GESELLSCHAFT
FÜR INFORMATIK

Gunnar Auth, Tim Pidun (Hrsg.)

GI Edition Proceedings Band 341
6. Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023)

26. und 27. Oktober 2023
Dresden, Deutschland

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-341
ISBN 978-3-88579-735-7
ISSN 1617-5468

Volume Editors
Prof. Dr. Gunnar Auth
Hochschule Meissen (FH) und Fortbildungszentrum
Herbert-Böhme-Straße 11, 01662 Meißen
gunnar.auth@hsf.sachsen.de

Prof. Dr. Tim Pidun, MBA
Hochschule für Technik und Wirtschaft Dresden
Friedrich-List-Platz 1, 01069 Dresden
tim.pidun@htw-dresden.de

printed by Köllen Druck+Verlag GmbH, Bonn

Vorwort zur RVI 2023 – Von der E-Government-Vision zum digitalen Verwaltungschaos?

Gunnar Auth [1] und Tim Pidun [2]

Die GI-Fachtagung Rechts- und Verwaltungsinformatik (RVI) 2023 hat den Anspruch, den Dialog zwischen Wissenschaft und Praxis über die digitale Transformation von Staat und Verwaltung durch wissenschaftlich gesicherte Erkenntnisse voranzubringen. Diese Zielsetzung teilen sich auch die beiden beteiligten Disziplinen Rechtsinformatik und Verwaltungsinformatik, verfolgen sie aber aus unterschiedlichen Blickwinkeln. Aufgrund der fachlichen Expertise der Autoren in der Verwaltungsinformatik (VI), konzentrieren wir uns im Folgenden auf einige Zusammenhänge zwischen VI und Verwaltungsdigitalisierung.

Trotz jahrzehntelanger Anstrengung befindet sich die digitale Transformation des öffentlichen Sektors beinahe ebenso lange in einer sich zuspitzenden Krise, deren Auswirkungen mittlerweile sowohl das Vertrauen der Bürgerinnen und Bürger in die Handlungsfähigkeit des Staats als auch die Wettbewerbsfähigkeit der Wirtschaft bedrohen (vgl. [Eu23], [IT22], [Me21]). Der Verlauf dieser Krise, beginnend mit der Umsetzung von seinerzeit noch als E-Government-Vorhaben bezeichneten Initiativen, ist gekennzeichnet durch zahlreiche gescheiterte oder extrem verzögerte und verteuerte Vorhaben wie etwa der Kommunikationsdienst De-Mail [Kr21], die seit 2015 laufende IT-Konsolidierung des Bundes [Bu22] oder der gesetzlich bis Ende 2022 verordnete Onlinezugang zu allen Verwaltungsleistungen [Re23].

In enger Anlehnung an die Mutterdisziplin Wirtschaftsinformatik (vgl. [Di19, HHR07, Re11]) untersucht die VI als zentralen Gegenstand Informationssysteme der öffentlichen Verwaltung, die Informationen speichern, verarbeiten und bereitstellen, um die Ausführung von Verwaltungs- und Regierungsaufgaben zu unterstützen. Verwaltungsinformationssysteme (VIS) lassen sich in die Kernkomponenten Mensch, Aufgabe und Technik gliedern und werden daher auch als sozio-technische Systeme charakterisiert. Innerhalb des VIS wird der automatisierte Teil der Aufgaben inklusive der dazu erforderlichen Softwarekomponenten und Daten als Anwendungssystem bezeichnet, in der Verwaltungspraxis häufig auch Fachanwendung genannt [Le16]. Das hier nur grob skizzierte VIS-Modell liefert der VI einen

[1] Hochschule Meißen (FH) und Fortbildungszentrum, Fachbereich Digitale Verwaltung, Herbert-Böhme-Str. 11, 01662 Meißen, Deutschland, gunnar.auth@hsf-meissen.de, https://orcid.org/0000-0002-3013-2739
[2] Hochschule für Technik und Wirtschaft Dresden, Friedrich-List-Platz 1, 01069 Dresden, Deutschland, tim.pidun@htw-dresden.de, https://orcid.org/0000-0003-1331-1732

doi:10.18420/rvi2023-999

Bezugsrahmen, in dem Digitalisierungsphänomene, -methoden und -artefakte ganzheitlich unter Berücksichtigung von Mensch, Aufgabe und Technik betrachtet werden. Bei der Gestaltung und Realisierung praktischer Lösungen lässt sich dadurch eine nicht selten zu beobachtende einseitige Auslegung von Digitalisierungsvorhaben als IT-Projekte genauso vermeiden, wie die ebenfalls problematische simple Umkehr in Digitalisierung als Organisationsprojekt. In beiden Fällen handelt es sich um verengte Perspektiven, die Komplexität durch Verkürzung ausblenden, statt diese durch geeignete Bewältigungsansätze zu adressieren. Bei der theoretischen Betrachtung von Informations- und Anwendungssystemen hat sich seit geraumer Zeit allgemein eine ganzheitliche Lebenszyklusperspektive etabliert, die neben der Konzeption und Entwicklung solcher Systeme auch die Phasen Betrieb, Weiterentwicklung und schließlich Außerbetriebnahme berücksichtigt [HRS14]. Auf diesem Grundverständnis fußen moderne Konzepte für Entwicklung und Management digitaler Lösungen, die Produkt-, Nutzer-, Service- und Innovationsorientierung betonen [AAK21]. Erst dadurch gelingt es führenden Unternehmen, die Potenziale digitaler Technologien in einem herausfordernden Umfeld zu erschließen. Im Kern lässt sich bei all diesen Konzepten das Streben nach kontinuierlicher Verbesserung ausmachen, wie es auch im Geschäftsprozessmanagement aus organisatorischer Perspektive verankert ist.

Verbesserung erfordert Veränderung und damit Abkehr von der Bewahrung des Status quo. Zur Bewältigung neuartiger Herausforderungen werden neue Herangehensweisen und Lösungen benötigt. Die VI als Wissenschaftsdisziplin erforscht auf wissenschaftlicher und interdisziplinärer Basis neue Problemlösungen und Methoden für die Verwaltungsdigitalisierung und bietet für diese ein bislang bei weitem nicht ausgeschöpftes Potenzial. Mit der Einrichtung von neuen VI-Studiengängen an Hochschulen des öffentlichen Diensts (HöD) und Hochschulen für angewandte Wissenschaften (HAW) in nahezu allen Bundesländern sowie an der Hochschule des Bundes während der letzten Jahre verfolgen die Hochschulträger insbesondere das Ziel, dringend erforderliche Nachwuchskräfte mit den für die Digitalisierung der Verwaltung erforderlichen Kompetenzen akademisch auszubilden. Insbesondere an HöD wird von den Hochschulträgern Forschung und Transfer gegenüber der Lehrverpflichtung vergleichsweise geringe Bedeutung zugemessen, was sich in hohen Lehrdeputaten, komprimierten Studienabläufen mit sehr wenig vorlesungsfreien Zeiten und mangelnden strukturellen Rahmenbedingungen für Forschung und Transfer niederschlägt [El22]. Dagegen wird großer Wert auf den Praxisbezug des Studiums gelegt, um die Absolventinnen und Absolventen möglichst passgenau auf den Berufseinstieg in die vorherrschende Verwaltungspraxis vorzubereiten und somit die immer drängendere Nachfrage der Verwaltung nach qualifiziertem Nachwuchs möglichst kurzfristig zu befriedigen. Wenngleich diese Ausrichtung der Studiengänge aus Sicht der Einstellungsbehörden durchaus nachvollziehbar ist, führt sie nicht zwangsläufig zu Nachwuchskräften, die als Agents of Change mit besonders ausgeprägter, wissenschaftlich fundierter Transformations- und Innovationskompetenz die Verwaltungsdigitalisierung vorantreiben.

