Digitale Unterschrift

Ina Bolinski, Felix Rissel

Die erste Meldung zu COVID-19 im Nachrichten-Archiv auf der Website der Ruhr-Universität Bochum (RUB) datiert auf den 31. Januar 2020 und berichtet von der Ausrufung eines internationalen Gesundheitsnotstands durch die Weltgesundheitsorganisation (WHO) (vgl. Ruhr-Universität Bochum 2020). Am 15. März 2020 informierte die RUB ihre Studierenden und Beschäftigten darüber, dass der Campus bis auf einen Notfallmodus den Betrieb vollständig einstellt. Ab diesem Zeitpunkt und ohne nennenswerte Vorbereitungszeit arbeiteten die Mitglieder der RUB dezentral im jeweils eigenen Homeoffice. Diese Situation stellte eine besondere Herausforderung für eine Verwaltung dar, die bis dato primär mit ausgedruckten Formularen und analogen Unterschriften arbeitete. Die Signatur wurde dabei handschriftlich mit einem Stift auf Papier durch die unterzeichnende Person aufgebracht – eine Praxis, die die körperliche Präsenz des Menschen und die materielle Präsenz des Dokumentes erforderte. Dieses Verfahren, tief in unserer Kultur verwurzelt, verleiht der Signatur einen zentralen Stellenwert, indem sie eine Urszene der Autorisierung darstellt, die durch ihre Symbolkraft und die Performanz des Unterschreibens geprägt ist – eine Handlung, die über das bloße Schreiben hinausgeht, da sie im Akt des eigenhändigen Setzens die Präsenz der unterzeichnenden Person markiert und deren Anwesenheit situativ bezeugt (vgl. Richter 2024; vgl. Derrida 1972). Die COVID-19-Pandemie, in der der Umgang mit Distanz plötzlich zentral wurde, hat in vielen deutschen Universitäten nicht nur die Notwendigkeit zur Beschleunigung der digitalen Transformation in den Verwaltungsstrukturen sichtbar gemacht, auf Schwachstellen in den Arbeitsprozessen hingewiesen und den verstärkten Einsatz digitaler Lösungen (weiter) forciert.[1] Auch die digitale Unterschrift rückte damit als effiziente, kontaktlose Möglichkeit zur Dokumentenunterzeichnung in den Fokus.

An der RUB gehören zu den häufigsten Unterschriften, die von unterschriftsberechtigten Personen geleistet werden, jene auf Kontierungsbögen für die Buchhaltung sowie

1 »Kürzlich wurde etwas ernüchternd festgestellt, dass die Improvisation in der Krisensituation der Coronapandemie zuweilen mehr als kluge Strategien und ausgefeilte Planungsmethoden bei der Digitalisierung der Verwaltung bewirken konnte« (Andermatt 2022, zitiert nach: Guckelberger 2023).

auf Vertragsangelegenheiten. Auch während der Pandemie mussten Rechnungen gezahlt und Verträge geschlossen werden. Daher wurde vielfach die Post zum Verschicken der Dokumente bemüht, was für die Mitarbeiter*innen bedeutete, einen Teil der Arbeitszeit in Warteschlangen vor einer Postfiliale anzustehen. Parallel entstand die durch eine Sonderregelung ermöglichte Praxis, Dokumente digital einzusenden.[2] Diese erlaubte es den Verwaltungsmitarbeiter*innen, die digitalen Dokumente mit Bilddateien von eingescannten Unterschriften zu versehen und sie dann an eine zentrale E-Mail-Adresse zu senden. Dies war allerdings nur dann möglich, wenn die zeichnungsberechtigte Person in einer separaten E-Mail die Zustimmung zur Verwendung der digitalisierten Unterschrift gab und den zweckgebundenen Einsatz bestätigte. Mit der Aufhebung der sogenannten Coronaregelungen zum Februar 2023 wurde diese Sonderregelung wieder außer Kraft gesetzt und Rechnungen und Kontierungen werden seitdem erneut in Papierform verarbeitet. Gleichzeitig wurde deutlich, dass es an einer nachhaltigen, digitalen Lösung für interne Verwaltungsprozesse fehlte. Um diesem Bedarf gerecht zu werden, führte die RUB im April 2024 *RUBSign* ein, eine elektronische Unterschrift, die speziell für den hausinternen Gebrauch entwickelt wurde. Diese Signaturart erzeugt eine zusätzliche Dokumentenseite mit einer digitalen Unterschriftengrafik (Grafiksignet), ist damit jedoch für ein geschäftliches Außenverhältnis nicht vorgesehen.

