Das mediale Monopol des Staates und seine Verteidigungslinien

Jens Schröter

»Eine Urkunde ist ein Schriftstück, das durch seine formalisierte Gestaltung rechtsverbindliche Glaubwürdigkeit erhält.«[1] Dokumente in der Gestalt von Urkunden sind ein zentrales Medium staatlicher und wirtschaftlicher Ordnung – sie legen etwa Besitzansprüche fest, bestimmen aber auch, z. B. in der Form von Personalpapieren, die Identität von Personen.[2] Wegen dieser zentralen Bedeutung für die, wie es Christoph Engemann im Anschluss an Michel Foucault treffend formuliert hat, *Gouvernemedialität*,[3] muss die *Echtheit* solcher Dokumente sichergestellt werden können. Es muss sicher sein, dass es sich wirklich um ein offizielles Dokument handelt, dass die auf ihm enthaltene Information zutreffend und verlässlich ist.[4] Dem Gewaltmonopol des Staates entspricht so gesehen auch ein mediales Monopol – bestimmte Typen von Dokumenten dürfen nur von den zuständigen Stellen verfertigt werden, Fälschungen werden schwer bestraft (nach § 267 des StGB mit Geldstrafen oder Haftstrafen bis zu zehn Jahren). Doch um die Hersteller von Fälschungen zu bestrafen, müssen die Fälschungen erst einmal erkannt werden. Daher ist die Medialität von Urkunden und anderen staatlichen Dokumenten, z. B. Geldscheinen, den Medien des Staates und der Ökonomie, komplex.

1 Tilo Werner: Urkunde, in: Gert Ueding (Hg.): Historisches Wörterbuch der Rhetorik, Darmstadt 2009, Bd. 9, Sp. 934–941, hier S. 934.

2 Vgl. John Torpey: The Invention of the Passport, Cambridge 2000. Vgl. auch Edward Higgs: From Frankpledge to Chip and Pin: Identification and Identity in England, 1475–2005, in: Karel de Leeuw und Jan Bergstra (Hg.): The History of Information Security: A Comprehensive Handbook, Amsterdam/Oxford 2007, S. 243–262.

3 Vgl. Christoph Engemann: Write me down, make me real. Zur Gouvernemedialität digitaler Identität, in: Jan Hendrik Passoth und Josef Wehner (Hg.): Quoten, Kurven und Profile. Zur Vermessung der sozialen Welt, Wiesbaden 2013, S. 205–227.

4 Vgl. zur ständig steigenden Zahl von ›Identitätsdiebstählen‹, einem großen Problem, vor allem für die Geldwirtschaft, Chris Jay Hoofnagle: Identity Theft. Making the Known Unknowns Known, in: Harvard Journal of Law & Technology 1 (2007), S. 98–122. Vgl. auch Pieter Wisse: Semiotics of Identity Management, in: Karel de Leeuw und Jan Bergstra (Hg.): The History of Information Security: A Comprehensive Handbook, Amsterdam/Oxford 2007, S. 167–196.

Es gilt, dass »erst die spezifische Kombination von Urkundentext und Urkundenmedium die Beweiskraft der Urkunde konstituiert; die bloße Kopie eines Urkundentextes auf einem neuen Textträger hat keine Rechtsgültigkeit (es sei denn die Kopie wird wiederum beurkundet)«.[5] Das ›Urkundenmedium‹ muss mithin so beschaffen sein, dass es nicht leicht durch unautorisierte Personen nachzuahmen ist, bzw. es muss leicht feststellbar sein, ob eine gegebene Urkunde die richtige Medialität aufweist (andernfalls ist es eine Fälschung): »Die Eigenschaften bestimmter Medien regten auch zur Entwicklung von Techniken zur Fälschungssicherung an.«[6]

Vor diesem Hintergrund stellt sich die Frage nach dem »Medienwandel der Staatlichkeit«[7] – nicht nur in der Hinsicht, dass Staaten unter dem Eindruck der ›digitalen Revolution‹ neue digitale Dokumente (›E-Government‹) erzeugen und beherrschen müssen,[8] sondern auch in jener, dass die Ausbreitung neuartiger Medientechnologien immer wieder die Kriterien der Echtheit der Urkundenmedien bedrohen und daher Gegenreaktionen auslösen. Das mediale Monopol des Staates ist nicht ein- für allemal gegeben, sondern muss fortlaufend verteidigt werden – dabei wird eine durchaus militärisch anmutende Metaphorik verwendet. Es wird (hinsichtlich der Echtheit von Geld) von drei ›Verteidigungslinien‹ (*lines of defence*) gesprochen. Deren erste besteht in Verfahren, die normalen Bürgern erlauben sollen, eine Fälschung auf den ersten Blick zu erkennen. Sind die Fälschungen aber gut genug, gelingt das womöglich nicht mehr. Dann greift die zweite Verteidigungslinie. Diese wird gebildet von Personen, die professionell mit Geld arbeiten (also z. B. Bankangestellte oder Händler) und spezielle Geräte verwenden (wie z. B. Geldzählmaschinen). Entdecken auch diese die Fälschungen nicht, dann gibt es noch die letzte, dritte und höchste Verteidigungslinie um das mediale Monopol des Staates – die professionelle, forensische Untersuchung des verdächtigen Doku-

