mandatsrelevanz. Dieser Auffassung entsprechen auch die bereits zitierten Urteile des OVG Koblenz und des Bundesarbeitsgerichts (Schriftsatz vom 12. Februar 2007, S. 93 f.), denen auch das BMI inhaltlich nicht entgegengetreten ist.

Neben der großen Zahl der Wähler, die mit Wahlcomputer ihre Stimme abgeben mussten, ist vorliegend auch die Schwere der Wahlfehler zu berücksichtigen. Da insofern überhaupt keine hinreichend öffentliche Kontrolle der Wahlgeräte stattgefunden hat, können die entsprechenden Wahlfehler auch nicht sanktionslos bleiben.

Prof. Dr. Ulrich Karpen

Dr. Till Jaeger
Rechtsanwalt