Die eIDAS-Verordnung (Electronic Identification, Authentication and Trust Services) (vgl. Amtsblatt der Europäischen Union 2014) bildet seit dem 1. Juli 2016 die rechtliche Grundlage für digitale Unterschriften in der EU und unterscheidet drei Arten: Die *einfache elektronische Signatur* umfasst elektronische Daten wie eingescannte Unterschriften oder E-Mail-Signaturen, bietet jedoch nur ein geringes Sicherheitsniveau und ist für rechtlich relevante Dokumente oft unzureichend. Die *fortgeschrittene elektronische Signatur* muss eindeutig der unterzeichnenden Person zugeordnet sein, deren Identität verifiziert werden kann, und nachträgliche Änderungen am Dokument müssen erkennbar sein. Die *qualifizierte elektronische Signatur* erfordert ein qualifiziertes Zertifikat und eine sichere Signaturerstellungseinheit, bietet höchste Sicherheit und ist in Deutschland der handschriftlichen Unterschrift gleichgestellt, wodurch sie für alle rechtlich bindenden Dokumente zugelassen ist.

Die qualifizierte elektronische Signatur, die nun und im Folgenden als »digitale Unterschrift« bezeichnet wird, ist ein technisch anspruchsvoller Prozess, der Aspekte von Virtualität aufweist. Er bezieht sich auf Vertrauensketten und basiert auf einer hierarchischen Struktur. Diese Abhängigkeitsbeziehungen beginnen bei vertrauenswürdigen Zertifizierungsstellen (wie in Deutschland etwa bei der Deutschen Telekom), die sogenannte Wurzelzertifikate (root certificates) ausstellen (vgl. Busch 1998). Von diesen Wurzelzertifikaten ausgehend wird die Zertifikatskette gebildet, die die Vertrauenswürdigkeit des gesamten Systems strukturiert und absichert, um zu den Zertifikaten der jeweiligen Organisationen zu führen. Während die technische Umsetzung digitaler Unter-

2 »Ich bin Professorin an der Uni. Die Finanzierung von Forschungsprojekten mit ihrem Personal muss sichergestellt sein. Deshalb muss ich auch weiterhin Dokumente unterschreiben wie Finanzberichte und Mittelanforderungen. Aber Homeoffice ist nicht Uni. […] Hier drucke ich aus, unterschreibe, fotografiere ich das Dokument, stecke es in einen Briefumschlag und suche eine Briefmarke« (Nana 2020).

schriften in verschiedenen Systemen grundsätzlich ähnlich funktioniert, können sich diese Systeme in ihren spezifischen hierarchischen Vertrauensstrukturen unterscheiden. So kann jedes System eigene Wurzelzertifikate und davon entstehende Vertrauensbäume verwenden, wobei die Kette stets bei der Wurzelzertifizierungsstelle beginnt und über nachgeordnete Instanzen zu den Zertifikaten der jeweiligen Organisationen führt (vgl. BMBF 2020).