5 Werner: Urkunde (wie Anm. 1), Sp. 936.

6 Ebd. Dort finden sich interessante Hinweise auf historische Verfahren der Echtheitssicherung, wie etwa die Kerbhölzer. Vgl. auch Thomas Vogtherr: Urkunden und Akten, in: Michael Maurer (Hg.): Aufriß der Historischen Wissenschaften in sieben Bänden, Stuttgart 2002, Bd. 4 (Quellen), S. 146–167, hier S. 154 dazu, dass die »Standardisierung des Aussehens« von Urkunden »eine Sicherung gegen Urkundenfälschung« ist. Auf S. 157 bemerkt Vogtherr, dass die »moderne Diplomatik, die wissenschaftliche Lehre von den Urkunden, um 1700 ihren Anfang« nahm: »Die Grundfrage war damals und ist bis heute das *discrimen veri ac falsi*, die Unterscheidung des Echten vom Falschen.«

7 Engemann: Write me down (wie Anm. 3), S. 212.

8 Vgl. Christoph Engemann: Im Namen des Staates. Der elektronische Personalausweis und die Medien der Regierungskunst, in: Zeitschrift für Medien- und Kulturforschung 2/2 (2011), S. 211–228.

ments in Laboratorien. Die komplexe Medialität von Banknoten z. B. steht im Dienste aller drei Verteidigungslinien; es gibt Merkmale, die sowohl auf die Wahrnehmungs- und Umgangsgewohnheiten normaler Bürger, professionelle Händler als auch auf Spezialisten für Fälschungen zugeschnitten sind.[9]

Die historische Entfaltung des Kampfes um das mediale Monopol des Staates soll im Folgenden schlaglichtartig an zwei medienhistorischen Umbrüchen aufgezeigt werden. Der *erste* Umbruch ist die Ausbreitung der Fotokopierer ab den 1960er und der Farbkopierer ab den 1980er Jahren. Mit diesen Technologien standen zunehmend leistungsfähigere Verfahren zur Herstellung von Kopien zur Verfügung. So sehr der Fotokopierer einerseits Instrument der Effizienzsteigerung und Beschleunigung der Zirkulation von Schriftstücken in staatlichen und ökonomischen Bürokratien war, so sehr war er andererseits auch eine potentielle Bedrohung für die Dokumente, insofern er das Kopieren signifikant erleichterte. Eine Reaktion darauf war der zunehmende Einsatz optischer Dokumentensicherheit, d.h. von Markierungen: z. B. auf Geldscheinen, die von Fotokopierern nicht kopiert werden können bzw. nur so, dass die Nutzer der drei Verteidigungslinien zumindest in der letzten Instanz erkennen können, dass es sich nicht um das korrekte ›Urkundenmedium‹ handelt.

Der *zweite* Umbruch ist jener zu den Personalcomputern ab den 1990er Jahren und den mit ihnen verbundenen Peripherien wie Scanner und Farbdrucker, die ebenfalls in zuvor ungekanntem Ausmaß Reproduktionen erlaubten. Die speziellen optischen Markierungen auf Dokumenten aus der historischen Verteidigung gegen die Fotokopierer bleiben bestehen, die digitale Datenverarbeitung durch die Computer erfordert und erlaubt aber neue zusätzliche Sicherheitsmerkmale. Zusammenfassend schreibt Schell:

»In the last two decades of the 20th century, security printers and document issuers were confronted with color copiers combined with laser printers […], and home reproduction units consisting of a PC linked with a scanner and an inkjet printer. The existing armoury obviously became less effective if not obsolete and at least new *firstline* features were urgently requested: The threat was tackled this time by introducing: 3D devices, optically variable printed images and regarding the *second-line of defence*, printed covert images, tracers and/or taggants.«[10]

9 Vgl. Karel Johan Schell: History of Document Security, in: Karel de Leeuw und Jan Bergstra (Hg.): The History of Information Security: A Comprehensive Handbook, Amsterdam/Oxford 2007, S. 198–241, hier S. 219.