Dabei konstatieren Christ et al. [CAB22] in ihrer Untersuchung über digitale Kompetenzen in der öffentlichen Verwaltung in Deutschland sogar eine doppelte Kompetenzlücke. Einerseits fokussieren die in Stellenanzeigen nachgefragten Kompetenzen primär auf technische Kenntnisse und Fähigkeiten, betonen also die Einführung der Digitalisierung in der

Verwaltung und den Umgang mit entsprechender Technik (E-Kompetenzen), andererseits fehlen eher nach innen gerichtete Innovations-, Kollaborations- und Agilitätskompetenzen, die den Digitalisierungsgedanken und das entsprechende Denken in der Verwaltung befördern (Digitale Kompetenzen). Diese Betrachtung des Bedarfs der Abnehmerseite wird auch durch die Erkenntnisse einer Untersuchung der vermittelten Kompetenzen der einschlägigen Hochschulen auf der Angebotsseite ergänzt [Pi23]: Derzeit dominiert demnach in der Verwaltungsinformatik eine dienstherrenbezogene Ausbildung, die eher auf die Vermittlung der notwendigen Kompetenzen in der landesspezifischen öffentlichen Verwaltung fokussiert und die o.a. Kompetenzen eher nachrangig vermittelt. Dagegen gibt es einige wenige informatikorientierte Angebote, die zwar die Vermittlung technischer Kompetenzen betonen, dabei aber in der Regel auch immer dienstherrenorientiert bleiben. Die Autoren empfehlen daher, je nach Einsatzbereich der Absolventen genau zwischen verwaltungswissenschaftlich- und informatikorientierten Ausbildungen zu unterscheiden.

Neben den Einrichtungen der unmittelbaren Staatsverwaltung gibt es allerdings auch sehr viele Organisationen, die keine Behörden sind, beispielsweise Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Diese gehören üblicherweise zwar nicht zum Adressatenkreis der dienstherrenorientierten Hochschulen, sind allerdings auch dringend auf gut ausgebildetes Fachpersonal angewiesen. Legen wir außerdem die Definition nach Kaack [Ka90, S. 140] zugrunde, bei der die Verwaltungsinformatik die „Wissenschaft der informationstechnikgestützten Gestaltung von Verwaltungshandeln“ ist, greift die Beschränkung auf den öffentlichen Dienst insgesamt zu kurz und eröffnet damit die Einsatzmöglichkeit der Verwaltungsinformatiker auch in privaten Unternehmen, die als Dienstleister für öffentliche Auftraggeber arbeiten, beispielsweise Beratungs- oder Softwarefirmen. Darüber hinaus betrifft das auch jedes private Unternehmen, in dem gesetzlich vorgeschriebene, verwalterische Aufgaben durchgeführt werden müssen, beispielsweise durch die Einführung eines Whistleblowing-Managementsystems, eines Systems zur Überwachung der Lieferketten-Compliance oder einer Online-Zeiterfassung. Damit erweitert sich der Einsatzbereich eines Verwaltungsinformatikers auf praktisch jede Organisation, in der Verwaltungshandeln automatisiert werden muss, sei es zum Nutzen einer privatrechtlichen oder einer öffentlich-rechtlichen Institution.

Darüber hinaus erkennen Koddebusch et al. [Ko22] generell einen zunehmenden, massiven Bedarf an Aus- und Weiterbildung in der öffentlichen Verwaltung, insbesondere da die derzeitigen Angebote nicht ausreichen, um die Anforderungen an die technologiebezogenen Kompetenzentwicklung im öffentlichen Sektor insgesamt abzudecken. Das Beispiel des Freistaats Sachsen bestätigt diese Erkenntnis: 2023 besteht dort eine Unterdeckung von ca. 50% des Bedarfs an Absolventen des Bachelorstudiums Digitale Verwaltung [Be23]. Dabei teilen das Land und die Kommunen sich die Ausbildungsplätze hälftig [Sä20], so dass wir von mindestens dem gleichen unterdeckten Verhältnis auch für die sächsischen Kommunen ausgehen müssen, und in den meisten anderen Bundesländern dürfte die Lage ähnlich angespannt sein. Die Hochschulabsolventen werden dabei regelmäßig im gehobenen Dienst im Rahmen von Neueinstellungen eingesetzt, allerdings besteht auch für alle diejenigen Beschäftigten, die bereits in den Verwaltungen tätig sind, ein Bedarf an Weiterbildung, um die Herausforderungen der Digitalisierung zu meistern. Diese Mitarbeitergruppe ist dabei durch einen hohen Anteil an nicht-digital-affinen Personen im mittleren bis höheren Alterssegment

gekennzeichnet. Neben der Vermittlung von technischen Kompetenzen sind hierbei auch die Berücksichtigung ihrer kognitiven und sozio-emotionalen Fähigkeiten besondere Herausforderungen [Kr23].

Insgesamt muss also die Ausbildung in der Verwaltung breiter aufgestellt werden – die Informatik-Fakultäten sollten mehr Angebot an speziellem Domänenwissen einerseits und interdisziplinärem Methodenwissen andererseits zur öffentlichen Verwaltung anbieten, damit der Einsatzbereich der Verwaltungsinformatik sich nicht nur auf den öffentlichen Dienst direkt beschränkt, sondern alle die Arbeitgeber adressiert werden, die etwas mit öffentlicher Verwaltung oder dem Verwalten als Dienstleistung zu tun haben. Hierzu gibt es bereits sich ergänzende Angebote aus verwaltungswissenschaftlichen und Informatikstudiengängen [Pi23]. Des Weiteren sollten auch Aus- und Weiterbildungen der Verwaltungsinformatik angeboten werden, die die derzeit schon im Beruf Stehenden adressieren, und die im Rahmen eines regulären Studiums nicht absolviert werden können. Fortbildungen und Zertifikate, die Teilaspekte anbieten und direkte Probleme in Verständnis und Ausführung lösen, sind hier die Formate und Inhalte der Wahl. Dies dient der direkten Befähigung von schon im Beruf stehenden Funktionsträgern.

Schließlich müssen auch an HöD und HAW Rahmenbedingungen geschaffen werden, die das Erschließen der Potenziale anwendungsorientierter Forschung und zielgerichteten Transfers von Forschungsergebnissen in Studieninhalte und Verwaltungspraxis befördern.

Dass theoretische Problemlösungen oftmals vorhanden sind und die praktische Umsetzung erfolgreich gelingen kann, zeigt das Programm der RVI, für das in einem doppel-blinden Begutachtungsverfahren von insgesamt 21 wissenschaftlichen Einreichungen zehn für die Präsentation im Scientific Track angenommen wurden, was einer Annahmequote von 48% entspricht. Unter den angenommenen Arbeiten bildet Künstliche Intelligenz einen wenig überraschenden Themenschwerpunkt, ergänzt durch ein breites Spektrum an Beiträgen zu Konzepten und Modellen der Rechts- und Verwaltungsinformatik. Auf deren praktische Anwendung fokussiert der Professional Track. Abgerundet wird das Programm durch studentische Beiträge, eine Poster Session und mehrere Workshops, in denen Inhalte von Wissenschaftlern und Praktikern im direkten Dialog erarbeitet werden.

Literaturverzeichnis

[AAK21] Alt, R.; Auth, G.; Kögler, C.: Continuous Innovation with DevOps. Springer, Cham, 2021.

[Be23] Bettina Holtz-Nebel: Übernahmemanagement Sachsen. Persönliche Mitteilung per E-Mail, 2023.

[Bu22] IT-Konsolidierung des Bundes. Bericht nach § 88 Absatz 2 BHO an den Haushaltsausschuss des Deutschen Bundestages. Zielerreichung. Bonn, 2022.

