Digitaler Wandel in Estland

Robert Terbach
Universität Leipzig
Seminar "Wissen in der modernen Gesellschaft"
Wintersemester 2014/2015

31. März 2015

Inhaltsverzeichnis

1 Einführung

Das Internet war zuerst eine akademische Angelegenheit, Wissenschaftler tauschten ihre Ergebnisse, Fragen und Rechenkapazitäten miteinander aus. Dann wurde es für die breite Masse verfügbar, es ermöglicht Jedem mit jedem Anderen schnell zu kommunizieren. Heute ist es praktisch von riesigen Konzernen kontrolliert, die mit den Daten ihrer Nutzer Milliarden verdienen, es hat sich sehr stark kommerzialisiert. Parallel ist auszumachen, wie die Regierungen und Gesellschaften der Welt sich das Internet zu Nutze machen wollen. Im sogenannten Arabischen Frühling spielt das Internet eine große Rolle beim Umsturz der unterdrückenden Regierungen. In Russland oder China dient es als mächtiges Propagandainstrument. Manch ein Politiker ist sich noch unklar darüber, welche Möglichkeiten von Regierungsseite das Medium bietet[1].
Einen Schritt weiter ist bereits der erst junge Staat Estland und zieht damit international viel Aufmerksamkeit auf sich. Ohne finanzielle Altlasten oder gewachsene behindernde Strukturen haben sie einen radikalen Umschwung von der technologischen Brache, die die Sowjetunion hinterließ, vollführt und gelten heute vielerorts als Vorreiter im digitalen Staatswesen. *E-stonia*, wie der Präsident sein Land liebevoll nennt[2], ist in aller Munde. Es fällt in einem Atemzug mit dem Silicon Valley, sogar die Staatsbürgerschaft wird in die elektronische Welt überführt. Estland trägt seine sozio-technologische Revolution nach außen.
Die Dystopien aus George Orwells 1984 oder Gattaca[1] hingegen führen für die Einwohner technologisierter Staaten zu Unfreiheit, gar totaler Überwachung. Insbesondere in 1984 kann der Protagonist nie sicher sein ob er beobachtet wird oder nicht. Er hat keine Privatsphäre, kann sich niemals unerkannt durch die Stadt und sogar die umgebende Natur bewegen und muss sich dementsprechend verhalten. Weil er das nicht tut, führt es ihn in die Katastrophe.
Bisher nutzen die Esten die digitalen Dienste ihres Staates gerne: Amtsgänge führen nicht zu stundenlangen Wartezeiten und die Steuererklärung oder ein Auto anmelden ist in wenigen Minuten gemacht. Es scheint sich gar größeres Vertrauen in den Staatsapparat aufzubauen. Hier sollen die in

[1] `http://www.imdb.com/title/tt0119177/`

Estland verwendeten Technologien sowie Gesetze erläutert werden, auf denen das öffentliche Leben grundlegend aufbaut, damit bewertet werden kann ob Estland es schafft die Freiheit des Einzelnen und der Gesellschaft nicht zu gefährden. Ziel ist die Erkundung der Frage ob es sogar zu einer größeren Freiheit und Mitbestimmung führen kann.

2 Historischer Überblick

Die wirtschaftliche Isolation durch die Sowjetunion hat Estland nach der erneuten Unabhängigkeit weiterhin eng an Russland gebunden. Um diesem Verhältnis zu entkommen hat sich das Land radikal erneuert und eine Neuausrichtung sowohl gesellschaftlich, als auch wirtschaftlich gewagt, mit modernsten Mitteln soll das Land international konkurrenzfähig sein. Das Wort *erneut* deutet bereits die bewegte Geschichte Estlands an, die im Folgenden zusammengefasst werden soll, um ein historisches Verständnis für die aktuellen Geschehnisse entwickeln zu können.
Im Mittelalter waren estnische Städte Teil der Hanse und durch internationalen Handel geprägt. Lange Zeit war das Land freiwillig ein Teil Schwedens, wurde jedoch im Jahr 1710 Russland angegliedert. Die Bevölkerung war in zwei Schichten aufgeteilt, die Baltendeutsche Oberschicht und estnischsprachige Bauern. Die Russischen Besetzer ermöglichten den Esten selbst Land zu erwerben und teilhabe am Bildungssystem. Mit Gründung der ersten estnischsprachigen Zeitung in den 1850ern begannen die aufkommenden eigenen Intellektuellen eine eigene kulturelle Identität aufzubauen. Auf ihrer Sprache basierend konnten sich die Esten gegenüber den Russen und Deutschen absetzen und gründeten ihre eigenen Kultur schaffenden Vereine, etwa Chöre oder Orchester[3].
Ende des 19. Jahrhunderts jedoch starteten die Zaren jedoch eine Russifizierungsinitiative. An Schulen sollte von da an Russisch gelehrt werden und das Selbstbewusstsein ein russisches werden. Auch die nach wie vor auf Deutsch funktionierenden Einrichtungen, etwa das Rechtssystem oder die Universität wurden umgestellt und wichtigste Ämter mit Russen besetzt. Der aufkommende eigene Nationalstolz der einverleibten Staaten sollte begraben werden[4].
Die Beendigung der Klassengesellschaft und dafür weitere Entfremdung von

den Obrigkeiten sorgten stattdessen für eine Stärkung der Estnischen Identität. Die Urbanisierung und Industrialisierung ermöglichten breiteren Bevölkerungsschichten Zugang zu höherer Bildung, die entstehenden Eliten gründeten Parteien und konnten erstmals 1904 die Kommunalwahlen in Tallinn gewinnen[5]. Erst nach der Oktoberrevolution 1917 jedoch konnten sich die Esten nach gescheiterten Versuchen tatsächlich Unabhängig erklären[6], welche jedoch nur durch den Freiheitskrieg 1918-1920 durchgesetzt werden konnte[7]. Im *Frieden von Tartu* erkannte Sowjetrussland Estland auf alle Zeit als selbständigen demokratischen Staat an[8].
Die Freiheit ändere Jäh im zweiten Weltkrieg, der für Estland in erneuter Besatzung durch die Sowjetunion endete. Die Baltendeutschen wurden vertrieben, viele Esten deportiert und ermordet, stattdessen wurden viele Russen angesiedelt[6], sodass diese einen Bevölkerungsanteil von über 25% stellen[9]. Durch die Nähe zu Finnland war Estland jedoch nicht völlig von Europa isoliert, dortiges Fernsehen konnte empfangen werden und die westlichen Mächte setzten Radiosender wie etwa Radio Free Europe gezielt der Propaganda hinter dem Eisernen Vorhang entgegen[10]. Die sogenannte Singende Revolution läutete während des sich bereits androhenden Zerfalls der Sowjetunion die Wende ein[11]. Insbesondere die Kulturschaffenden des Landes konnten durch Besinnung auf estnisches Nationalgut viele Bürger zu erneuten Demokratiebewegungen motivieren. Es wurden viele Konzerte und Festivals im ganzen Land organisiert und erstmals wieder die unter den Sowjets verbotene Nationalhymne gesungen. Die ersten Versuche wurden von Moskau nicht anerkannt, die Bewegung war aber nicht mehr aufzuhalten, sodass im Jahr 1990 die Dritte Republik Estland deklariert wurde[12]. Während des Putsches in Moskau im August 1991 konnte die Souveränität, gemeinsam mit Litauen und Lettland, durchgesetzt und die volle Unabhängigkeit zurückerlangt werden[6].
2004 folgte der Beitritt in die NATO, sowie der OECD, 2011 die Einführung des Euro. Das heutige Estland hat bei einer Größe von 45.227km^2, etwas kleiner als Niedersachsen, rund 1,3 Millionen Einwohner[9]. Von 2005 bis 2014 war Andrus Ansip von der liberalen Estnischen Reformpartei Premierminister. Seit Ende 2014 ist er Vizepräsident der Europäischen Kommission und für den digitalen Binnenmarkt zuständig. Er wurde abgelöst von Taavi Rõivas, dieser war zum Zeitpunkt seines in Amt tretens gerade einmal 34 Jahre alt[13]. Auch

sein Minister für Bildung und Forschung Jevgeni Ossinovski[14], geboren im Jahr 1986, gehört zu der neuen jungen Generation Politiker. Bei der Wahl Anfang März 2015 konnte er trotz leichter Stimmverluste die größte Fraktion bilden[15], die Regierungsbildung ist zur Zeit noch nicht abgeschlossen.