10 Ebd., S. 220.

1. Die Xerographie und die optische Verteidigungslinie

Der Kampf zwischen Fälscherinnen und Fälschern und den Spezialistinnen und Spezialisten ist alt, denn Echtheitsmarkierungen wie Wasserzeichen wurden schon im 14. Jahrhundert eingesetzt.[11] Allerdings ist das 20. Jahrhundert, nach dem großen Wort Walter Benjamins, das Zeitalter der technischen Reproduzierbarkeit. Schon Benjamin selbst betonte, dass die technische Reproduzierbarkeit keineswegs nur die Kunst erfasst.[12] Allerdings hatte Benjamin erstens nicht die Reproduzierbarkeit von Geld und anderen Dokumenten und zweitens – natürlich – nicht die Entwicklung der Xerographie im Blick. Jenes Verfahren entwickelte sich, obwohl die ersten erfolgreichen Experimente Chester Carlsons schon 1938 stattfanden, aufgrund verschiedener technischer, aber auch finanzieller Probleme erst langsam (und nach dem frühzeitigen Tod Benjamins). Mit dem Beginn der 1960er Jahre zog die Technologie dann immer schneller in die Büros ein und ist heute nicht mehr wegzudenken.[13] Ein, wenn nicht *das* zentrale Motiv von Carlson, sich

11 Vgl. ebd., S. 198–204. Vgl. auch Gerhard F. Strasser: The Rise of Cryptology in the European Renaissance, in: Karel de Leeuw und Jan Bergstra (Hg.): The History of Information Security: A Comprehensive Handbook, Amsterdam/Oxford 2007, S. 277–325.

12 Vgl. Walter Benjamin: Das Kunstwerk im Zeitalter seiner technischen Reproduzierbarkeit. Drei Studien zur Kunstsoziologie, Frankfurt am Main 1977, S. 13.

13 Vgl. zu den Details ihrer Entwicklung Joseph Mort: The Anatomy of Xerography. Its Invention and Evolution, Jefferson/NC 1989. Zur Gründung von Xerox und der Durchsetzung der Fotokopierer vgl. v. a. S. 59 und S. 62–69. Vgl. auch Joseph Mort: Xerography: A Study in Innovation and Economic Competitiveness, in: Physics Today 47 (1994), S. 32–38. Vgl. Monika Domman: Autoren und Apparate. Die Geschichte des Copyrights im Medienwandel, Frankfurt am Main 2014, S. 235–267, die die Geschichte der Fotokopierer instruktiv in die Geschichte des Copyrights einbettet, allerdings mit keinem Wort Kopierschutz- und Dokumentensicherheitstechnologien erwähnt. Vgl. Lisa Gitelman: Paper Knowledge. Toward a Media History of Documents, Durham/London 2014, S. 83–110, die die Geschichte der Fotokopie aus Sicht von Nutzerpraktiken erzählt, auch am Beispiel des Kopierens geheimer Dokumente – doch auch hier spielt die Geschichte der medialen Dokumentensicherung keine Rolle. Das hat damit zu tun, dass interne Papiere, die dann kopiert und der Öffentlichkeit zugespielt werden, selten so stark geschützt sind, da es oft Papiere für den schnellen täglichen Gebrauch sind. Außerdem spielt es für die Presse, der die Papiere zugespielt werden, keine Rolle, ob das vorliegende Papier ›echt‹ ist, denn es kommt nur auf den ggf. skandalösen Inhalt an. Noch genauer: Natürlich will auch die Presse keine gefälschten Dokumente zitieren und sich blamieren, doch deren Echtheit bezieht sich auf den Inhalt und nicht auf die Echtheit in dem Sinne, dass es nur dieses eine Dokument sein darf, das einen bestimmten Zustand (etwa eine Staatsbürgerschaft) performiert.

einem automatischen Kopierverfahren zuzuwenden, war, die langwierigen und mühsamen Prozeduren der Vervielfältigung von Schriftstücken in bürokratischen Arbeitszusammenhängen zu erleichtern.[14] In der Tat war die Beschleunigung solcher papierbasierten Verwaltungsprozesse von zentralem Interesse. Firmen, die Fotokopierer hatten, konnten ihre Arbeitsprozesse beschleunigen und erhofften sich einen Vorteil in der Marktkonkurrenz. Diese Situation wirkte als eine Art Beschleuniger, eine ›supervening social necessity‹,[15] für die Akzeptanz des Fotokopierers – und bald schon war Xerox ein Großkonzern.[16]