[CAB22] Christ, J.; Auth, G.; Bensberg, F.: Die doppelte Kompetenzlücke – Eine empirische Analyse digitaler Kompetenzanforderungen in Stellenanzeigen der öffentlichen Verwaltung in Deutschland. In (Richenhagen, G.; Dick, M. Hrsg.): Public Management im Wandel. Springer, Wiesbaden, S. 75–98, 2022.

[Di19] Disterer, G.: Was ist Verwaltungsinformatik? In (Schmid, A. Hrsg.): Verwaltung, eGovernment und Digitalisierung. Springer, Wiesbaden, S. 41–51, 2019.

[El22] Elbel, T.: Kann man Hochschullehrer überlasten? Rechtliche Parameter der Festlegung der professoralen Lehrverpflichtung an staatlichen Hochschulen für angewandte Wissenschaften. Zeitschrift für Beamtenrecht 1+2/70, S. 12–18, 2022.

[Eu23] Europäische Kommission: Digital Decade Country Report 2023: Germany. https://ec.europa.eu/newsroom/dae/redirection/document/98643, Stand: 30.09.2023.

[HHR07] Heinrich, L. J.; Heinzl, A.; Roithmayr, F.: Wirtschaftsinformatik. Einführung und Grundlegung. Oldenbourg, München, Wien, 2007.

[HRS14] Heinrich, L. J.; Riedl, R.; Stelzer, D.: Informationsmanagement. Grundlagen, Aufgaben, Methoden. De Gruyter Oldenbourg, Berlin, 2014.

[IT22] Initiative D21; TU München: eGovernment MONITOR 2022. https://initiatived21.de/uploads/03_Studien-Publikationen/eGovernment-MONITOR/2022/egovernment_monitor_22.pdf, Stand: 26.09.2023.

[Ko22] Koddebusch, M. et al.: The Increasing e-Competence Gap: Developments over the Past Five Years in the German Public Sector. In (Fui-Hoon Nah, F.; Siau, K. Hrsg.): HCI in Business, Government and Organizations. Springer, Cham, S. 73–86, 2022.

[Kr23] Krause, T. A.: Digital Literacy in der öffentlichen Verwaltung. In (Krause, T. A.; Schachtner, C.; Thapa, B. Hrsg.): Handbuch Digitalisierung der Verwaltung. transcript Verlag; UTB, Bielefeld, S. 13–32, 2023.

[Kr21] Krempl, S.: "Ziele gänzlich verfehlt": Bundesrechnungshof rügt De-Mail-Fiasko. https://www.heise.de/news/Ziele-gaenzlich-verfehlt-Bundesrechnungshof-ruegt-De-Mail-Fiasko-6281540.html, Stand: 24.09.2023.

[Le16] Leps, O.: Nutzung und Akzeptanz von E-Government-Fachanwendungen in der öffentlichen Verwaltung. Eine empirische Analyse am Beispiel des europäischen Binnenmarkt-Informationssystems. Logos Verlag Berlin, Berlin, 2016.

[Me21] Mertens, P.: Ist Deutschland wirklich ein „digitales Entwicklungsland“ – kann die Institutioneninflation helfen? Wirtschaftsinformatik & Management 3/13, S. 194–205, 2021.

[Pi23] Pidun, T. et al.: (K)ein funktionierender Markt? Nachfrage und Angebot für das Studium der Verwaltungsinformatik. In (Gesellschaft für Informatik Hrsg.): Proceedings Informatik Festival 2023, 2023 (in Erscheinung).

[Re23] Reimer, H.: OZG – Gesetzgebung in Not. Datenschutz und Datensicherheit – DuD 4/47, S. 201, 2023.

[Ka90] Kaack, H.: Verwaltungsinformatik als anwendungsspezifische Informatik. In: Reuter, A. (Hrsg).: GI — 20. Jahrestagung II. Springer, Berlin, Heidelberg, S. 133-145, 1990.

[Re11] Reinermann, H.: Verwaltungsinformatik - auch eine Wirtschaftsinformatik! In (Heinrich, L. J. Hrsg.): Geschichte der Wirtschaftsinformatik. Springer, Berlin, Heidelberg, S. 131–145, 2011.

[Sä20]: Sächsisches Amtsblatt Nr. 42/2020, Sächsische Staatskanzlei, S. 1174, 2020.

Sponsoren

Wir danken den folgenden Unternehmen und Institutionen herzlich für die Unterstützung der Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023).

PD
Berater der öffentlichen Hand GmbH

dataport kommunal

Lecos GmbH

Procilon GmbH

Gesellschaft für
Wissensmanagement e.V.

GISA GmbH

IMTB Group GmbH

Tagungsleitung

Gesamtleitung:

Gunnar Auth,
Hochschule Meißen (FH) und Fortbildungszentrum

Tim Pidun,
Hochschule für Technik und Wirtschaft Dresden

Programmkomitee

Rainer Alt	Universität Leipzig
Jürgen Anke	Hochschule für Technik und Wirtschaft Dresden
Tobias Brandt	Universität Münster
Michael Breidung	Landeshauptstadt Dresden
Bettina Distel	Universität Münster
Wolfgang Eixelsberger	Fachhochschule Kärnten
Torsten Eymann	Universität Bayreuth
Benjamin Fabian	Technische Hochschule Wildau
Peter Fettke	DFKI und Universität des Saarlandes
Roland Franke	BearingPoint
Norbert Frick	Hochschule der Deutschen Bundesbank
Steffen Gilge	Sächsische Staatskanzlei
Stefan Handke	Hochschule für Technik und Wirtschaft Dresden
Moreen Heine	Universität zu Lübeck
Markus Helfert	Maynooth University
Holger Hünemohr	Hochschule RheinMain
Oliver Jokisch	Hochschule Meißen (FH) und Fortbildungszentrum
Achim Kempe	Robotron Datenbank-Software
Ulrich Lohmann	Hochschule des Bundes für öffentliche Verwaltung
Matthias Lohse	Hochschule für Technik und Wirtschaft Dresden
Tobias Mettler	Universität Lausanne
Dagmar Lück-Schneider	Hochschule für Wirtschaft und Recht Berlin
Isabell Peters	Kommunale Hochschule für Verwaltung Niedersachsen
Stephan Raimer	Fachhochschule für Verwaltung und Dienstleistung
Stephan Rein	Technische Hochschule Wildau
Michael Räckers	Universität Münster
Detlef Rätz	Hochschule Meißen (FH) und Fortbildungszentrum
Birgit Schenk	Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg
Marie-Sophie Schönitz	Deloitte
Erich Schweighofer	Universität Wien
Tobias Siebenlist	Hochschule Rhein-Waal

Ingmar Soll	dataport.kommunal
Christoph Sorge	Universität des Saarlandes
Andreas Spichiger	Berner Fachhochschule und Schweizer Bundeskanzlei
Basanta Thapa	Nationales E-Government Kompetenzzentrum
Nils Urbach	Frankfurt University of Applied Sciences und Fraunhofer FIT
Anne-Dore Uthe	Hochschule Harz
Jörn von Lucke	Zeppelin Universität Friedrichshafen
Maria A. Wimmer	Universität Koblenz

Organisationskomitee

Jürgen Anke	Hochschule für Technik und Wirtschaft Dresden
Gunnar Auth	Hochschule Meißen (FH) und Fortbildungszentrum
Stefan Handke	Hochschule für Technik und Wirtschaft Dresden
Oliver Jokisch	Hochschule Meißen (FH) und Fortbildungszentrum
Tim Pidun	Hochschule für Technik und Wirtschaft Dresden
Detlef Rätz	Hochschule Meißen (FH) und Fortbildungszentrum

Inhaltsverzeichnis

Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
14 Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023

Federal Cybersecurity Architecture and Information Security Management

Adoption and Diffusion of the NIS-2 Requirements

Thomas Rehbohm [1] Frank Moses [2]

Abstract: Europe, the federal government, the federal states, municipalities, and their business enterprises are facing the challenges of a hybrid threat situation. At a time when information technology is growing faster than ever before, information cyber security and security management system (ISMS) assessment have become one of the most important aspects of most public sector organisations. The dependency on technology for almost every single process in public sector organisations has put ISMS at the top of the corporate agenda. For public organisations in particular, the NIS 2 Directive describes abstract requirements for the development of an ISMS. At the same time, minimum requirements should be defined that help municipal administration set up an information security management system quickly and easily. This paper summarizes the different requirements and generates a foundation for a rough procedural model, for implementing the upcoming requirements of the NIS 2 Directive quickly and easily in local governments. In particular, the current discussion focuses on securing ICT infrastructures and services of all providers of services of general interest. European and national regulations provide the framework for an appropriate response to this threat to the common good. The federal cybersecurity architecture of a member state such as Germany, presented here, must fit into the European context. Procedures for the implementation of information security management systems complement this theoretical model. This thesis presents a federal cybersecurity model.