3 Digitalisierungsbestrebungen

Durch die bereits erwähnte Möglichkeit finnisches Fernsehen und internationales Radio zu empfangen, war in Estland durchaus bekannt, was im Rest der Welt passierte, kulturell eine europäische Prägung vorhanden. Nach ende des Eisernen Vorhangs bauten sie schnell Wirtschaftsverbindungen zu Finnland und Schweden auf und insbesondere finnische Touristen brachten Geld und Kulturgüter ins Land.
Technologisch war das Land durch die Planwirtschaft jedoch an Bedarf und vorhandenen Ressourcen vorbei aufgebaut worden[16]. In einem Interview mit USA Today[17] beschreibt der heutige Präsident Toomas Hendrik Ilves die Situation: "1993 hatte Estland ein Telefonsystem von 1938." Aus Helsinki kam damals das Angebot deren altes, analoges System zu übernehmen, Ilves, zu der Zeit Botschafter Estlands in den USA[2], sorgte jedoch dafür, dass stattdessen auf modernste Technologie gesetzt wird: "Wir wollen nicht in Technologien von 1979 hängen bleiben" war seine Antwort. Seit 2013 sind 95% der Fläche Estlands mit 4G LTE-Netzen abgedeckt[18], schon 2016 sollen die ersten Pilotversuche mit dem Nachfolger starten[19]. Die Entwicklung entzieht mittlerweile den Kabelbetreibern die Kunden, einige nutzen wegen der konkurrenzfähigen Preise ausschließlich mobiles Internet[20]
Ilves, der selbst als Flüchtling in den Vereinigten Staaten von Amerika aufwuchs und dort bereits im Alter von 13 Jahren Programmieren lernte, ist wohl die federführende Hand in der Modernisierung des Landes geworden. Schon vor der Unabhängigkeit war er politisch für Estland aktiv, arbeitete bei dem Radiosender Radio Free Europe, zuletzt als Redaktionsleiter, und war damit wichtiger Teil der empfangbaren westlichen Medienlandschaft[21]. Früh erkannte er den Vorteil größtmöglicher Automatisierung für sein kleines Land. In einer Geschichte, die er der BBC erzählte, berichtet er von einem Industriebetrieb, der durch Computer statt mehrere tausend nur noch 100

Beschäftigte benötigt. Bei nur 1,4 Millionen Einwohnern ermöglicht das den Anderen in vorher möglicherweise nicht existierenden Gewerben zu arbeiten:

> We need to really computerise, in every possible way, to massively increase our functional size,

so seine Schlussfolgerung[2]. Um seine Ideen in die Tat umzusetzen und das Volk in die Lage zu versetzen diesen Weg zu beschreiten stieß Ilves 1996 das Tiigrihüpe Programm an. Ziel war das Land großflächig mit moderner Computer- und Netzwerkinfrastruktur auszustatten, insbesondere die Schulen und Universitäten, sowie für die notwendige Ausbildung zu sorgen[22]. Heute gibt es ein weiteres Programm[2], welches Programmieren schon Grundschülern näher bringen soll[2]. Die Namen Progetiiger und Tiigrihüpe spielen bereits auf den Spitznamen *Baltic Tiger* an, den die baltischen Länder im Zuge ihrer raschen wirtschaftlichen Entwicklung, in Anlehnung an die Tigerstaaten[3], erhalten haben.
Nicht nur im Spitznamen sondern auch in den Zahlen zeigen sich die Erfolge der radikalen Modernisierung: 99% der Steuererklärungen werden online eingereicht, Bankgeschäfte werden beinahe ausschließlich über das Internet abgewickelt. Die steigende Wahlbeteiligung, insbesondere der Anteil, der online Wählt, zeigen, dass die Bevölkerung bereit ist diesen Weg zu gehen. Bei den unter 45 Jährigen benutzt fast jeder regelmäßig Computer und das Internet, und selbst bei über 65 Jährigen ist beinahe jeder Zweite online aktiv[23].
In der Welt hat sich Estland mit seinen Erfolgen einen Namen gemacht und gilt vielen als digitaler Vorreiter[17]. Außerhalb der infrastrukturellen Erneuerung, oder vielmehr darauf aufbauend florieren in Estland viele junge Unternehmen in der Technologiebranche. Von weltweiter Berühmtheit ist hier vor allem Skype, der mittlerweile von Microsoft für 8,5 Milliarden US-Dollar gekaufte Videotelefonieanbieter[2]. Im Zuge der europäischen Kommission versucht die EU von dieser Erfahrung zu profitieren und die EU insgesamt auf diesen Pfad zu führen, dazu hat Kommissionspräsident Jean-Claude Juncker Ende 2014 den vorherigen Premierminister Estlands, Andrus Ansip, zum

[2]Progetiiger: `http://progetiiger.ee/`
[3]`http://de.wikipedia.org/wiki/Tigerstaaten`

Kommissar für den digitalen Binnenmarkt ernannt[24].

4 Dienste

4.1 Digitale Signaturen

Für die verschiedenen nun elektronisch angebotenen Dienste benötigt es eine technologische Grundlage. Bei Entwurf des Systems wurde prinzipiell von der klassischen analogen Handlungsweise ausgegangen. Dort ist eine handschriftliche Unterschrift das Mittel der Wahl Verträge anzuerkennen und die Absicht ihnen Folge zu leisten zu bekunden. Die Grundkonzepte der Unterschrift sollen nun definiert werden um die Übertragung in ein elektronisches Analog und die dafür notwendigen Bedingungen verfolgen zu können.

Unterschrift Rechtlich gilt bisher vor allem die Unterschrift als gültige Identifikation sowie Garantie der Echtheit des unterschriebenen Dokumentes. Hier ergeben sich sofort drei zu klärende Begrifflichkeiten. Die *Unterschrift* ist im einfachsten Fall (in Deutschland) der Nachname der unterschreibenden Person. Es gibt hier jedoch einige Bedingungen sowie Abschwächungen. Der Schriftzug muss zum einen individuell sein, in sauberen Druckbuchstaben geschrieben erfüllt er diese Bedingung dementsprechend nicht. Zweitens muss er den Namen wiedergeben, zwingend dabei den Nachnamen. Drittens muss der Name ausgeschrieben sein, es reicht also nicht den Anfangsbuchstaben unter ein Dokument zu schreiben. Eine volle Lesbarkeit ist jedoch nicht notwendig[25, 26].
Aus der Individualität des Schriftzuges leitet sich die *Identifikation* her. Jemand, der die Unterschrift einer Person kennt, kann von der Unterschrift wieder zurück auf den Unterschreibenden schließen. Die Identität ordnet also dem Schriftzug eine eindeutige Person zu[26]. Außerhalb von Dokumenten, etwa bei anwesenden Personen, kann die Identitätsfeststellung durch Vergleich mit dem amtlich beglaubigten Lichtbildausweis gesichert werden[27].
Die Unterschrift soll auch die *Echtheit* des Dokumentes garantieren[26]. Die Person kennt also den Inhalt und hat dies bestätigt, und hat, viel wichtiger

noch, das vorliegende Dokument eigenhändig mit einem Dokumentenechten Stift markiert. Es kann theoretisch also kein Papier ihre Unterschrift haben, das diese nicht kennt.