Doch dieser vielfach gefeierte Mythos des visionären Erfinders, der mit einer zunächst für verrückt gehaltenen Idee am Ende ein Vermögen macht und die Welt – es versteht sich von selbst – zum Besseren verändert, krankt an dem Mangel aller linearen Mediengeschichten, nämlich an der Ausblendung, dass neue Technologien sich nicht allein als Erfolge beschreiben lassen, sondern auch völlig neue Probleme produzieren. Denn die Xerographie warf einen Schatten voraus, und dieser war die Gefährdung des medialen Monopols des Staates. Die ersten Kopierer waren umständliche, fehleranfällige Geräte, die zudem nur schwarz-weiß kopieren konnten und insofern keine Bedrohung darstellten. Doch das änderte sich: »From the 1960s until the late 1970s, the copiers reproduced in black and white were neither threatening graphic arts and printers nor its *niche* of security printers. That threat changed when colour copying and laser printing arrived«.[17] Eine der Verteidigungsmaßnahmen ist, dass der Farbraum der Farbkopierer begrenzt ist. Abb. 1 (S. 18) zeigt, dass der von Kopierern darstellbare Farbraum (das unregelmäßige Sechseck, in dem ›W Color Copier‹ steht) nur einen Ausschnitt aus dem möglichen Farbraum darstellt: »So in order to optimise the effectiveness of the use of colour against colour reproduction, a person has to choose a colour outside of the RGB gamut and outside the colour copier hexagon, which is why the US dollar is green, the Euro ten is stone red, while the Euro twenty is blue violet, etcetera.«[18] Das durch keine ästhetische Theorie aufzuklärende Rätsel, warum die Banknoten die Farben haben, die sie haben, erklärt sich also ganz einfach – ihre bloße Farbigkeit war und ist bereits eine Verteidigungslinie um das mediale Monopol des Staates. Die Farbe als solche ist bereits eine Barriere.

14 Ebd., S. 49. Vgl. David Owen: Copies in Seconds. Chester Carlson and the Birth of the Xerox Machine, New York 2004, S. 70 und S. 82.

15 Vgl. Brian Winston: Media Technology and Society. A History from the Telegraph to the Internet, London, New York 1998, S. 6.

16 Vgl. Owen: Copies in Seconds (wie Anm. 14), S. 180f., S. 192, 222–225 und 239–243.

17 Schell: History of Document Security (wie Anm. 9), S. 217.

18 Ebd.

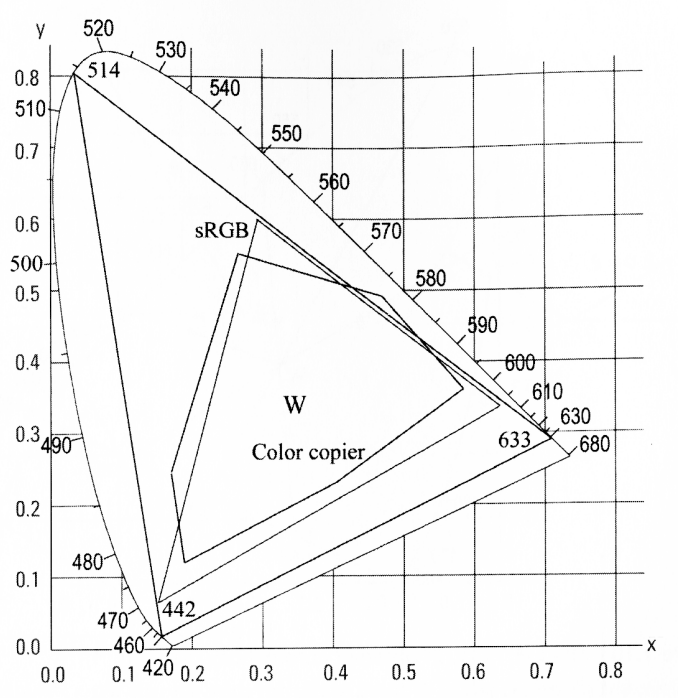

Abb. 1: CIE 1931 Farbdiagramm, aus: Renesse: Optical Document Security, S. 18.

Doch dies änderte sich schon kurze Zeit später: Einerseits wurden die Farbkopierer besser; so nennt Schell das Jahr 1980 als die Zeit, in der sich die Farblaserkopierer auszubreiten begannen.[19] Dazu kommt andererseits und deutlich schwerwiegender, dass normale Nutzer (also die ›erste Verteidigungslinie‹) womögliche Verfärbungen gar nicht bemerkten (denn dazu müsste man ja das in Abb. 1 dargestellte Farbraumschema kennen) – es schien also ratsam, sich nicht allein auf die Farbigkeit zu verlassen.

Schon in den 1970er Jahren kam es zu nervösen Reaktionen auf die neuen Technologien, es wurden internationale Arbeitsgruppen gebildet.[20] Neue Verfahren mussten her, die den Kopierern neuen und zusätzlichen Widerstand entgegensetzen konnten. Mittlerweile hat sich das Repertoire der *Optical Document Security* drastisch erweitert.[21]

19 Vgl. ebd., S. 217.

20 Vgl. ebd., S. 200.

21 Vgl. als besten und umfassendsten Überblick Rudolf L. van Renesse: Optical Document Security, 3. Auflage, Boston, London 2005.