Keywords: Security Architecture, Federal Government Institutions

1 Introduction

For a federal state in Germany, the respective member state and the European Union, the availability of important consumer goods and infrastructures is part of public services. The public administration is responsible as a guarantor at all levels of the protection of the

[1] Institute of Computer Science, University of Rostock Germany, Thomas.Rehbohm@uni-rostock.de

[2] Institute of Computer Science, University of Rostock Germany, Frank.Moses@uni-rostock.de

doi:10.18420/rvi2023-006

state, economy, and society [RiBM16, S.261], [WaWe20, S.710]. State institutions must act, since the Federal Republic of Germany and its states are obliged to place human needs, including economic ones, at the centre of their activities [Bund82, S.82–118].

The current threat situation leaves no room for discretion here, information security is endangered and thus higher than ever [Bund22a]. In particular, due to successful attacks on e.g., municipal IT infrastructures or on the IT systems of hospitals, Germany is also called upon to do more for the cooperation of all actors and for a common approach to strengthen resilience.

A functionally effective and federal cybersecurity architecture must be underpinned by the information security management systems of the respective actors. In this context, the strategy and motivation of the state, business and society as well as municipalities are fundamentally comparable, although it is recognized that commercial enterprises serve other stakeholders.

The architectural superstructure is to be produced in consultation with all the federal states and, at best, should be seamlessly embedded in European architecture. According to statements by the Federal Minister of the Interior on the expansion of the German BSI into a central office for cyber security matters, [Bund22b] a third security pillar is to be created along the lines of the Federal Criminal Police Office (BKA) and the Federal Office for the Protection of the Constitution (BfV). The transfer of competencies in the field of cyber security of the states, in favour of the federal government, may require adjustments but are not the focus of this work.

The research object of this thesis relates to an effective interaction of a federal cybersecurity architecture, which is substantiated with information security management systems - regardless of the framework included - according to the CISIS12 process model and adequately takes into account the requirements of the NIS 2 Directive [MoRe22] [Euro23].

In chapter 2 we give an overview of the state of the art. This is followed by chapter “3 Methodology" that describes the phases of the Design Science approach, which are progressed through step by step. Chapter "4 Federal Cybersecurity Architecture” describes the development of the cybersecurity architecture, considering the requirements of the NIS 2 Directive (chapter 5). These results were structured in a further step in order to develop and describe a rough process model based on them. The results will be used to realize an implementation in practice with the help of the CISIS12 process model (section 6). This process model has already been successfully tested in an artificial environment. Currently, the procedure model is being tested in a real environment with different test subjects. The section 7 briefly summarises the result.

The goal of our research is to identify the specifics of public sector organisations and develop an Cyber Security Architecture and ISMS Approach tailored to their demands. The current requirements of the NIS-2 Directive [Rich22] should be considered.

2 State of the art

Research contributions in the context of cyber and information security, combined with topics such as information security management systems, cybersecurity law and cybersecurity architectures, have continued to grow due to the current threat situation and topicality.

European contributions in the field of services of general interest are mainly concerned with internal market law, competition law and, in the context of structural and demographic change, with social, care and health systems. In principle, these are contributions that concern the common good but do not represent the services of general interest related to the ICT structures of a region. State interaction between actors in services of general interest is currently not a research focus; rather, contributions to cybersecurity law are in current discussions [KiBa20] or civil security [GuKW17] in the context of services of general interest. An in-depth literature review is part of the article "Security Management, Cyber Security and Services of General Interest: Empirical Study in German Municipalities" [RKCS22]. The following examples are extracted from this and are intended to illustrate the topic as examples.

The federal system of the United States is comparable to Germany. In "The Cybersecurity Policy Challenge – The Tyranny of Geography," Kamarck recommends that a seamless architecture of collaboration must emerge because, unlike governments, cybersecurity threats are borderless [Andr12].

At the European level, Krajweski's "Services of general interest beyond the single market" states that in the Treaty of Lisbon, the Member States (national, regional and local authorities) of the European Union, among others, have general responsibility for the "provision, commissioning and organisation" of services of general interest [Kraj15].

At the national level, the authors of "Cyber Security in Critical Infrastructures" state that the cooperative approach in the field of cyber security has proven its worth, especially because trusting cooperation between the state and business is a "shared mission" [DüFi18].

3 Methodology

This work is part of a research project aiming at methodical and technological support for cybersecurity architecture and information security management in public sector organisation units. The project follows the paradigm of design science research (DSR) [JoPe14]. DSR is a research paradigm aiming at problem-solving in organizational settings with a focus on developing valid and reliable knowledge for designing the required solutions. DSR research projects typically consist of several phases and require

the use of different research methods depending on the DSR phase and intended design solution.

This paper concerns the phase requirements definition and design and development of the design solution, i.e., the core artefact.

Table 1 provides an overview of the research activities performed in the different phases of the DSR process, the research methods used for these activities, the results achieved and the sections of this paper providing information about the results.

According to the DSR paradigm, the problem investigation must investigate two aspects: the knowledge base and the business relevance. The knowledge base consists in general of the published scientific work in the area under investigation. Using a literature analysis, we identified relevant existing work. The results presented in section 1 confirm that there is no tailored approach in science for a Cyber Security Architecture in the federal context. The business relevance has to show that the research challenge is not only relevant for a small number of organizations, i.e., an isolated "local" problem to solve but has substantial relevance in organizational practice and deserves research. In addition to previous studies confirming the general relevance of a Cyber Security Architecture implementation, a survey among Public Sector Organisations also confirms the existence of inhibiting factors. The **phase of requirements definition** in DSR addresses the initial definition of the core artefact that is supposed to address the **identified problems**, and the identification of requirements that the artifact must meet. The artefact in our context is a procedural approach tailored to the needs of Public Sector Organisations on how to introduce ISMS and the Cyber Security Architecture. The needs of Public Sector Organisations are expressed by the requirements which in turn are derived from the inhibiting factors in combination with identified success factors. **Design and development** of the artefact in DSR is an iterative process accompanied by demonstration or evaluation. As the artefact in its current form is documented in a handbook (already published [MoSa22]). **Demonstration** means exposing the first applicable version of the artefact to a real-world application case or experts from the field. Evaluation can use different strategies, like initial evaluation in a lab setting or evaluation in real-world cases. **As the artefact** already is used by many Public Sector Organisations, we chose a combination of real-world **evaluation** and evaluation based on the features of the artefact.