Asymmetrische Verschlüsselung Um vergleichbare Aufgaben digital erfüllen zu können müssen diese Eigenschaften dementsprechend in digitale Gegenüber abgebildet werden. Eine Möglichkeit dies zu tun ist die so genannte Public-Key-Infrastruktur. Grundlage dessen sind zwei Komponenten. Zum einen asymmetrische Verschlüsselung und darauf aufbauend ein Zertifizierungsprozess für die öffentlichen Schlüssel. Für asymmetrische Verschlüsselung besitzt jeder Teilnehmer ein einzigartiges Paar Schlüssel. Einen nennt man *privaten* und einen *öffentlichen* Schlüssel. Grundsätzlich dient dieses Verfahren zur sicheren Nachrichtenübertragung durch einen unsicheren Übertragungsweg. Der Private Schlüssel muss dabei zwingend geheim gehalten werden, der Öffentliche wird dementsprechend anderen Nutzern mitgeteilt.
Wird eine Nachricht mit dem privaten Schlüssel verschlüsselt, kann sie mit dem öffentlichen entschlüsselt werden. Wird andersherum eine Nachricht per öffentlichem Schlüssel codiert, macht der private Schlüssel sie wieder lesbar. Möchte eine Person Alice einer Person Bob eine Nachricht übermitteln, verschlüsselt sie diese zweifach: Erstens mit ihrem privaten Schlüssel, der Empfänger kann diesen Teil mit dem bekannten öffentlichen Schlüssel von Alice lesen. Da dieser Schlüssel wie bereits beschrieben allgemein bekannt ist kann auch jeder Dritte diese Nachricht lesen. Im zweiten Schritt wird die Nachricht mit Bobs öffentlichen Schlüssel verschlüsselt, dieses Schloss kann nur Bob mit seinem privaten Schlüssel öffnen.

Public-Key-Infrastruktur Die öffentlichen Schlüssel, im englischen *public-key*, daher auch der Name Public-Key-Infrastruktur, werden nun von einer vertrauenswürdigen Stelle zertifiziert. Diese Autorität bestätigt die Authentizität, also die Echtheit, des Schlüssels. Gewissermaßen gleicht dies dem per Stempel amtlich beglaubigten Photos auf einem Personalausweis. Dieses Zertifikat enthält nun den öffentlichen Schlüssel von Alice sowie ihren Namen,

es wird also bestätigt, dass dieser Schlüssel Alice gehört.
Theoretisch kann ein unbefugter Dritter einen amtlichen Stempel besitzen um die Echtheit eines Photos zu bestätigen, gleichermaßen ist bei dem Zertifikat bisher nicht sicher, dass es kein Unbefugter ausgestellt hat. Um dies zu tun wird es ebenfalls mit dem privaten Schlüssel der Ausstellungsstelle signiert. Wir stehen nun wieder vor dem selben Problem, mit dem öffentlichen Schlüssel der Ausstellungsstelle kann das Zertifikat gelesen werden, es ist allerdings nicht sicher, dass dieser Schlüssel von vertrauenswürdiger Stelle kommt. Er muss ebenso von einer höheren Stelle zertifiziert werden. Darum spricht man bei dieser Technik von einem hierarchischen System. Diese verketteten Zertifikate nennt man auch Validierungspfad oder Zertifizierungspfad. Offensichtlich kann dieser Pfad nicht beliebig fortgeführt werden, es muss eine oberste Stelle geben, der ohne weitere Zertifizierung vertraut werden kann.

Abbildung Wie eine Unterschrift digital funktionieren kann wurde oben bereits angedeutet. Als Alice ein Dokument mit ihrem privaten Schlüssel codierte, konnte jeder Beliebige ausschließlich mit ihrem öffentlichen Schlüssel die Nachricht lesen, Alice muss also das Objekt verschlüsselt haben. Dabei muss nicht zwangsweise das gesamte Dokument verschlüsselt werden. Es wird dann eine Signatur für das Dokument erstellt und mit dem privaten Schlüssel signiert. Der Empfänger kann dann überprüfen ob die Signatur, die er erstellt das gleiche Ergebnis ergibt[28, 29]. Dies garantiert, dass Alice den Inhalt kennt und niemand Drittes diesen im Nachhinein verändert hat. Die *Individualität* des Schlüsselpaares wird über hinreichend komplexe Zufallsverfahren sichergestellt. Über die Zertifikatshierarchie wird die *Identifikation* sichergestellt, der Schlüssel selbst enthält keine Information über den Inhaber.

Estlands eID In Estland stellt der Staat diese hierarchische Infrastruktur zur Verfügung, jeder Bürger erhält eine Chipkarte, die sowohl als klassischer Personalausweis persönliche Angaben sowie ein Photo aufgedruckt hat, als auch im digitalen Teil zusätzlich zwei Schlüsselpaare sowie die zugehörigen Zertifikate enthält. Das Zertifikat ist mit Namen und, wegen möglichen

Namenskollisionen, einer nationalen ID-Nummer an eine Person gebunden. Zusätzlich enthält es eine offizielle e-Mailadresse. Außer den genannten Daten sowie den Aufgedruckten enthält die Karte keine weiteren Informationen. Weitergehende Daten werden in anderen Datenbanken gespeichert[30].
In den oben beschriebenen Szenarien war immer lediglich ein Schlüsselpaar in Verwendung, die Karte enthält jedoch zwei von diesen. Das Erste dient lediglich zur Identifizierung, vergleichbar mit dem Vorzeigen des Personalausweises, wogegen das Zweite zur rechtsgültigen Unterschrift, gleichbedeutend einer handschriftlichen Unterschrift, genutzt wird[31] . Sie sind durch zwei verschiedene PINs gesichert. Zur Identifizierung ist ein vier- bis zwölfstelliger PIN nötig, zur Signatur fünf bis zwölf Stellen[32], der Nutzer kann also erkennen welche er gerade benutzt. Seit 2007 sind die Zertifikate und die Karten selbst jeweils 5 Jahre gültig, nach Ablauf der Zeit müssen sie ersetzt werden[33]. Dementsprechend sind sie nicht geeignet Daten langfristig verschlüsselt zu speichern. Um die elektronischen Dienste zu nutzen ist ein Kartenlesegerät notwendig, diese sind günstig erhältlich, die notwendige Software wird für alle gängigen Betriebssysteme (Windows, Mac OS X, Linux) zur Verfügung gestellt.

4.2 Anwendungen

Der Ausweiskarte auf Anwenderseite steht eine große dezentrale Infrastruktur auf staatlicher Seite gegenüber, welche es sowohl dem Staat und anderen Verwaltungsorganen, als auch privatwirtschaftlichen Anbietern ermöglicht verschiedenste Dienste aufzubauen. Die X-Road genannte Umgebung standardisiert technische Funktionsweise der Serviceanbieter und die organisatorische Grundstruktur. Die Architektur X-Roads stellt ein einheitliches Kommunikationsprotokoll sowie die nötigen Sicherheitsvorrichtungen zur Verfügung. Die eigentlichen Anwendungsserver sind hinter einheitlichen Sicherheitsservern versteckt und somit für die Entwickler systemunabhängig. Sie stellen die Kommunikation zwischen verschiedenen Dienstanbietern oder Nutzern unter Verschlüsselung sicher. Ein zentraler Server erhält dabei statistische Informationen über jeden Transfer sowie einen Hash, der ermöglicht im Nachhinein die Übertragungsketten nachzuvollziehen, so kann kein Serverprotokoll unent-

deckt manipuliert werden. Außerdem stellt der zentrale Server die Zertifikate der am System teilnehmenden Server zur Verfügung[34, 35] Über X-Road sind mittlerweile über 2000 Dienste verfügbar, die Daten sind auf über 170 Datenbanken verteilt. Diese Infrastruktur bildet damit die Basis für beinahe jede datenbezogene Handlung in Estland[36].