»The dramatic shifts in reproduction technology since the 1970s […] brought issuers and producers of security documents to the point of strengthening their potential. They expanded in-house research and development groups; outsourced dedicated research assignments; and united to share efforts. The history of the development of holography runs more or less parallel with this growing awareness.«[22]

Hier taucht die Holographie als eine Technologie auf, deren Entwicklung und Ausbreitung maßgeblich von den Bedürfnissen der Dokumentensicherheit angetrieben wurde. Zwar ist die Geschichte der Holographie wohl komplexer,[23] dass aber eines ihrer wichtigsten Einsatzgebiete seit den 1980er Jahren in der Dokumentensicherheit liegt, ist unstrittig: »In 1983 MasterCard International, Inc. launched the first credit cards carrying embossed holograms that were produced by the American Bank Note Company in New York. The MC holograms were the widest distribution of holography in the world at that time.«[24] Heutzutage sind auf fast allen Geldscheinen,[25] Kreditkarten[26] oder Personalausweisen[27] Hologramme oder zumindest der Holographie ähnliche Verfahren im Einsatz.[28] Die Holographie ist keine exotische Spezialtechnik, es gibt vielmehr eine veritable holographische Alltagskultur, deren Existenzgrund in der Verteidigung des medi-

22 Schell: History of Document Security (wie Anm. 9), S. 231.

23 Vgl. Sean Johnston: Holographic Visions. A History of New Science, Oxford 2006.

24 Schell: History of Document Security (wie Anm. 9), S. 231.

25 Vgl. Ian M. Lancaster und Astrid Mitchell: The Growth of Optically Variable Features on Banknotes, in: SPIE Proceedings 5310, San Jose, CA 2004, S. 34–45.

26 Vgl. Don Tomkins: Application of Holograms to Credit Cards, in: ICMA. The Voice of the Plastic Card Industry (May/June 1998), S. 8–17.

27 Auf deutschen Personalausweisen etwa das sogenannte ›Identigram‹-Verfahren, vgl. Bundesministerium des Innern: Das Identigram. Ein neues Sicherheitsmerkmal für Pässe und Personalausweise, unter: https://www.bundesdruckerei.de/sites/default/files/identigramr_flyer.pdf (16.03.2014).

28 Wie z. B. Kinegramme, vgl. Wikipedia: Kinegramm (Sicherheitstechnik), unter: http://de.wikipedia.org/wiki/Kinegramme (16. 03. 2014). Oft werden diese Verfahren, insofern sie auf demselben wellenoptischen Wissen beruhen, unter dem Oberbegriff ›Holographie‹ oder ›Hologramme‹ zusammengefasst, obwohl das im strengen Sinne nicht korrekt ist. So werden in der, in Sicherheitsanwendungen oft benutzten (vgl. Sean F. Johnston: Holographic Visions, Oxford 2006, S. 220), ›*dot matrix holography*‹ keine Interferenzmuster zwischen Objekt- und Referenzwelle aufgezeichnet, sondern mithilfe von Interferenz zwischen zwei Strahlen schreibt man Bildpunkte, die Beugungsgitter sind, und setzt so ein Bild digital zusammen. Vgl. Mindaugas Andrulevičius, Tomas Tamulevičius und Sigitas Tamulevičius: Formation and Analysis of Dot-Matrix Holograms, in: Materials Science (Medžiagotyra), 4 (2007), S. 278–281.

alen Monopols des Staates besteht. Holographische Bilder – wie etwa die plastische Abbildung einer kleinen weißen Taubenskulptur auf einer *Visacard* – können mit Fotokopierern nicht reproduziert werden, da Holographie auf der Wellenoptik beruht und die mit ihr transportierte Information von dem geometrisch-optischen Abbildungssystem eines Fotokopierers nicht übertragen werden kann.[29] Im Alltag – der *first line of defence* – zeigt sich das für Normalbürger darin, dass das farbig schillernde, blickwinkelabhängige und oft dreidimensionale Erscheinungsbild einer holographischen Markierung in einer Kopie verschwindet. Durch eine solche optische Markierung wird die Echtheit des Urkundenmediums verbürgt – und gegen auch die allerbesten Farbkopierer (oder Scanner) verteidigt.[30]