DSR Phase	Research activity	Result	Section / Literature
Problem Investigation	Literature analysis to determine the state of research	Inhibiting factors and critical success factors visible in the literature	section 1 [MoSK22a]
	A survey to determine business relevance	Inhibiting factors visible in the practice of Public Sector Organisations	section 2.2 [MoSK22b]
Define	Argumentative-deductive	Summary of inhibiting	section 4

Requirements	work to derive requirements from results of problem investigation	and success factors List of requirements	
Design and develop Artifact	Conceptual-deductive work to design procedural model based on requirements	ISM procedural model and handbook	summary of this paper section 4 [MoSa22]; [MoRe23]
Demonstrate	Application of Cyber Security Architecture	Not covered in this work	
Evaluate Artifact	Evaluation	Not covered in this work	

Table 1: Research activities performed in DSR phases and their results

First, we have primarily considered the requirements of the NIS-2 Directive in this document. At the same time, we have identified further important requirements through a literature review. We merged both lists of requirements to create an overarching list of requirements as a foundation for the development of a rough procedural model.

4 Federal Cyber Security Architecture

Cyber Security architectures should be an elementary component of digital services of general interest in Germany's federal system. [Scha18] Essential actors of a regional structure must be actively connected in such a way that joint interaction can take place before, during and after cybersecurity events. The architectures, which are as harmonious as possible between the federal states, together with the federal government, represent the level of overall security that meets the requirements of European regulation. Initially, the core processes and support processes as well as the processes for the strategy of an enterprise architecture are modelled in the architecture. The inter-organizational process design of the cybersecurity organization is documented as an enterprise architecture that is to be further developed into a reference architecture. The modelling of the reference architecture was done in the modelling language ArchiMate and is shown as an example in Figure 1 on the top. In addition to research, enterprise architecture management has also evolved to provide practical support for decision-support functions in organizations such as administration [SiFS14].

The research presented here aims to determine the interlocking of a federal architecture with the information security management systems of the systemically important actors. Within the framework of a study and expert interviews, various requirements and goals for a federal Cyber Security Architecture were derived [ReKa22], [RKCS22], [RSCK22] and [ReSK00].

The foundation of such an architecture is formed by the support processes, namely **legislative processes**. Furthermore, **communication and cooperation**.

The pillars of the actual Cyber Security Architecture are built on this foundation.

- Compliance
- Risk management
- Operation
- Control and improvement
- Safety standards

On top of these supporting pillars lies the level of strategy and motivation as an umbrella.

Legislative processes: This is an essential support process that includes the obligation of the federal states to initiate legislation and regulations in line with external and internal requirements and to adapt them to the changed European regulations.

Communication and cooperation include all necessary actors and tasks to detect and defend against cybersecurity threats.

Within the framework of the core processes (pillars of the architecture), the following tasks are focused on:

Compliance: Initial and recurring identification of essential legal frameworks.

Risk Management: Monitoring the change in threats to the federal infrastructure and related threats to it and related processes.

Operation: All tasks that guarantee the operation of the cybersecurity architecture.

Control and improvement: Steering committee for assessing resilience and deriving concrete measures to maintain or improve it.

Security standards: All tools, measures and procedures that promote operations on the one hand and the resilience of the cybersecurity architecture on the other, especially in information security.

This cybersecurity architecture aims to achieve the following objectives: legal certainty, applicability, resilience, sustainability, and cooperation. **Strategy and motivation are the** umbrella process that is mapped in the architecture and visualizes the expectations of the stakeholders.

In addition to these two dimensions of "**strategy, core and support processes" and** "**goals**", the cybersecurity architecture consists of another dimension. These are processes that can be individually designed by the users to the respective context. The figure below summarizes these three dimensions (Figure 1**)**

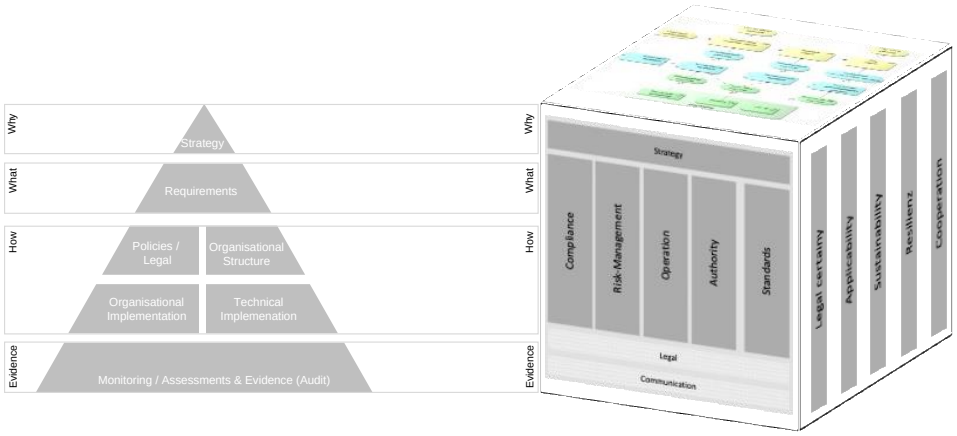

Figure 1: Cybersecurity Cube (Architecture, Goals, and Processes)

5 NIS 2 Directive

The Network and Information Systems Directive 2 (NIS-2) [Weis23] is a European directive that aims to improve cybersecurity in critical infrastructures and digital services. It significantly expands the scope and obligations of the previous Directive and thus provides for various measures to achieve the objective of improved resilience, including:

- **Mandatory security requirements**: Operators of critical infrastructure and digital services must implement appropriate safeguards to identify and prevent threats.
- **Security incident reporting**: Operators must report security incidents to national authorities and share information about these incidents to improve response capability.
- **Establishment of CSIRTs**: National authorities must establish Computer Security Incident Response Teams (CSIRTs) to respond to security incidents.
- **Regular security audits**: Operators must conduct regular security audits and review their security measures to ensure they are adequate and in line with current threats.
- **Cooperation between Member States**: Member States need to work together and share information to join Cybersecurity Cube (Architecture, Goals, and Processes) to combat threats and improve cybersecurity in Europe.

These measures are intended to ensure that critical infrastructures and digital services in Europe, including Germany, are safe and secure, and that they can respond to threats and prevent attacks. In practice, the development and sustainable establishment of an information security management system (ISMS) form an essential foundation for the implementation of the NIS 2 Directive, as an ISMS helps to ensure the security of critical infrastructures and digital services and to respond quickly and effectively to

threats.[EcKo23] In Art. 21 of the NIS 2 Directive, four **core requirements** are formulated that must be met by an ISMS [Weis23]. These include:

- **Policies**: Risk & Information Security Policies
- **Incident Management**: Prevention, detection, and management of cyber incidents
- **Business Continuity**: Business Continuity Management, Crisis Management
- **Supply Chain Management**: Security in the supply chain — up to secure development at suppliers
- **Procurement**: Security in the procurement of IT and network systems
- **Effectiveness**: Requirements for measuring cyber and risk measures
- **Training**: and Cyber Security Hygiene
- **Cryptography**: Specifications for cryptography and, where possible, encryption
- **Personal**: Human Resources Security
- **Physical access control**
- **Asset Management** (ISMS)
- **Authentication**: Use of multi-factor authentication (MFA) and single sign-on (SSO)
- **Communication**: Use of secure voice, video, and text communication
- **Emergency communication**: Use of secure emergency communication systems

At this point, the cyber security architecture described above provides a frame of **reference**. First and foremost, a **strategy** must be formulated by the deploying organisation to define the why in the implementation of the cyber security architecture. This is followed by the definition of **requirements** for the respective context. The organizational and **technical implementation** of the requirements is coordinated by an appropriate **organizational structure** and flanked by appropriate **guidelines**. Corresponding evidence must be generated, for example, by audits, which can then also be used as **proof of guarantee** against third parties.