Neben typischen behördlichen Verwaltungsaufgaben wie zum Beispiel Fahrzeuganmeldung oder Wohnsitzänderung haben sich viele weitere Anwendungsgebiete gefunden. Für den öffentlichen Nahverkehr kaufen die Esten ihre Tickets online und weisen sich an den Lesegeräten der Fahrzeuge lediglich aus[37]. Die Identifizierungdienste erlauben also das Aufbauen beliebiger personalisierter Anwendungen. So funktioniert die eID nicht nur als Personalausweis, sondern auch als Führerschein, Krankenversicherungskarte und beliebiges mehr. Den tiefsten Eingriff in persönliche Daten gibt es wohl im Gesundheitsbereich. Alle Patientenakten liegen Zentral gespeichert, so haben Ärzte Zugriff auf die Einträge von anderen Ärzten, neben Text auch andere Datensätze wie etwa Röntgenaufnahmen. Der Vorteil liegt auf der Hand, Patienten müssen nicht selber dafür Sorge tragen beim Arztwechsel oder einer Überweisung die notwendigen Daten zu transportieren. Überhaupt ist sichergestellt, dass verschiedene Krankenhäuser auf dieselben aktuellen Daten zugreifen können. Für Patienten hat dies noch weitere Vorteile: Rezepte für Medikamente werden nicht mehr auf Papier ausgestellt, sondern in einer Datenbank gespeichert und in der Apotheke mit Hilfe der Karte abgerufen. Besonders in diesem sensiblen Bereich betonen die Befürworter jedoch den Vorteil eines Computers. Ein solcher sei weder bestechlich, noch können unbemerkt Dritte eine Papierakte zu Gesicht bekommen. Bei jenen ist nie Nachvollziehbar wer diese wann gelesen hat, oder gar wie eine verschwunden ist. Zu den digitalen Akten dagegen wird jeder Zugriff nachvollziehbar protokolliert und sogar den Betroffenen gemeldet[38].
Parallel zu den Kartendiensten gibt es mit den *M-Services* die Möglichkeit sich über ein Mobiltelefon zu identifizieren oder zu bezahlen, etwa Parktickets, Theaterkarten oder Supermarkteinkäufe. Auch die Ergebnisse der Schulabschlussprüfungen werden, wenn gewünscht, per SMS versandt. Hierzu sind spezielle SIM Karten notwendig, die der Mobilfunkprovider ausstellt. Auf

diesen sind genau wie auf der Karte zwei Schlüsselpaare installiert. Dazugehörig ist eine Applikation auf dem Gerät, die die benötigte PIN abfragt und die Verbindung mit dem Identifizierungsserver aufbaut[39]. Diese Identifizierungsfunktion wird immer beliebter, da sie kein Kartenlesegerät erfordert und somit noch komfortabler und beinahe allgegenwärtig verwendbar ist[37].

4.3 Wahlen

Mit der Einführung der elektronischen Stimmabgabe bei den Kommunalwahlen 2005 kann Estland wie kein zweites Land auf 10 Jahre Erfahrung zurückblicken. Wurde diese Möglichkeit zu Beginn noch sehr spärlich genutzt, gerade einmal 1,9% der abgegebenen Stimmen waren digital, sind es bei den Parlamentswahlen im März 2015 bereits über 30%[40]. Das sogenannte I-voting funktioniert dabei vergleichbar zu der klassischen analogen Briefwahl[41]:

1. Der Wähler weist sich aus
2. Er erhält den Stimmzettel sowie zwei Umschläge
3. Den ausgefüllten Stimmzettel verschließt er im anonymen Umschlag
4. Dieser wird im personalisierten Umschlag verschlossen und dem Wahlbezirk zugesandt
5. Erneut wird geprüft, ob der Wähler berechtigt ist, wenn dem so ist, der innere anonyme Umschlag in die Wahlurne geworfen

Auf diese Weise ist sichergestellt, dass nur berechtigte Personen wählen können, durch die erneute Prüfung sichergestellt, dass nur eine Stimme abgegeben wurde, und zuletzt, dass das Wahlgeheimnis gewahrt ist.
Ebenso wie die Briefwahl wird die elektronische vor dem eigentlichen Wahltag durchgeführt. Dafür ist ein Zeitfenster von sieben Tagen vorgesehen. Für diesen Mechanismus benötigt der Wähler einen Computer mit Internetanschluss, sowie seinen Ausweis und einen Kartenleser. Als Alternative für die Letzteren beiden Komponenten ist seit 2011 die *mobile-ID* möglich. Der Ablauf ist analog:

1. Der Wähler besucht die vorgesehene Internetseite[4]
2. Er lädt die benötigte Applikation herunter und führt diese aus
3. Identifikation über den PIN1 Code über das gewünschte Eingabegerät
4. Stimmabgabe
5. Signatur seiner Wahl mit der PIN2 und damit Übertragung der verschlüsselten Stimme
6. Am Wahltag wird der äußere, signierte Ümschlag"mit dem Wählerverzeichnis abgeglichen und die Stimme heraus getrennt
7. diese ist nun anonym und zur Auszählung bereit

Dabei kann sogar nach Abgabe die Stimme im Nachhinein nochmals geändert werden, entweder beliebig oft digital, oder durch reguläre Wahl am Wahltag. Dies soll sicherstellen, dass die Stimmabgabe freiwillig und unbeeinflusst stattfinden kann. Etwa 2,5% der elektronischen Stimmen wurden bei der letzten Wahl innerhalb des Zeitfensters geändert.
So wie der Anteil der elektronischen Stimmen kontinuierlich ansteigt, steigt auch die Wahlbeteiligung in Estland insgesamt über die vergangenen Jahre an. Bei der Parlamentswahl 2007 lag sie bei 61,9%, 2015 bei 64,2%[40]. Die Möglichkeit online zu Wählen scheint dabei ein wichtiger Faktor zu sein, in einer Umfrage gaben 10% der e-Wähler an, dass sie nicht auf Papier wählen würden[42, S. 19]. Gerade für ältere Menschen, für die der Weg zur Wahlurne eine Anstrengung ist, kann bequemes Wählen von Zuhause eine gute Alternative sein. So zeigt eine Statistik des Wahlkomitees, dass 25% der e-Wähler älter als 55 Jahre sind, die Verbreitung der digitalen Wahl ist durch alle Altersklassen gleichmäßig verteilt[40]. Das Wahlkomitee bemüht sich um das Vertrauen der Bürger in die Technik, der Quellcode für die Wahlen ist zwar geschlossen von der Technologiefirma Cybernetica[5] in Tallinn entwickelt, seit 2013 jedoch öffentlich zur Einsicht freigegeben[6][41].

[4] `https://www.valimised.ee`
[5] `http://cyber.ee/en/`
[6] `https://github.com/vvk-ehk`

4.4 Digitale Staatsbürgerschaft

Auch auf Internationaler Ebene will Estland seine moderne Infrastruktur anbieten. So läuft seit Ende 2014 das Pilotprojekt zur virtuellen Staatsbürgerschaft[43]. Für 50€kann jeder nicht per Haftbefehl gesuchte oder als Terrorist eingestufte Mensch die so genannte *e-Residency* beantragen. Jedes Mitglied dieser digitalen Gemeinde erhält ebenfalls eine eID-Karte und Zugriff auf beinahe alle Services wie auch tatsächliche Einwohner Estlands insbesondere also Identifizierung sowie Signierung[44]. Lediglich das Wahlrecht und die Aufenthaltsgenehmigung in der Europäischen Union bleiben ihnen vorenthalten. In der Testphase ist noch ein Besuch in Estland zur Identitätsprüfung bei der Polizei notwendig, in Zukunft soll dies auch in estnischen Auslandsvertretungen möglich sein.
Das Projekt will ambitioniert bis 2025 etwa 10 Millionen Menschen von dieser Idee überzeugen. Zur Erinnerung: Estland selber hat lediglich etwas mehr als 1,3 Millionen Einwohner. Das Ziel ist wenig Überraschend wirtschaftlich zu Verstehen, der baltische Staat ist für junge Firmen durchaus attraktiv, Gewinn, der wieder investiert wird, muss nicht versteuert werden[45]. Eine ideale Bedingung für schnelles Wachstum kleiner Unternehmen.
Estland hat es zudem leicht gemacht neue Unternehmen zu Gründen, alles ist online innerhalb von einer Viertelstunde erledigt. Dabei werden die gleichen Daten dafür benötigt wie in anderen Ländern auch. Jedoch muss sich der Gründer nicht mehr in Person von Amt zu Amt bewegen, warten, Papiere ausfüllen und noch auf Bearbeitung warten. Die Daten werden automatisch von den verschiedenen Datenbanken zusammengetragen, schließlich ist alles notwendige den Behörden längst bekannt[46].