2. Computer und die algorithmische Verteidigungslinie

Die Erwähnung der ›Scanner‹ verweist bereits auf den nächsten Medienwandel, der erneut eine Veränderung der Sicherheitstechniken provozierte. Zwar sind die holographischen Sicherheitsmerkmale auch für die Scanner (und angeschlossenen Computer z. B. mit Adobe Photoshop) unreproduzierbar; optische Sicherheitsmerkmale funktionieren aber, wie oben bemerkt, dadurch, dass – zumindest in der *first line of defence* – durchschnittliche Nutzer von Dokumenten wie Pässen oder Geld auch erkennen können müssen, dass die Sicherheitsmarkierung auf dem Urkundenmedium nicht so aussieht, wie sie aussehen sollte. Daher gibt es eine intensive Pädagogik, um Nutzer dieses Wissen zu vermitteln, etwa den ›Euroblütentrainer‹ auf www.polizei-beratung.de, mit dem man Schritt für Schritt lernen kann, die Echtheit des Urkundenmediums zu erkennen.[31] Doch diese Pädagogik kann scheitern, denn es könnte ja sein, dass die Nutzer sie nicht nutzen und mithin gar nicht wissen, wie die Markierungen aussehen sollen, in einer entsprechenden Situation durch schlechte Lichtverhältnisse nicht recht sehen können oder irgendwie anderweitig abgelenkt sind. Daher ist es ein naheliegender Gedanke, den menschlichen Faktor aus zumindest der ersten Verteidigungslinie herauszunehmen[32] und

29 Vgl. Jens Schröter: Das holographische Wissen und die Nicht-Reproduzierbarkeit, in: Stefan Rieger und Jens Schröter (Hg.): Das holographische Wissen, Berlin 2009, S. 77–86.

30 Natürlich hat es nicht an Versuchen gefehlt, Hologramme zu fälschen, doch die Ergebnisse waren selten überzeugend. Vgl. David Pizzanelli: Counterfeit Holograms and Simulations, in: SPIE Proceedings 3314, San Jose, CA 1998, S. 86–96.

31 Vgl. unter: http://www.bluetentrainer.polizei-beratung.de/blueten_euro/trainer_d.html (17. 03. 2014).

32 Bei der zweiten und dritten Verteidigungslinie stellt das kein Problem dar, da es sich in der zweiten Linie um professionell mit Geld arbeitende Personen handelt, die mithin

den Schutz noch stärker an technische Vorrichtungen zu delegieren, was mit digitalen Technologien zumindest im Prinzip möglich wird. Schell hat das bündig zusammengefasst: »Instead of adding features that are difficult to reproduce, codes are embedded that thwart reproduction.«[33] D.h.: »Another idea might be to incorporate features that locate copier type and serial number or that hamper the copier mechanism itself.«[34] Was nichts anderes bedeutet, als dass moderne Fotokopierer auf ihre Kopien einen für das menschliche Auge nicht sichtbaren Punktecode einbauen, der es erlaubt, genau festzustellen, um welchen Kopierer an welchem Ort es sich handelt.[35] Rosengart hat präzisiert, dass es mithilfe dieser Punkte möglich ist, bis zu 512 Bit, d.h. 64 Byte, verborgen auf eine Farbkopie zu schreiben. »Damit wäre es sogar möglich, jede Kopie einzeln zu kennzeichnen oder zumindest die aktuelle Uhrzeit/Datum auf der Kopie zu vermerken.«[36] Was aus Sicht derjenigen, die Fälscher verfolgen, sinnvoll sein mag, hat allerdings bedenkliche Nebenwirkungen: »Wer wird sich noch trauen, Bestechungsskandale aufzudecken und entsprechende Beweise, z. B. an die Presse, weiterzureichen, wenn er weiß, dass die Anonymität einer Kopie nicht mehr gewährleistet ist, sondern dass z. B. sein Arbeitgeber als Besitzer des Gerätes ein Dokument bis in eine bestimmte Abteilung, ein bestimmtes Büro zurückverfolgen kann?«[37] Auch könnte die Vervielfältigung unliebsamer politischer Schriften zurückverfolgt werden, eine Option, die in autoritären und totalitären Staaten auf Interesse stoßen dürfte.[38]

Auf www.polizei-beratung.de wird angemerkt: »Viele Täter reagieren auf die Entwicklungen des Technikmarktes erstaunlich flexibel. Die meisten Farbkopierer sind inzwischen mit Codierungssystemen ausgerüstet, mit dem sich eine Farbkopie dem jeweiligen Kopierer genau zuordnen lässt. Deshalb weichen immer mehr

sensibler gegenüber Fälschungen sein dürften und zudem Gerätschaften haben, um Fälschungen zu erkennen, z. B. die Geldscheinprüfer der Firma Safescan, vgl. Automatische Geldscheinprüfer, unter: https://www.safescan.com/de/products/30/automatische-geldscheinprufer/ (17. 03. 2014). Bei der dritten Linie handelt es sich ohnehin um Spezialisten für Fälschungserkennung.