Das zugrundeliegende Prinzip der asymmetrischen Kryptografie funktioniert ähnlich wie die gängige Email-Verschlüsselung PGP (Pretty Good Privacy): Zur Signierung eines Dokuments generiert eine Software zunächst eine Prüfziffer, die die Integrität des Dokuments sicherstellt. Diese Prüfziffer wird anschließend mit dem privaten Schlüssel (private key), der der signierenden Instanz zugeordnet ist, verschlüsselt, um sie dann zusammen mit dem Dokument zu versenden. Die empfangende Instanz nutzt dann den öffentlichen Schlüssel der signierenden Instanz, um die Prüfziffer zu entschlüsseln und so die ursprüngliche, bei der Signaturerstellung erzeugte Prüfziffer im Klartext zu erhalten. Zur Integritätsprüfung generiert die empfangende Instanz nun ebenfalls eine Prüfziffer aus dem erhaltenen Dokument. Stimmen die beiden Prüfziffern überein, ist die Integrität des Dokuments gewährleistet und die digitale Unterschrift als gültig anerkannt. Der öffentliche Schlüssel dient dabei ausschließlich zur Entschlüsselung der Signatur, während der private Schlüssel – als notwendiges Mittel zur Signaturerstellung – unerlässlich für die Wahrung der Authentizität des Prozesses bleibt.

In diesem Zusammenspiel von öffentlichen und privaten Schlüsseln, von Prüfziffern und Zertifikaten, wird Vertrauen nicht mehr – wie bei der handschriftlichen Unterschrift – direkt durch die unterzeichnenden und beglaubigenden Personen geschaffen, sondern entsteht durch das komplexe Zusammenspiel technischer Akteure, die die Integrität und Vertrauenswürdigkeit der Signatur sicherstellen (vgl. Manz 2024).

Vertrauen ist als eine zutiefst soziale Kategorie auf menschliche Beziehung und symbolische Interaktion angewiesen. Niklas Luhmann beschreibt Vertrauen als eine grundlegende Voraussetzung für die Reduktion sozialer Komplexität: Es erlaubt uns, Entscheidungen in unsicheren Situationen zu treffen und damit der Ungewissheit künftiger Handlungen anderer zu begegnen (vgl. Luhmann 1989). Dieses Verständnis von Vertrauen wird bei der Verwendung von digitalen Unterschriften neu verhandelt, da hier technische Akteure – wie Algorithmen, Zertifikatsketten und Verschlüsselungsprotokolle – eine zentrale Rolle in der Vertrauensbildung übernehmen. Im Rahmen digitaler Unterschriften wird der Prozess der Vertrauensbildung auf technische Instanzen verlagert, die keine emotionalen oder moralischen Eigenschaften besitzen, sondern ihre Vertrauenswürdigkeit durch kryptografische Protokolle und hierarchische Zertifizierungsstellen gewinnen. Vertrauen wird in diesem Modell nicht als exklusive Eigenschaft menschlicher Interaktion gesehen, sondern als eine Qualität, die im Zusammenspiel von Technologien und Menschen entsteht, wenn die beteiligten technischen Komponenten als stabil und funktional wahrgenommen werden (vgl. zu nichtmenschlichen Akteuren, die an der Vertrauensbildung beteiligt sein können Latour 2010). Die technische Vertrauenskette basiert somit nicht auf einer direkten (auch körperlichen) Bindung an die*den Unterzeichner*in, sondern auf vermitteltem Vertrauen, dessen Legitimation durch Wurzelzertifikate und mathematische Verfahren gewährleistet wird. Während die traditionelle Unterschrift als physische Spur die körperliche Anwesenheit

und Absicht der unterzeichnenden Person symbolisiert, wird die digitale Unterschrift zu einer Signatur, bei der Vertrauen durch ein System digitaler Autorisierungen statt durch menschliche Interaktion entsteht.

Diese Transformation des Vertrauensbegriffs zeigt, wie Vertrauen zunehmend technisch abgesichert wird. Zudem lässt sich konstatieren, dass besonders bürokratische Prozesse und die damit verbundenen Dokumentationspraktiken zu einer Entfremdung und Entpersönlichung durch standardisierte Verfahren führen, wenn an die Stelle des direkten, zwischenmenschlichen Vertrauens funktionale Eigenschaften des Systems etabliert werden (vgl. Kafka 2012).[3] Die beschriebenen Prozesse ersetzen menschliche Intuitionen und den sozialen Charakter von Vertrauen durch technische Instanzen, deren reibungsloses Funktionieren die Grundlage für die Gültigkeit digitaler Unterschriften bildet.