5 Rechtliche Grundlagen

Nachdem die technische Infrastruktur sowie Anwendungsfälle erläutert wurden, sollen in diesem Abschnitt die rechtlichen Rahmenbedingungen zum Schutz von persönlichen Daten dargelegt werden. Werden sensible Daten wie etwa Krankenakten zentral gespeichert müssen diese gegen unbefugten Zugriff geschützt werden. Auf Basis dieser Gesetze sind Einschränkungen in der

Arbeit mit persönlichen Daten vorgesehen und der Umgang reguliert. Im Einzelfall können die Rechte gerichtlich verhandelt werden, zur Unterstützung der Betroffenen, ebenso Überwachung von Daten sammelnden Einrichtungen ist das Data Protection Inspectorate eingerichtet. Das wesentliche Gesetz auf welches dieses sich stützt ist der Personal Data Protection Act. Diese beiden sollen im Folgenden eingeführt und deren Aufgaben vorgestellt werden.

5.1 Personal Data Protection Act

Wichtigste rechtliche Basis für Datenschutz ist der Personal Data Protection Act[38] . Anfang des Jahres 2008 in Kraft getreten soll dieser die Rechte natürlicher Personen[7], insbesondere deren Privatheit im Zusammenhang mit digitaler Datenverarbeitung schützen. Speziell werden dort Rahmenbedingungen unter denen personenbezogene Daten verarbeitet werden dürfen beschrieben, wie die staatliche Kontrolle darüber funktionieren soll, sowie Verantwortung und Haftbarkeit der Datenverarbeiter.
Grundsätzlich unterscheidet das Gesetz zwei Stufen persönlicher Daten, die erste benennt persönliche Daten als einer identifizierten oder identifizierbaren natürlichen Person zuordenbare Daten. Im zweiten Schritt wird eine Teilmenge davon als *sensibel* definiert, für diese werden später strengere Regeln bei der Verarbeitung festgelegt. Als sensibel gelten solche, die politische, religiöse oder philosophische Ansichten offenbaren, Daten bezüglich ethnischer Herkunft, Gesundheitszustand, Sexualleben oder gewerkschaftliche Aktivitäten. Weiterhin sind genetische sowie biometrische Daten besonders geschützt sowie Informationen zu laufenden noch nicht veröffentlichten Rechtsverfahren.
Was genau unter Verarbeitung von persönlichen Daten verstanden wird, ist ebenfalls definiert:

> **§ 5. Processing of personal data**
> Processing of personal data is any act performed with personal data, including the collection, recording, organisation, storage, alteration, disclosure, granting access to personal data, consultation and retrieval, use of personal data, communication, cross-usage,

[7]Eine natürliche Person ist ein real lebender Mensch. Dem gegenüber sind *juristische* Personen, also Organisationen, hier nicht eingeschlossen.

> combination, closure, erasure or destruction of personal data or several of the aforementioned operations, regardless of the manner in which the operations are carried out or the means used.

Das Gesetz sieht im folgenden Paragraphen für all diese Daten das Prinzip *so viel wie nötig, so wenig wie möglich* vor. Daten sollen[8] nur für ein festgelegtes Ziel gesammelt werden und nur in dem Ausmaß, wie es für Erfüllung dessen notwendig ist. Darüber hinaus dürfen sie nur mit Einverständnis der Betroffenen oder Erlaubnis einer amtlichen Autorität verarbeitet werden. Daneben ist das Partizipationsprinzip in Absatz sieben für Individuen von besonderer Reichweite: Betroffene sollen Benachrichtigt werden über Datensammlung, sie sollen Zugriff auf die Daten bekommen und sie korrigieren können. Diese Prinzipien werden im Verlaufe des Textes weiter spezifiziert, so wird den Betroffenen die Wahl der Art des Zugriffes auf die Daten gewährt, ein Verarbeiter kann und darf dies nicht durch hohe Kosten für den Anfragenden verhindern. Unter diesen Daten ist auch enthalten welche Dritten diese erhalten oder anderweitig verarbeitet haben. Ebenso sind Reaktionszeiten des Verarbeiters festgelegt. Es wird viel Wert darauf gelegt, dass Personen den Verlauf der Verarbeitung ihrer Daten verfolgen können. Für sensible Daten wird festgelegt, dass die Person explizit auf die Sensibilität der Daten hingewiesen werden muss und diese zustimmen muss, bevor Verarbeitung stattfinden darf. Ein Paragraph, der aktuell stark an Bedeutung gewinnt räumt Betroffenen das Recht ein eine Veröffentlichung von persönlichen Daten anzufechten. Diese dürfen Veröffentlichungen verbieten und verlangen, dass bereits Veröffentlichtes wieder entfernt wird.
Die Einhaltung dieser Rechte wird durch das Data Protection Inspectorate überwacht und wenn nötig auf juristischem Wege durchgesetzt. Wenn sensible Daten verarbeitet werden soll, muss der Verarbeitende dies dem Inspectorate mitteilen, ein Unternehmen kann zur eigenständigen Überwachung eine von der direkten Verarbeitung unabhängigen Person als Beobachter beim Inpectorate registrieren. Dieser trägt dann die Verantwortung vor Ort und muss Verarbeitungen protokollieren, Verstöße verhindern und gegebenenfalls

[8] Im englischen Text wird das Wort *shall* genutzt, welches jedoch selbst in Gesetzeskontext nicht eindeutig interpretiert wird. Die Unterscheidung zwischen *sollen* und *müssen* ist nicht völlig klar, siehe z.B.: `http://definitions.uslegal.com/s/shall/`

melden. Das Inspectorate kann auch die Verarbeitung von sensiblen Daten untersagen, sollte es keine Notwendigkeit für sie geben oder die Sicherheit der Daten nicht gewährleistet werden können.

5.2 Data Protection Inspectorate

Wie bereits erwähnt, ist es die Aufgabe des Data Protection Inspectorates(DPI), für die Einhaltung beziehungsweise Umsetzung des Personal Data Protection Acts zu sorgen. Das DPI untersteht dabei der Regierung Estlands, der Generaldirektor wird im 5-Jahres-Zyklus vom Justizminister vorgeschlagen. Viljar Peep hat seit 2008 diese Funktion inne, zuletzt wurde er 2013 wiederernannt. Neben dem Personal Data Protection Act(PDPA) ist es weiterhin durch den Public Information Act(PIA)[47], den Electronic Communications Act(ECA) sowie durch weitere internationale Gesetzgebung ermächtigt[48] . Das DPI wurde 1999 gegründet, drei Jahre nach Einführung des ersten Gesetzes zum Schutz persönlicher Daten. Während der PDPA wie oben beschrieben einzelne Individuen und deren persönliche Daten schützt, ermöglicht der PIA jedem Bürger Zugriff auf Informationen, die für öffentliche Nutzung bestimmt sind. In der Zweckbeschreibung dieses Gesetzes wird dies mit dem Verweis auf eine *open society* benannt. Es soll dementsprechend der Öffentlichkeit ermöglichen die Arbeit der Regierungsorgane zu kontrollieren. Der ECA reguliert, seinem Namen entsprechend, die elektronische Kommunikation und soll insbesondere freien, technologieunabhängigen Wettbewerb sicherstellen.
In seinem 5-Jahresbericht[49], in welchem Peep die Arbeit der letzten fünf Jahre zusammenfasst und Ziele und Aufgaben für die Zukunft formuliert, sieht der Generalinspektor zwar die Hauptaufgabe, wie es durch die erläuterte Gesetzgebung vorgesehen ist, im Schutz von einzelnen Personen gegen die Behörden und Wirtschaftsunternehmen, er weist aber darauf hin, dass sich die tatsächliche Arbeit in eine andere Richtung verschiebt und deutlich vermehrt. Durch das Teilen in soziale Medien gelangen mittlerweile derart viele persönliche Daten durch dritte Personen öffentlich ins Internet, dass der Schutz von Individuen voreinander eine der wichtigsten Aufgaben geworden ist. Für die Zukunft erwartet er weiterhin deutlich steigende Datenmengen und auch neue Quellen, etwa durch Videokameras und Drohnen in der Öffentlichkeit, insbe-

sondere mit den sich weiterentwickelnden Gesichtserkennungsalgorithmen. Es entstehen also nicht einfach mehr Daten sondern insbesondere Daten, die wie im PDPA beschrieben, identifizierbaren Personen zugeordnet werden können. Im Gegensatz zu der aktiven Verteidigung der eigenen Persönlichkeitsrechte steckt die digitale Gesellschaft, wie sie der Public Information Act vorsieht, noch in den Kindesschuhen, wie Peep kritisiert:

> Reusing public information as open data has not really gained a lot of ground in Estonia yet. The requirement to disclose information in a machine-readable form and as a full downloadable database has firstly not been sufficiently implemented and secondly has not found sufficient use in the private sector.