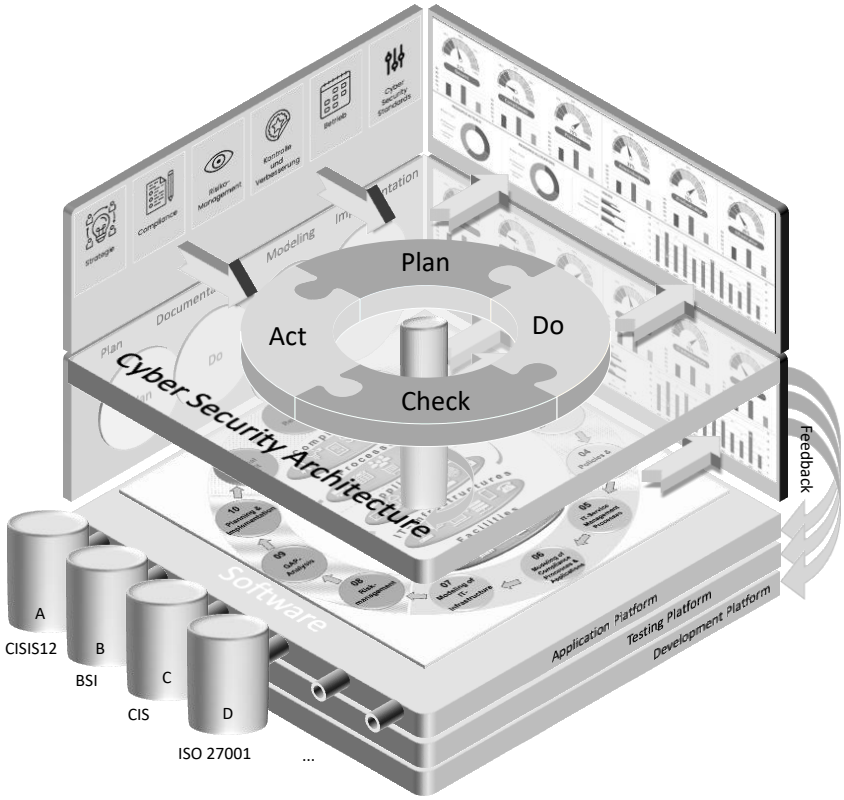

Figure 2: Cyber Security Architecture with ISMS

The elements of the cybersecurity strategy are complemented by the cybersecurity strategy (Figure 2**)**. After the theoretical derivation, strategy, requirements, and implementation measures must now be transferred to a practicable procedural model. First and foremost, the requirements of the core processes of the cybersecurity architecture act on an axis of rotation, which in turn drives the development and establishment of an ISMS. With the help of the Deming Circle, individual adaptations from the cybersecurity architecture can be transferred to the ISMS. From the ISMS, aggregated results are fed back into the control centre of the higher-level cybersecurity architecture, which allows the legally required supervisory management to be fulfilled. The user can decide for himself which standard (BSI baseline protection, ISO/IEC 27001, or others) should be used to set up and establish the ISMS.

6 CISIS12

Public organisations in particular often lack the necessary resources and expertise to set up an ISMS with which the measures formulated in the NIS 2 Directive can be implemented [MoSK22c]. Here, the CISIS12 (Compliance and Information Security in 12 Steps) process model [MoRe23] offers a quick and easy introduction to the topic of ISMS for public organizations [MoSa22].

Step 1 Guideline: The focus of the first step is the creation of a guideline on information security as one of the reference documents of the CISIS12 standard and an essential element of an ISMS.[MoSK22c] **Step 2 Raising awareness among employees**: In many projects, the consideration of employees is only at the end of the project [TFSG18]. However, it is precisely the issue of cyber security that primarily affects employees and managers. As part of step 2, a process must be established based on an appropriate concept to ensure training, sensitisation, and information for employees. However, it is important that after employees have been sensitized for the first time, sustainability is ensured by the training concept in a target group-specific manner. **Step 3 Information security team**: The roles necessary for the development of the ISMS are fixed here in writing, tasks, rights and obligations are defined and an ISMS team is formed. Depending on the size of the organization, it is necessary to determine with which roles the upcoming ISMS project is to be carried out and which employees have roles in the core team and which employees have roles in the extended security team. Regardless of this organizational structure, a member of the organizational leadership must be integrated into the extended team in any case [ChMC16]. **Step 4 IT documentation structure**: The PDCA cycle immanent in a management system focuses on the "P for plan". No successful project, without a good plan. Against this background, step 4 of the CISIS12 process model focuses on the creation and updating of a documentation structure suitable for the ISMS [SuOY22]. Documentation that is intended to support the organization in the operation of the ISMS on the one hand, but also serves as proof of certification on the other, must meet the requirements of structure, clarity, completeness, comprehensibility, correctness, traceability, objectivity, integrity, and authenticity. The CISIS12 standard lists the 16 mandatory documents (e.g., guidelines, training and awareness-raising concept, operating manual and network plan to a management report including implementation and risk treatment plan and emergency manual). In addition to these certification-relevant reference documents, further documents are inevitably created when the 12 steps are completed, e.g. work instructions, process descriptions or concepts. Almost all documentation must be made known to the employees and therefore controlled. **Step 5 IT service management**: One of the main differences to other ISMS process models is the implementation of IT service management in the CISIS12 process model. The implementation of clearly defined and described IT service management processes is a key success factor for increasing information security and .dem maturity of the ISMS [Awan17]. In step 5, the three essential IT service management processes (maintenance, malfunction and change processes) are to be set up in an organization-specific manner or

the processes that already exist in reality are to be integrated into the ISMS and further developed. **Step 6 Compliance, Processes and Applications**: CISIS12 has taken up the requirements from practice, namely, to integrate the legal requirements and contractual obligations (compliance) as well as the process view into the management system and includes five levels of consideration, namely the compliance and process layer as well as the application and infrastructure and building level. Thus, CISIS12 offers a view that corresponds to that of the management level, namely "Which legal requirements and compliance requirements must the management level meet and how can these be implemented in practice (corporate governance)?". Thus, the CISIS12 process model makes it easier for the management level to act and delegate the necessary tasks to set up and establish an ISMS while at the same time meeting the legal requirements and minimizing the liability risks of the management level. This means that in **step 6**, the business processes that are essential for the organization are identified and evaluated concerning the protection requirements of confidentiality, integrity, and availability. This can be done with the help of tools, as can the assignment of modules and measures. **Step 7** IT infrastructure: The recording of IT infrastructure objects (e.g. servers, clients, active network components, etc.) is derived from the business processes identified in step 6 and the applications necessary for these business processes and forms an important pillar of the ISMS [ChKP22]. Thus, a simplification for the user also occurs here. In this way, attention can be drawn to the implementation of the module and measure assignment. **Step 8 Risk management**: Risk management is a major innovation in the CISIS12 process model [KiCK22]. The geopolitical events of the past few months have shown that the development of an information security management system is no longer a hygiene factor (hygiene factor = works without it, but a little worse). No, an ISMS is now a "must-have" (state of the art) for all organizations and a risk management system established in it is an important tool for learning from the past and being able to better assess future events. **Step 9 Target/actual comparison**: In step 9, the measures from the CISIS12 building block catalogue modelled in steps 6 and 7 are evaluated concerning the degree of implementation. This evaluation process takes place within the framework of a group dynamic process and represents a self-evaluation. This process may be supported by external third parties. **Step 10 Implementation**: The degree of implementation of the individual measures determined in Step 9 can be transferred to an implementation plan in Step 10 with the help of tools, if necessary. Individual measures can be prioritized, their financial and personnel expenses can be recorded, and the roles of the initiator and the implementer can be defined with the help of tools. No system is perfect, and more is always possible. This also applies to the ISMS built with CISIS12. The maturity level of a management system with CISIS12 only develops with several runs. The initial audit is therefore referred to as a system audit, whereby the certification audit focuses on the documentation and implementation of the plan documents (lived security process). The surveillance audit then examines how the ISMS has developed further and how this further development affects the maturity level. **Step 11 Internal Audit**: In step 11, CISIS12 requires the organization to create an appropriate audit program. This audit program

should then include the respective certification as well as internal audits. With the help of internal audits, the organization itself should be able to examine its own ISMS for weaknesses and improve it accordingly [Pohl19]. **Step 12 Revision**: CISIS12 steps 1 to 11 must be completed regularly (e.g. annually). However, changes and additions can also be introduced into the management system at any time. Step 12 summarizes the results of the final PDCA phase and ends with the preparation of a management report. Step 12 summarizes the results of the final PDCA phase and ends with the preparation of a management report. At the same time, the management report is one of the certification-relevant reference documents. As soon as the management level has approved the management report including its assets, the next PDCA phase can begin and the continuous improvement process can be initiated [PrSu22]. The entire process is supported by the CISIS12 circuit – possibly tool-based.