Als paradigmatisches Beispiel für die Virtualität und Abstraktion moderner Signifikationsprozesse repräsentiert die digitale Unterschrift mehr als nur einen einzelnen Schritt in der Digitalisierung von Verwaltungsvorgängen: Sie steht für die Transformation, die durch veränderte körperlich-materielle Akte zugunsten immaterieller-kryptografischer Prozesse im gesamten bürokratischen und administrativen Bereich stattfindet. Und sie unterscheidet sich von der traditionellen, handschriftlichen Signatur, die unmittelbar sicht- und greifbar bleibt und über einen materiellen Eigenwert verfügt, die die unterzeichnende Person mit dem Dokument verbindet. Die digitale Unterschrift ist ein Index, der technisch generiert ist und auf abstrakte Weise die Authentizität und Integrität des Dokumentes markiert, ohne dabei eine visuell erkennbare Spur zu hinterlassen (vgl. Sanders 1983; Krämer/Kogge/Grube 2007). In der Signatur als digitalem Code manifestiert sich eine Form der vermittelten Präsenz, die über algorithmische Prozesse hergestellt wird. Mit dem Verweis auf den Status des Digitalen – als eine von der materiellen Welt losgelöste, aber dennoch operativ wirkmächtige Dimension – entwickelt sich eine eigene Logik der Repräsentation und Verifikation. Das virtuelle Moment der digitalen Unterschrift zeigt sich insbesondere in der Loslösung von Körper und Materialität, die traditionell mit dem Akt der Unterschrift mit Stift und Papier verbunden sind. Diese materielle Präsenz fehlt der digitalen Unterschrift, die stattdessen in einem rein immateriellen Raum existiert. Ihre Existenz wird an zwei Punkten möglich: dem Prozess der Verschlüsselung und dem der Entschlüsselung. Das Virtuelle dieser Unterschrift ist daher nicht nur eine Abstraktion im physischen Raum, sondern vielmehr ein Zustand der Koexistenz von Daten, die erst in der richtigen Reihenfolge und durch eine technische Entschlüsselung zu einer funktionalen Authentizität führen.

Die digitale Unterschrift, so wenig interessant sie auf den ersten Blick scheinen mag, ist innerhalb der Virtuellen Universität ein eindrückliches Beispiel für die gleichzeitige Entmaterialisierung und Virtualisierung bürokratischer Verwaltungsakte. Sie verdeutlicht darüber hinaus, dass virtuelle Objekte im digitalen Raum zwar von Kategorien wie z.B. Sicht- und Greifbarkeit losgelöst, dennoch aber an Handlungen rückgebunden sind

3 Kafka zeigt, dass in der modernen Bürokratie das Vertrauen, das auf persönlicher Interaktion basierte, zunehmend auf die »Macht des Papiers« verlagert wurde, wobei schriftliche Dokumente und bürokratische Strukturen als Garant für Ordnung und Verlässlichkeit dienen.

und Eigenschaften funktionaler Konstitution aufweisen. Anders als bei anderen virtuellen Phänomenen, die mit Begriffen wie Abbildungen oder Simulationen der Realität verbunden werden, ist die digitale Unterschrift eine virtuelle Realität der Authentizität, die im Moment ihrer Ver- und Entschlüsselung existiert und nur durch die Aktivierung des kryptographischen Apparats ihre Existenz als »echte« Unterschrift entfaltet. Sie ist damit in ihrer Beglaubigungsleistung und Täuschungsunanfälligkeit der echten Unterschrift auf eine gewisse Weise überlegen, sie ist daher sowohl eine Repräsentation von Identität als auch eine eigenständige, technologisch erzeugte Präsenz, die in einer nichtmateriellen Dimension zur Geltung kommt. Als solche ist die digitale Unterschrift mehr medial vermittelter Prozess als stabiles Objekt: sie entsteht und vollzieht sich im Moment der Überprüfung und Verifikation durch spezifische kryptografische Verfahren. In diesem Zusammenhang wird das Virtuelle nicht als bloße Abstraktion oder als Abwesenheit von Materialität und sozialem Handeln verstanden, sondern als Bedingung für ein Setting, in dem Authentizität erst durch die technologische Vermittlung von Verschlüsselung und Entschlüsselung erzeugt wird. Mit der digitalen Unterschrift wird das Virtuelle zu einer neuen Praktik der Annäherung und vertrauensbildendenden Authentizitätsherstellung.