[49] Seine Aufgabe für die aktuelle Amtszeit sieht er in internationaler Zusammenarbeit, mit dem Ziel Daten zu schützen, und gleichzeitig Überregulierung zu verhindern, um eine open society voranzutreiben.

6 Digitalisierung - Risiko oder Chance?

6.1 Aussenpolitische Risiken

Dem bisher kennengelernten praktischen Nutzen tiefgreifender digitaler Vernetzung steht aber auch ein Angriffsrisiko gegenüber. In der Vergangenheit haben Angriffe wie der Computerwurm *Stuxnet* gezeigt, dass gezielte Angriffe auf kritische Infrastruktur eines Landes aus der Ferne möglich sind. Estland selbst ist ebenfalls Ziel ausländischer Angriffe geworden: 2007 wurde ein russisches Kriegerdenkmal der Besatzungszeit aus dem Stadtzentrum Tallinns zu einem Soldatenfriedhof versetzt. Die russische Minderheit protestierte dagegen. Es kam zu Ausschreitungen mit mehreren Verletzten und einem Toten[50]. Im Zuge dieser Auseinandersetzung wurden auch die digitalen Angebote einiger öffentlicher Einrichtungen, darunter Banken, der Regierung und der Polizei lahmgelegt. Zeitweise war auch der Notruf nicht zu erreichen. Glücklicherweise führte der Angriff in diesem Fall nicht zu weiteren Personenschäden, jedoch musste zur Verteidigung gegen die Angriffe der von außen eingehende Internetverkehr blockiert werden[51]. Unternehmen wie Banken sind durch

ein derartiges Szenario akut bedroht. Es ist bis heute nicht vollständig geklärt, wer für die Angriffe verantwortlich war, nur für einen Teil konnte ein russischer Este verurteilt werden.[52].
Die elektronischen Wahlen sind ein weiterer möglicher Angriffspunkt. Eine Manipulation wurde bisher jedoch nicht nachgewiesen. Der Sicherheitsforscher Alex Halderman kritisiert dabei, dass keine öffentlichen Testläufe vor den Wahlen stattfanden, die gezielt hätten angegriffen werden können. Dennoch konnte sein Team einige Schwachstellen im Verfahren und der Software im Labor aufdecken[53]. Es ist also nicht auszuschließen, dass Manipulationen stattfinden können. Sie raten dazu auf elektronische Wahlen zu verzichten[54].
Angriffe auf Wahlen in einem modernen EU-Staat klingen vielleicht nach Phantasie, jedoch kommen mit den Enthüllungen Edward Snowdens viele Details ans Licht, mit welchen Mitteln hochgerüstete Geheimdienste arbeiten. Der Konflikt mit Russland ist für die Esten, insbesondere nach den jüngsten Ereignissen in der Ukraine, nach wie vor nicht beendet[55], Russland stationiert erneut Raketen in EU-Nähe, die NATO rüstet das Baltikum auf[56] und beidseitig werden Militärmanöver geprobt[57]. Die Annexion der Krim zeigt, dass Russland durchaus zu Erweiterungen seiner Grenzen bereit ist. So unklar wie die Parteien in dem Konflikt sind, erscheint auch eine versteckte Operation in Estland denkbar, zumal es dort ebenfalls eine russische Minderheit gibt. Ebenso spiegelt die Bevölkerung diesen Konflikt in ihren Wahlergebnissen 2015 wieder[55].

6.2 Der Grat zwischen Überwachungsstaat und Freiheit

Auch auf privater Ebene birgt die Computerisierung einige Risiken. Wie Generalinspektor Peep anmerkte, ist die größte Herausforderung der Datenschützer derzeit Personen voreinander zu schützen. Insbesondere Jugendliche laden unbedarft Videos voneinander ins Internet, teilweise ohne böse Absicht, teilweise auch um Anderen zu schaden. In sozialen Netzen sind Mobbingaktionen keine Seltenheit. Etwas, das einmal im Internet veröffentlicht wurde, ist nicht ohne weiteres dem Zugriff wieder zu entziehen.
Er betont, dass allerorten immer mehr Photo- und Videokameras im Einsatz sind. Durch Gesichtserkennungsalgorithmen, die nicht nur Plattformen wie

Facebook[58] einsetzen, sondern die gleichermaßen auch zur Strafverfolgung verwendet werden können, bildet sich mehr und mehr eine Welt, in der es Menschen unmöglich ist Aufnahmen aus dem Weg zu gehen. Weltweit fordern die Polizei- und Geheimdienstbehörden mehr Befugnisse Daten aufzunehmen und auszuwerten[59, 60, 61]. Sogar Verschlüsselungsmechanismen ganz zu verbieten wird vorgeschlagen[62] Da auf modernen Ausweisdokumenten biometrische Photos Standard sind und in Estland der Staat sogar die Kryptographieschlüssel selber ausstellt, sind Warnungen vor Totalüberwachung, wie etwa im Roman 1984, nicht unernst zu nehmen. Auch wenn Ilves die Sicherheit der Schlüssel eher mit der von *Lavabit*, dem E-Mail-Service von Edward Snowden, vergleicht, Restzweifel werden von den Netzaktivisten Estlands nur über Vertrauen aus dem Weg geräumt[63]. Die estnischen Verantwortlichen beziehen jene aber in die Entwicklung mit ein, X-Road besteht nach eigenen Angaben aus freien Komponenten, die Bemühungen keine Fehler zu machen und das Vertrauen der Bevölkerung zu gewinnen sind nicht abzustreiten.
Was als Kritikpunkt bleibt ist, wie Peep kritisiert, dass zur Veröffentlichung bestimmte Dokumente der Verwaltungseinrichtungen nicht ausreichend verarbeitbar herausgegeben werden. Mittlerweile finden sich, genau dieses Problem betreffend, rund um die Welt Freiwillige, die genau solche Daten verwenden wollen. Ausgehend von der Organisation *Code for America* haben sich viele Lokalgruppen gebildet, die offenen Code programmieren oder Firmen gründen um öffentliche Daten und Dienste für Bürger verständlich und nutzbar darzustellen[64].
Das Internet ist keine zentral gesteuerte Instanz, sondern formt und verformt sein Gestalt angepasst an die Verwendungsarten der Nutzer. Die Frage ob das Internet einen Staat, die Demokratie, verändert ist demnach beinahe falsch gestellt. Schalken [65, S. 161] formuliert die besser passende Frage was für Organisationsformen, welche Potentiale für Demokratie bestehen in einer Gesellschaft, in die die weiträumige Vernetzung eingebettet ist. Diese Gelegenheit müssen alle Regierenden nutzen um eine Gesellschaft für alle Menschen gemeinsam und effizient zu gestalten. Es zeigt sich also, dass es hier zwei Seiten gibt, die aufeinander zugehen müssen. Die Risiken für Einzelpersonen sind groß, in der Summe ein gesamtgesellschaftliches Problem. Gleichzeitig bietet sich eine Chance die Grenzen zwischen Regierung und

Bevölkerung abzubauen. Es bedarf auf beiden Seiten die Sensibilität und nötiges Fachwissen mit den neuen Technologien umzugehen.
Der estnische Ansatz ist bisher sehr pragmatisch, sie wissen um ihre kleine Bevölkerung und nutzen die Möglichkeiten der Informationstechnik um Arbeit, die nicht unbedingt von einem Menschen gemacht werden muss zu automatisieren. Das Beispiel Firmengründung zeigt dies in aller Deutlichkeit. Bisher ist von keinem Datenmissbrauch die Rede, und die estische Netzgemeinde hat eher Angst davor, dass eine EU-weite Lösung schlechter sein könnte, als die Ihrige. Das junge Estland hat beim Aufbau seiner neuen politischen Strukturen zukunftsorientiert gehandelt. Wenn die Gesellschaft, noch voran die Regierung, es schaffen ihre freiheitlich demokratischen Werte auch im Digitalen umzusetzen, wird Estland den Weg als Vorreiter mit einem positiven Bild gehen können. Somit kann der digitale Staat, die digitale Gesellschaft ein Element des Freiheitsgewinns sein.