33 Schell, History of Document Security (wie Anm. 9), S. 224.

34 Ebd., S. 222.

35 Vgl. ebd., S. 223.

36 Frank Rosengart: Datenspur Papier, in: Die Datenschleuder 86 (2005), S. 19–21, hier S. 21.

37 Big-Brother-Award-Jury, zit. in: ebd., S. 21.

38 In autoritären Staaten wurden Fotokopierer von Seiten der Regierung wenig geschätzt, da sie die unkontrollierte Vervielfältigung von Information erlauben, z. B. in der UdSSR, vgl. Jakob Steinschaden: Digitaler Frühling. Wer das Netz hat, hat die Macht? Wien 2012, S. 112; vgl. auch Gitelman: Paper Knowledge (wie Anm. 13), S. 84. Doch die neuen Möglichkeiten, Kopien zu markieren, macht sie für Diktaturen wieder interessant.

Täter bei der Herstellung ihrer ›Blüten‹ auf die Hilfe eines Computer-Scanners aus.«[39] Der Kampf um das mediale Monopol geht weiter – und der Einsatz von heimischen Computern und ihrer Peripherie war auch eine Antwort auf die technische Delegation, mit der Kopierer Kopien lokalisierbar machten. Doch mit der Ausbreitung der bedrohlichen Digitaltechnologie in Haushalte,[40] mit der Ausbreitung der »häuslichen Vervielfältigung«,[41] rückt die Front ebenfalls dorthin vor: »Einigen Druckerherstellern zufolge soll in naher Zukunft jeder Tintenstrahldrucker und jeder Farblaserdrucker für Zuhause eine individuelle Markierung auf dem Papier hinterlassen.«[42]

Ein anderer Ansatz ist, den Prozess des Kopierens komplett zu unterbinden. Mit analogen Techniken ist das nicht möglich, bei digitalen schon. Es werden in den Vorlagen Muster untergebracht, so genannte *Taggants*,[43] die von den datenverarbeitenden Systemen von Fotokopierern, aber auch von Programmen wie *Photoshop* (ab Version 8) erkannt werden können. Taucht ein entsprechendes Muster auf, gibt es verschiedene Reaktionen: Es werden nur schwarze Seiten gedruckt, der Hinweis ›Kopie‹ wird auf dem Dokument angebracht – oder das Gerät (z. B. ein Kopierer) oder eine Software (z. B. *Photoshop*) verweigert vollständig die Arbeit, bei Ausgabe eines entsprechenden Hinweises, wie im Eigenversuch festgestellt werden konnte (siehe Abb. 2, S. 23).

---

39 Polizeiliche Kriminalprävention der Länder und des Bundes: Hier kann Ihnen etwas blühen, unter: http://www.polizei-beratung.de/themen-und-tipps/betrug/falschgeld.html (17. 03. 2014).

40 Vgl. Renesse: Optical Document Security (wie Anm. 21), S. xiv.

41 Roger-Pol Droit: Was Sachen mit uns machen. Philosophische Erfahrungen mit Alltagsdingen, Hamburg 2005, S. 152. Droit bezieht das aber noch auf den Fotokopierer und nicht auf die häuslichen Computer, wobei das verwundert, denn Fotokopierer waren anders als Scanner und Drucker sehr selten häuslich verfügbare Technologien.

42 Rosengart: Datenspur Papier (wie Anm. 36), S. 21.

43 Schell: History of Document Security (wie Anm. 9), S. 223 f. Eines der bekanntesten Beispiele für einen solchen *taggant* ist die sogenannte EURion-Konstellation, eine Punktwolke, die auf Euro-Banknoten zu finden ist und von Kopierern etc. erkannt werden soll. Der von der Central Banks Counterfeit Deterrence Group (Banknoten und Fälschungsbekämpfung, unter: http://www.rulesforuse.org (31. 03. 2014)), einer Arbeitsgruppe von 27 Zentralbanken und anderen Institutionen, die Banknoten herstellen, entwickelte Algorithmus CDS (Counterfeit Deterrence System) wird in Software wie *Photoshop* implementiert. Der genaue Mechanismus ist, aus naheliegenden Gründen, geheim. Steven J. Murdoch von der University of Cambridge untersucht dies seit einiger Zeit: Software Detection of Currency, unter: https://www.cl.cam.ac.uk/~sjm217/projects/currency/ (last update am 12. 10. 2009), (31. 03. 2014).

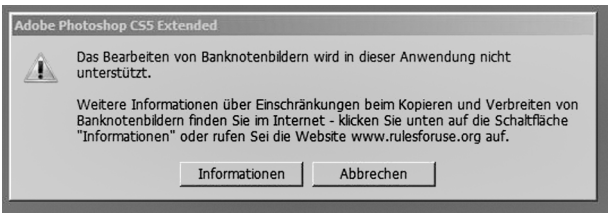

Abb. 2: Warnhinweis von *Photoshop* beim Versuch des Scannens einer 50-Euro-Note (Screenshot).