Literatur

Amtsblatt der Europäischen Union (2014): Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, L 257, 28. August 2014, S. 73–114.

Andermatt, Kevin C. (2022): »Kritik der Digitalen Verwaltung: Von Mythen, Medien und Mimesis«, in: Lyn Ellen Pleger/Alexander Mertes (Hg.), Digitale Transformation der öffentlichen Verwaltung in der Schweiz, Wiesbaden: Springer Gabler, S. 89–118. https://doi.org/10.1007/978-3-658-36591-2_5.

BMBF (Hg.) (2020): Leitlinie für digitale Signatur-/Siegel-, Zeitstempelformate sowie technische Beweisdaten (Evidence Record), in: bsi.bund.de (26.03.2020). Online unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Leitlinie_fuer_digitale_Signatur-Siegel-Zeitstempelformate.pdf (letzter Zugriff: 27.11.2024).

Busch, Carsten (1998): »Zur Bedeutung von Metaphern in der Entwicklung der Informatik«, in: Dirk Siefkes et al. (Hg.), Sozialgeschichte der Informatik. Studien zur Wissenschafts- und Technikforschung, Wiesbaden: Deutscher Universitätsverlag, S. 69–83. https://doi.org/10.1007/978-3-663-08954-4_5.

Derrida, Jacques (1972): »Signatur Ereignis Kontext«, in: Ders. (1988), Randgänge der Philosophie, Wien: Passagen-Verlag, S. 291–314.

Guckelberger, Annette (2023): »Entwicklung und aktuelle Leitbilder der Verwaltungsdigitalisierung in Deutschland«, in: Natalia Kohtamäki/Enrico Peuker (Hg.), Die Digitalisierung der öffentlichen Verwaltung. Deutsch-polnische Perspektiven, Tübingen: Mohr Siebeck, S. 3–21.

Kafka, Ben (2012): The Demon of Writing: Powers and Failures of Paperwork, New York: Zone Books. https://doi.org/10.2307/j.ctv14gpj6p.

Krämer, Sybille/Kogge, Werner/Grube, Gernot (Hg.) (2007): Spur: Spurenlesen als Orientierungstechnik und Wissenskunst, Frankfurt a.M.: Suhrkamp.

Latour, Bruno (2010): Eine neue Soziologie für eine neue Gesellschaft: Einführung in die Akteur-Netzwerk-Theorie, Frankfurt a.M.: Suhrkamp.

Luhmann, Niklas (1989): Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität, Stuttgart: Enke.

Manz, Olaf (2024): Digitale Signatur: Unterschreiben mit Hilfe der Algebra, Berlin/Heidelberg: Springer Spektrum. https://doi.org/10.1007/978-3-662-68417-7.

Nana, Lilih (2020): »ich kuvertiere und abends bringe ich meinen Müll raus«, in: coronarchiv.blogs.uni-hamburg.de (04.2020). Online unter: https://www.coronarchiv.de/item?id=556 (letzter Zugriff: 07.09.2024).

Richter, Tilmann (2024): Politiken des Unterschreibens. Universität, Untergrund und Apparat 1949–2017. Dissertationsschrift, Ruhr-Universität Bochum.

Ruhr-Universität Bochum (2020): »Coronavirus. Die RUB genehmigt keine Reisen mehr nach China«, in: news.rub.de (01.2020). Online unter: https://news.rub.de/vermischtes/2020-01-31-coronavirus-die-rub-genehmigt-keine-reisen-mehr-nach-china (letzter Zugriff: 03.12.2024).

Sanders, Charles (1983): Phänomen und Logik der Zeichen. Hg. und übers. von Helmut Pape, Frankfurt a.M.: Suhrkamp.