7 Summary, Conclusions and Outlook

The NIS 2 Directive requires in Art. 21 fourteen measures to be implemented by federal states. The developed cybersecurity architecture forms a good procedural model for identifying, planning, implementing and sustainably establishing and controlling these measures and associated requirements. An essential tool here is the selection of a suitable process model for the further implementation of an information security management system as the basis of a higher-level cybersecurity architecture. The presented cybersecurity architecture can be used can be underpinned by the CISIS12 process model. The implementation of CISIS12 is open. An ISMS can be set up with the native CISIS12 catalogue. However, it is also possible to use other module measure catalogues with the process model, e.g., "BSI-IT-Grundschutz", "BSI-Kommunalprofil" or ISO/IEC 27001, CIS-Controls, or other proprietary measures. In particular, the aspects of the NIS 2 guideline such as guidelines, awareness and training measures for employees, incident management, business continuity management and implementation of technical and organizational measures can be implemented in a target group-adapted manner with the help of the CISIS12 process model. The result is an overall cybersecurity architecture that can meet the requirements of the NIS 2 Directive. It does not matter whether users choose a top-down approach or a bottom-up approach. Due to the interlocking of the two architectures, each approach can be started independently of the other and the necessary information can be exchanged via interfaces (Figure 1**)**.

One limitation of the present work is that the presented theoretical cybersecurity architecture has not yet been evaluated practically. Plans are currently underway to verify the architecture in conjunction with the establishment of an ISMS in a municipal organization. The logical final step is the evaluation of the overall architecture in the country context. For this purpose, the overall architecture is to be presented within the framework of the working group on the cyber security of the federal states. Depending on the evaluation results, the architecture will be further developed.

References

[Andr12] Andreasson, K. J. (Hrsg.): Cybersecurity: public sector threats and responses, Public administration and public policy. Boca Raton, FL : CRC Press, 2012 — ISBN 978-1-4398-4663-6

[Awan17] Awan, Jawad Husaain: Security strategies to overcome cyber measures, factors and barriers. In: Engineering Science and Technology International Research Journal Bd. Vol.1, No. 1 (2017)

[Bund22a] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2022 (2022)

[Bund22b] Bundesministerium des Innern und für Heimat: Bundesinnenministerin stellt Cybersicherheitsagenda vor. URL https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/07/cybersicherheitsagenda.html. — Bundesministerium des Innern und für Heimat

[Bund82] Bundesverfassungsgericht: Entscheidungen der amtlichen Sammlung - 2 BvR 1187/80. Bd. 61, 1982

[ChKP22] CHODAKOWSKA, ANETA; KAŃDUŁA, SŁAWOMIRA; PRZYBYLSKA, JOANNA: Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. In: Lex Localis - Journal of Local Self-Government Bd. Vol. 20, No. 1 (2022)

[ChMC16] Choejey, Pema ; Murray, David ; Che Fung, Chun: Exploring Critical Success Factors for Cybersecurity in Bhutan's Government Organizations. In: Computer Science & Information Technology (CS & IT) : Academy & Industry Research Collaboration Center (AIRCC), 2016 — ISBN 978-1-921987-60-1, S. 49–61

[DüFi18] Dürig, Markus ; Fischer, Matthias: Cybersicherheit in Kritischen Infrastrukturen: Europäische und deutsche Regulierung — ein Überblick. In: Datenschutz und Datensicherheit - DuD Bd. 42 (2018), S. 209–213

[EcKo23] Eckhardt, Philipp ; Kotovskaia, Anastasia: The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. In: International Cybersecurity Law Review Bd. 4 (2023), Nr. 2, S. 147–164

[Euro23] Europäisches Parlaments und Rat: Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2023

[GuKW17] Gusy, C. ; Kugelmann, D. ; Würtenberger, T. (Hrsg.): Rechtshandbuch Zivile Sicherheit. Berlin Heidelberg : Springer, 2017 — ISBN 978-3-662-53288-1

[JoPe14] Johannesson, Paul ; Perjons, Erik: An Introduction to Design Science. Cham : Springer International Publishing, 2014 — ISBN 978-3-319-10631-1

[KiBa20] Kipker, D.-K. ; Barudi, M. (Hrsg.): Cybersecurity. 1. Auflage. München : C.H. Beck, 2020 — ISBN 978-3-406-73011-5

[KiCK22] Kitsios, Fotis ; Chatzidimitriou, Elpiniki ; Kamariotou, Maria: Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security

Management Systems: A Case Study in IT Consulting Industry. In: Sustainability Bd. 14, Multidisciplinary Digital Publishing Institute (2022), Nr. 3, S. 1269

[Kraj15] Krajewski, M. (Hrsg.): Services of general interest beyond the single market: external and international law dimensions, Legal issues of services of general interest. The Hague : T.M.C. Asser Press, 2015 — ISBN 978-94-6265-062-6

[MoRe22] Moses, Frank ; Rehbohm, Thomas: CISIS12. In: , CISIS12. (2022), Nr. 1, S. 11

[MoRe23] Moses, Frank ; Rehbohm, Thomas: CISIS12 für kleine und mittelständische Organisationen IN ZWÖLF SCHRITTEN ZUM RECHTSKONFORMEN ISMS (2023), Nr. 4, S. 14–19

[MoSa22] Moses, Frank ; Sandkuhl, Kurt: Mit CISIS12 ein ISMS aufbauen. In: Datenschutz und Datensicherheit - DuD Bd. 46 (2022), Nr. 10, S. 654–659

[MoSK22a] Moses, Frank ; Sandkuhl, Kurt ; Kemmerich, Thomas: Information security management in German local government. In: , 2022, S. 183–189

[MoSK22b] Moses, Frank ; Sandkuhl, Kurt ; Kemmerich, Thomas: Empirical Study on the State of Practice of Information Securty Maturity Management in Local Government. In: Zimmermann, A. (Hrsg.): Human Centred Intelligent Systems 2022 - Proceeding of the 15th International Conference on Human Centred Intelligent Systems (KES-HCIS-22). Smart Innovation, Systems and Technologies. : Springer. Accepted for publication. To appear June 2022., 2022

[MoSK22c] Moses, Frank ; Sandkuhl, Kurt ; Kemmerich, Thomas: Empirical Study on the State of Practice of Information Security Management in Local Government. In: Zimmermann, A. ; Howlett, R. J. ; Jain, L. C. (Hrsg.): Human Centred Intelligent Systems, Smart Innovation, Systems and Technologies. Singapore : Springer Nature, 2022 — ISBN 978-981-19345-5-1, S. 13–25

[Pohl19] Pohlmann, Norbert: Cyber-Sicherheit: das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung. Wiesbaden : Springer Vieweg, 2019 — ISBN 978-3-658-25397-4

[PrSu22] Preis, Benjamin ; Susskind, Lawrence: Municipal Cybersecurity: More Work Needs to be Done. In: Urban Affairs Review Bd. 58, SAGE Publications Inc (2022), Nr. 2, S. 614–629