Literatur

[1] Till Simon Nagel. "Angela Merkel entdeckt „Neuland"". In: *Handelsblatt* (Juni 2013). http://www.handelsblatt.com/politik/deutschland/das-netz-spottet-angela-merkel-entdeckt-neuland/8375342.html. zuletzt geprüft: 30. März 2015.

[2] Tim Mansel. "How Estonia became E-stonia". In: *BBC News* (Mai 2013). http://www.bbc.com/news/business-22317297. zuletzt geprüft: 30. März 2015.

[3] Toomas Karjahärm. "National Awakening". In: *Estonica* (2012). http://www.estonica.org/en/History/1850-1914_National_awakening/National_awakening/. zuletzt geprüft: 29. März 2015.

[4] Toomas Karjahärm. "Russification period". In: *Estonica* (2012). http://www.estonica.org/en/History/1850-1914_National_awakening/Russification_period/. zuletzt geprüft: 31. März 2015.

[5] Toomas Karjahärm. "Emergence of parties and the 1905 revolution". In: *Estonica* (2012). http://www.estonica.org/en/History/1850-1914_National_awakening/Emergence_of_parties_and_the_1905_revolution/. zuletzt geprüft: 31. März 2015.

[6] Wikipedia. *Geschichte Estlands*. http://de.wikipedia.org/wiki/Geschichte_Estlands. zuletzt geprüft: 31. März 2015. 2015.

[7] Wikipedia. *Estnischer Freiheitskrieg*. http://de.wikipedia.org/wiki/Estnischer_Freiheitskrieg. zuletzt geprüft: 31. März 2015. 2014.

[8] Ago Pajur. "Tartu Peace Treaty". In: *Estonica* (2012). http://www.estonica.org/en/Tartu_Peace_Treaty/. zuletzt geprüft: 31. März 2015.

[9] Wikipedia. *Estland*. http://de.wikipedia.org/wiki/Estland. zuletzt geprüft: 31. März 2015. 2015.

[10] Tõnu Tannberg. "Opposition to the regime". In: *Estonica* (2012). http://www.estonica.org/en/Tartu_Peace_Treaty/. zuletzt geprüft: 31. März 2015.

[11] Hiljar Tammela. “The Singing Revolution”. In: *Estonica* (2012). http://www.estonica.org/en/The_Singing_Revolution/. zuletzt geprüft: 31. März 2015.

[12] Einar Värä. “Breakthrough years”. In: *Estonica* (2012). http://www.estonica.org/en/History/1985-1991_Restoration_of_independence/Breakthrough_years/. zuletzt geprüft: 31. März 2015.

[13] Wikipedia. *Taavi Rõivas*. http://de.wikipedia.org/wiki/Taavi_R~oivas. zuletzt geprüft: 31. März 2015. 2015.

[14] Wikipedia. *Jevgeni Ossinovski*. http://de.wikipedia.org/wiki/Jevgeni_Ossinovski. zuletzt geprüft: 29. März 2015. 2015.

[15] Wikipedia. *Parlamentswahl in Estland 2015*. http://de.wikipedia.org/wiki/Parlamentswahl_in_Estland_2015. zuletzt geprüft: 31. März 2015. 2015.

[16] Tõnu Tannberg. “The command economy and its consequences”. In: *Estonica* (2012). http://www.estonica.org/en/History/1945-1985_The_Soviet_Period/The_command_economy_and_its_consequences. zuletzt geprüft: 31. März 2015.

[17] Kim Hjelmgaard. “From Jersey to Estonia, a president pushes technology”. In: *USA Today* (Dezember 2013). http://www.usatoday.com/story/news/world/2013/12/23/estonia-president-toomas-hendrik-ilves/3877149/. zuletzt geprüft: 31. März 2015.

[18] Kalev Aasmae. *4G beauty contest shoots Estonia to the top of Europe's LTE leaderboard*. http://www.zdnet.com/article/4g-beauty-contest-shoots-estonia-to-the-top-of-europes-lte-leaderboard/. zuletzt geprüft: 29. März 2015. Juni 2013.

[19] Anthony Cuthbertson. *Estonia plans 5G mobile network pilots in 2016*. http://www.ibtimes.co.uk/estonia-plans-5g-mobile-network-pilots-next-year-1486889. zuletzt geprüft: 29. März 2015. Feb. 2015.

[20] Visitestonia.com. *Communications: Mail, Phone & Internet in Estonia.* http://www.visitestonia.com/en/about-estonia/traveller-information/mail-phone-internet. zuletzt geprüft: 29. März 2015. 2015.

[21] Wikipedia. *Toomas Hendrik Ilves.* http://de.wikipedia.org/wiki/Toomas_Hendrik_Ilves. zuletzt geprüft: 31. März 2015. 2015.

[22] Wikipedia. *Tiigrihüpe.* http://en.wikipedia.org/wiki/Tiigrihüpe. zuletzt geprüft: 31. März 2015. 2015.

[23] Statistics Estonia. *IC32: COMPUTER AND INTERNET USERS AGED 16-74 BY GROUP OF INDIVIDUALS.* http://pub.stat.ee/px-web.2001/Dialog/varval.asp?ma=IC32&ti=COMPUTER+AND+INTERNET+USERS+AGED+16-74+BY+GROUP+OF+INDIVIDUALS&path=../I_Databas/Social_life/06Households/06Household_living_conditions/12Information_technology_in_household/&lang=1. zuletzt geprüft: 31. März 2015.

[24] European Commission. *Andrus Ansip.* http://ec.europa.eu/commission/2014-2019/ansip_en. zuletzt geprüft: 31. März 2015. 2014.

[25] Kanzlei Hoesmann. *Wann liegt eine rechtsgültige Unterschrift vor?* http://hoesmann.eu/wann-liegt-eine-rechtsgultige-unterschrift-vor/. zuletzt geprüft: 30. März 2015.

[26] Wikipedia. *Unterschrift.* http://de.wikipedia.org/wiki/Unterschrift. zuletzt geprüft: 31. März 2015. 2015.

[27] Wikipedia. *Identitätsfeststellung.* http://de.wikipedia.org/wiki/Identitätsfeststellung. zuletzt geprüft: 31. März 2015. 2014.

[28] Wikipedia. *Digitale Signatur.* http://de.wikipedia.org/wiki/Digitale_Signatur. zuletzt geprüft: 31. März 2015. 2015.

[29] Wikipedia. *Elektronische Signatur.* http://de.wikipedia.org/wiki/Elektronische_Signatur. zuletzt geprüft: 31. März 2015. 2015.

[30] *The Estonian ID Card and Digital Signature Concept.* http://id.ee/public/The_Estonian_ID_Card_and_Digital_Signature_Concept.pdf. zuletzt geprüft: 31. März 2015. AS Sertifitseerimiskeskus. Pärnu mnd 141. 11314 Tallinn, 2003.

[31] ID.ee. *PIN codes*. http://www.id.ee/index.php?id=31017. zuletzt geprüft: 30. März 2015.

[32] ID.ee. *How to change PIN1, PIN2 and PUK codes using ID-card utility?* http://www.id.ee/index.php?id=34284. zuletzt geprüft: 30. März 2015.