Fazit

Es gibt ein mediales Monopol des Staates: In demokratischen Staaten ist damit keine Kontrolle der traditionellen Massenmedien gemeint, aber selbst die demokratischsten Staaten üben eine strenge Kontrolle über ebenso alltägliche, aber in der Regel viel weniger beachtete Massenmedien aus – nämlich über die Urkundenmedien von Banknoten, Identitäts- und anderen wichtigen Dokumenten; aber auch über Sicherheitsmarkierungen zur Vermeidung von Produktpiraterie.[44] Man könnte nun versucht sein zu argumentieren, im Sinne des Wortes von der *Gouvernemedialität*, dass die medialen Verteidigungslinien eine Bedingung des staatlichen Gewaltmonopols sind, insofern etwa die Dokumente, die in politischen, polizeilichen und militärischen Befehlsketten zirkulieren, gesichert werden müssen. Nur wenn ihre Echtheit stabilisiert ist, können sie Befehle übertragen. Allerdings kann es ›Echtheit‹ nur geben, wenn die Differenz zwischen ›echt‹ und ›falsch‹ juristisch festgelegt und eine Fälschung überhaupt strafbar ist. Man kann z. B. mit digitalen Technologien im Prinzip verlustfreie Kopien von Musik- oder Filmdateien machen – doch das ist juristisch verboten, wesentlich um die Warenform, d. h. die kapitalistische Ökonomie, zu schützen.[45] Aber die juristisch geschützte Unterscheidung kann wiederum nur effektiv wirksam werden, wenn Markierungen auf den Urkundenmedien[46] eine unzulässige Kopie[47] erkennbar machen, ganz verhin-

44 Vgl. Holger Paul: Hologramme auf die Maschinen. Um sich vor Plagiatoren zu schützen, setzen die deutschen Maschinenbauer vor allem auf technologischen Vorsprung. Das reicht nicht aus, findet ihr Verband, in: Frankfurter Allgemeine Zeitung (19. 01. 2010), S. 20.

45 Vgl. Brian Winston: Media Technology and Society. A History: From the Telegraph to the Internet, Oxon 1998, S. 11 f. zum ›law of the suppression of radical potential‹; siehe auch Stefan Meretz: Der Kampf um die Warenform. Wie Knappheit bei Universalgütern hergestellt wird, in: Krisis 31 (2007), S. 52–89.

46 Bei digitalen Technologien muss man wohl eher von Markierungen ›in‹ den Medien sprechen, z. B. digitale Wasserzeichen und dergleichen.

47 Es kann auch zulässige Kopien geben, wie das Phänomen der ›beglaubigten Kopie‹ etwa zeigt, vgl. Wikipedia: Beglaubigung, unter: http://de.wikipedia.org/wiki/Beglaubigung

dern oder die Übeltäter lokalisierbar machen. Hier zeigt sich eine wechselseitige Irreduzibilität von juristischen und medialen Größen – nicht zuletzt auch darin, dass die verschiedenen Kopierschutzverfahren selbst wieder juristisch geschützt sind.[48] Die ›Urkunde‹ bzw. das ›Dokument‹ können also nur aufgrund dieser kausal nicht auflösbaren Verbindung von Recht und speziellen medialen Verfahren (wie z. B. Hologrammen) überhaupt existieren – denn ein Original gibt es nur, wenn der Unterschied von Original und Kopie erstens ein Unterschied ist, der einen Unterschied macht, und zweitens, wenn dieser Unterschied irgendwie feststellbar ist. Das bedeutet, dass durch den Fotokopierer oder die digitalen Medien (oder sonst irgendwie) keineswegs ein Zeitalter der Simulation angebrochen ist, in dem der Unterschied von Original und Kopie verschwindet.[49]

Notification

This research was supported in the framework of TÁMOP 4.2.4. A/2-11-1-2012-0001 »National Excellence Program – Elaborating and operating an inland student and researcher personal support system« key project. The project was subsidized by the European Union and co-financed by the European Social Fund.

(31. 03. 2015). Es gibt also nicht nur Original und Kopie, sondern mindestens noch die beglaubigte Kopie als Form dazwischen.

48 Vgl. Martin Senftleben: The Answer to the Machine Revisited. Kopierschutz aus juristischer Sicht, in: Jens Schröter u. a. (Hg.): Kulturen des Kopierschutzes I, Navigationen. Zeitschrift für Medien- und Kulturwissenschaften 10/1 (2010), S. 81–94.

49 Anders sieht dies, mit einem expliziten Bezug auf den Fotokopierer, Wolfgang Ernst: (In)Differenz. Zur Ektase der Originalität im Zeitalter der Fotokopie, in: Hans-Ulrich Gumbrecht, Karl Ludwig Pfeiffer (Hg.): Materialität der Kommunikation, Frankfurt am Main 1988, S. 498–518, insbesondere S. 508 und 512: »[D]enn längst verwischt das Xerox-Verfahren […] die Differenz zwischen Differenz und Nicht-Differenz von Original und Kopie.«