[33] ID.ee. *What are certificates?* http://www.id.ee/index.php?id=31015. zuletzt geprüft: 30. März 2015.

[34] Information System Authority Republic of Estonia. *X-Road Factsheet*. https://www.ria.ee/public/x_tee/X-road-factsheet-2014.pdf. zuletzt geprüft: 30. März 2015. 2014.

[35] Information System Authority Republic of Estonia. *X-Road Technical Factsheet*. https://www.ria.ee/public/x_tee/Xroad-technical-factsheet-2014.pdf. zuletzt geprüft: 30. März 2015. 2014.

[36] e-estonia.com. *X-Road*. https://e-estonia.com/component/x-road/. zuletzt geprüft: 31. März 2015.

[37] Botschaft von Estland in Berlin. *E-Estland*. http://www.estemb.de/estland/it. zuletzt geprüft: 31. März 2015. 2012.

[38] Riigikogu. *Personal Data Protection Act*. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/509072014018/consolide. zuletzt geprüft: 30. März 2015. 2014.

[39] e-estonia.com. *Mobile-ID*. https://e-estonia.com/component/mobile-id/. zuletzt geprüft: 31. März 2015.

[40] Vabariigi Valimiskomisjon. *Statistics about Internet Voting in Estonia*. http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics. zuletzt geprüft: 30. März 2015. 2015.

[41] Vabariigi Valimiskomisjon. *Internet Voting in Estonia*. http://www.vvk.ee/voting-methods-in-estonia/. zuletzt geprüft: 30. März 2015. 2015.

[42] Kristina Reinsalu. “The implementation of Internet democracy in Estonian local governments”. Verfügbar unter http://dspace.utlib.ee/dspace/handle/10062/8081, zuletzt geprüft: 30. März 2015. Diss. University of Tartu, 2009.

[43] e-estonia.com. *E-residency – up against great expectations*. https://e-estonia.com/e-residency-up-against-great-expectations/. zuletzt geprüft: 30. März 2015. 2015.

[44] e-estonia.com. *What is e-Residency?* https://e-estonia.com/e-residents/about/. zuletzt geprüft: 30. März 2015. 2015.

[45] Martin Weigert. “Alle sind Willkommen: Estland erfindet die virtuelle Staatsbürgerschaft”. In: *Netwertig.com* (2014). http://netzwertig.com/2014/11/12/alle-sind-willkommen-estland-erfindet-die-virtuelle-staatsbuergerschaft/. zuletzt geprüft: 30. März 2015.

[46] Ralf Kölbel und Gabor Paal. “Estland: Der durchdigitialisierte Staat - Vorreiter für Europa?” In: *SWR* (Nov. 2013). http://www.swr.de/swr2/wissen/estland-digital/-/id=661224/nid=661224/did=12419354/1j4iy32/. zuletzt geprüft: 29. März 2015.

[47] Riigikogu. *Public Information Act*. https://www.riigiteataja.ee/en/eli/510072014004/consolide. zuletzt geprüft: 30. März 2015. 2014.

[48] Estonian Data Protection Inspectorate. *Inspectorate*. http://www.aki.ee/en/inspectorate. zuletzt geprüft: 30. März 2015. 2014.

[49] Estonian Data Protection Inspectorate. *Implementation of the Public Information Act and the Personal Data Protection Act in 2013, Recommendations for 2014*. http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Aastaraamat%202013%20t6lkesse_en.pdf. zuletzt geprüft: 30. März 2015. 2014.

[50] FAZ.NET dpa. “Fast einhundert Verletzte bei Krawallen in Estland”. In: *FAZ.NET* (Apr. 2007). http://www.faz.net/aktuell/politik/ausland/streit-um-kriegerdenkmal-fast-einhundert-verletzte-bei-krawallen-in-estland-1435161.html. zuletzt geprüft: 30. März 2015.

[51] Jasper von Altenbockum. “Ist ein Internetangriff der Ernstfall?” In: *F.A.Z.* 138 (Juni 2007). Verfügbar unter http://www.faz.net/aktuell/politik/ausland/streit-um-kriegerdenkmal-fast-einhundert-verletzte-bei-krawallen-in-estland-1435161.html. zuletzt geprüft: 30. März 2015, S. 6.

[52] BBC News. “Estonia fines man for ’cyber war’”. In: *BBC News* (Jan. 2008). http://news.bbc.co.uk/2/hi/technology/7208511.stm. zuletzt geprüft: 31. März 2015.

[53] Thorsten Kleinz. “31C3: Internetwahlen sind manipulierbar”. In: *heise.de* (2014). http://www.heise.de/newsticker/meldung/31C3-Internetwahlen-sind-manipulierbar-2507408.html. zuletzt geprüft: 30. März 2015.

[54] J. Alex Halderman u. a. *Independent Report on E-voting in Estonia*. https://estoniaevoting.org/. zuletzt geprüft: 30. März 2015. 2014.

[55] N.N. “Estlands Regierung verliert Mehrheit”. In: *Sueddeutsche Zeitung* (2015). http://www.sueddeutsche.de/politik/parlamentswahl-estlands-regierung-verliert-absolute-mehrheit-1.2373590. zuletzt geprüft: 30. März 2015.

[56] ZEIT ONLINE, AFP und ab. “USA rüsten baltische Staaten gegen Russland auf’. In: *ZEIT ONLINE* (2015). http://www.zeit.de/politik/ausland/2015-03/russland-estland-lettland-litauen-usa-waffenlieferung. zuletzt geprüft: 30. März 2015.

[57] ZEIT ONLINE u. a. “Russland will Kurzstreckenraketen in Kaliningrad aufstellen”. In: *ZEIT ONLINE* (2015). http://www.zeit.de/politik/ausland/2015-03/russland-militaermanoever-kaliningrad-krim. zuletzt geprüft: 30. März 2015.

[58] Timo Brücken. “Facebook erkennt Sie auf jedem Bild”. In: *stern.de* (2013). http://www.stern.de/digital/online/neue-gesichtserkennung-deepface-facebook-erkennt-sie-auf-jedem-bild-2097338.html. zuletzt geprüft: 31. März 2015.

[59] Eike Kühl. “FBI sammelt Millionen Fotos von Unverdächtigen”. In: *ZEIT ONLINE* (2015). http://www.zeit.de/digital/datenschutz/2014-04/fbi-gesichtserkennung-datenbank. zuletzt geprüft: 30. März 2015.

[60] Kai Biermann. “Ein fast unmögliches Gesetz”. In: *ZEIT ONLINE* (2015). http://www.zeit.de/digital/datenschutz/2015-03/vorratsdatenspeicherung-heiko-maas-sigmar-gabriel-gesetz. zuletzt geprüft: 31. März 2015.

[61] Kai Biermann. “BND speichert 220 Millionen Telefondaten – jeden Tag”. In: *ZEIT ONLINE* (2015). http://www.zeit.de/digital/datenschutz/2015-01/bnd-nsa-metadaten-ueberwachung. zuletzt geprüft: 31. März 2015.

[62] Eike Kühl. “Cameron will Verschlüsselung verbieten”. In: *ZEIT ONLINE* (2015). http://www.zeit.de/digital/datenschutz/2015-01/cameron-grossbritannien-verbot-verschluesselung. zuletzt geprüft: 31. März 2015.

[63] Gábor Paál. “Durchdigitalisiert und sicher?” In: *Deutschlandfunk* (2013). http://www.deutschlandfunk.de/estland-durchdigitalisiert-und-sicher.684.de.html?dram:article_id=270634. zuletzt geprüft: 31. März 2015.

[64] Inc Code for America Labs. *About*. http://www.codeforamerica.org/about/. zuletzt geprüft: 31. März 2015. 2014.

[65] Kees Schalken. “Internet as a New Public Sphere for Democracy?” In: *Public Administration in an Information Age*. Hrsg. von Wim B.H.J. van de Donk und Ignace Th.M. Snellen. IOS Press, 1998. Kap. 10, S. 159–174.