[ReKa22] Rehbohm, Thomas ; Kalmbach, Peter: MMR-Aktuell 2021, 438461 - beck-online, Grundforderungen von Informations- und Cybersicherheit in Ländern. URL https://beck-online.beck.de/?vpath=bibdata/zeits/MMRAktuell/2021/438461.htm. - abgerufen am 2022-09-08

[ReSK00] Rehbohm, Thomas ; Sandkuhl, Kurt ; Kemmerich, Thomas: On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration. In: , S. 13

[RiBM16] Riek, Markus ; Bohme, Rainer ; Moore, Tyler: Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. In: IEEE Transactions on Dependable and Secure Computing Bd. 13 (2016), Nr. 2, S. 261–273

[Rich22] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie). Bd. 333, 2022

[RKCS22] Rehbohm, Thomas ; Kemmerich, Robin ; Cap, Clemens H. ; Sandkuhl, Kurt: Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen. In: Datenschutz und Datensicherheit - DuD Bd. 46 (2022), Nr. 7, S. 448–454

[RSCK22] Rehbohm, Thomas ; Sandkuhl, Kurt ; Cap, Clemens H. ; Kemmerich, Thomas: Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation. In: Abramowicz, W. ; Auer, S. ; Stróżyna, M. (Hrsg.): Business Information Systems Workshops, Lecture Notes in Business Information Processing. Cham : Springer International Publishing, 2022 — ISBN 978-3-031-04216-4, S. 291–303

[Scha18] Schallbruch, Martin: Schwacher Staat im Netz: wie die Digitalisierung den Staat in Frage stellt. Wiesbaden : Springer, 2018 — ISBN 978-3-658-19946-3

[SiFS14] Simon, Daniel ; Fischbach, Kai ; Schoder, Detlef: Enterprise architecture management and its role in corporate strategic management. In: Information Systems and e-Business Management Bd. 12 (2014), Nr. 1, S. 5–42

[SuOY22] Susukailo, Vitalii ; Opirsky, Ivan ; Yaremko, Oleh: Methodology of ISMS Establishment Against Modern Cybersecurity Threats. In: Klymash, M. ; Beshley, M. ; Luntovskyy, A. (Hrsg.): Future Intent-Based Networking, Lecture Notes in Electrical Engineering. Cham : Springer International Publishing, 2022 — ISBN 978-3-030-92435-5, S. 257–271

[TFSG18] Tatiara, R. ; Fajar, A. N. ; Siregar, B. ; Gunawan, W.: Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001. In: Journal of Physics: Conference Series Bd. 978, IOP Publishing (2018), Nr. 1, S. 012039

[WaWe20] Watson, Richard T. ; Webster, Jane: Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. In: Journal of Decision Systems Bd. 29, Taylor & Francis (2020), Nr. 3, S. 129–147

[Weis23] Weissmann, Paul: Die neue EU NIS 2 Direktive für Cyber Security in KRITIS. URL https://www.openkritis.de/it-sicherheitsgesetz/eu-nis-2-direktive-kritis.html. - abgerufen am 2023-05-09

Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 29

Auf dem Weg zu einer Kompetenz des Verlernens: Öffentliche Verwaltung für die Digitalisierung stärken

Marco Di Maria[1], Daniel Bierschwale[1], Paul-Ferdinand Steuck[1] und Ralf Knackstedt[1]

Abstract: Im Zuge der Digitalisierung stehen Mitarbeiter:innen der öffentlichen Verwaltung vor großen Herausforderungen. Insbesondere die beschleunigte Produktion von Wissen und dessen immer geringere Halbwertszeit erfordern Anpassungen im gewohnten Arbeitsstil und im Umgang mit neuen Aufgaben und Technologien. Das geforderte Kompetenzprofil wandelt sich: Altes Wissen und bestehende Herangehensweisen sind teils nicht mehr nützlich und müssen verlernt werden. Dazu haben wir eine vorläufige Definition für eine Kompetenz des Verlernens formuliert, bestehende E-Government-Kompetenzmodelle in Bezug auf Verlernen analysiert, Interviews mit sechs Verwaltungsmitarbeiter:innen geführt und die Kompetenzdefinition final angepasst. Zusätzlich haben wir Handlungsempfehlungen formuliert, wie Verwaltungsmitarbeiter:innen praktisch eine Verlernkompetenz entwickeln können. Damit unterstützen wir die Gestaltung von Aus- und Weiterbildungsprogrammen und bieten eine Ergänzung bestehender Kompetenzmodelle.

Keywords: Verlernen, Unlearning, Kompetenz, Digitalisierung, Verwaltung

1 Wandel in der Öffentlichen Verwaltung erfordert Verlernen

Die öffentliche Verwaltung (ÖV) steht im Zuge der Digitalisierung unter Veränderungsdruck [Li19]. Krisen wie die Covid-19-Pandemie wirken dabei als Verstärker [Ze23]. Die auf Stabilität ausgerichtete Organisationskultur [Sc85] der ÖV ist hierbei nicht immer vorteilhaft [KG20]. So können die bis dato in stabiler Umgebung förderlichen Routinen [ES15] – u. a. papier-basierte Antrags- und Meldeverfahren – zum Problem werden. Bereits 2006 rief die damalige Bundesregierung nach einer *"nachhaltigen Modernisierung von Staat und Verwaltung [,] einschließlich des Abbaus überflüssiger Bürokratie"* [BMI06, S. 5]. Das gilt vor allem, wenn unbekannte und komplexe Herausforderungen dazukommen [Fe00], z. B. bei der Adaption neuer Technologien wie Virtual Reality [LLW22] oder Künstlicher Intelligenz [AFL19]. Doch

[1] Universität Hildesheim, Betriebswirtschaft & Wirtschaftsinformatik, Universitätsplatz 1, 31141 Hildesheim, {marco.dimaria, bierschwaled, steuckp, ralf.knackstedt}@uni-hildesheim.de

doi:10.18420/rvi2023-016

auch ein erfolgreicher Technologieeinsatz allein reicht nicht für erfolgreiches E-Government [HS13]. Vielmehr ist im soziotechnischen Sinne eine Anpassung sämtlicher betroffener Prozesse, Organisationstrukturen und Mitarbeiter:innen [SS22] erforderlich. Anpassungsprozesse werden dabei teils durch Sicherheits- und Datenschutzbedenken bei Verwaltungsmitarbeiter:innen (VM) erschwert [SGF19]. Ferner übt Regulatorik an der Schnittstelle von Recht und Technik weiter Druck auf die VM aus, z. B. durch das Gesetz zu Förderung der elektronischen Verwaltung (EGovG) bzw. E-Government-Gesetz oder auch dem Onlinezugangsgesetz (OZG). Hier müssen VM in Kommunen in angemessener Zeit Gesetzesvorhaben umsetzen, auch wenn bestehende Strukturen und Prozesse einzelner Kommunen dies nicht begünstigen und die Kompetenzen der VM nicht ausreichen [RR21]. Sie hinken bei der Binnendigitalisierung, d. h. interner Strukturen und Prozesse im Back-Office, noch immer hinterher [Ha21b].

Gut ausgebildetes Personal ist unabdingbar, denn die Digitalisierung der ÖV hängt zu großen Teilen von der Kompetenz der VM ab [Li19], z. B. bei der Nutzung Künstlicher Intelligenz [Mi22]. [HP22] heben den Mangel an geeignetem Personal mit erforderlichen Kompetenzen zur Umsetzung von IT-Vorhaben als Risikofaktor hervor. [ACB21] weisen darauf hin, dass bisher digitale Kompetenzen in Stellenanzeigen der ÖV kaum berücksichtigt werden. VM sind besonders betroffen, da sich deren Kompetenzanforderungen stetig ändern und bestehendes Wissen und Können teils nicht mehr gefragt ist und erneuert werden muss [Og16]. Um der Dynamik der Digitalisierung gerecht zu werden, müssen VM passgenau aus- und weitergebildet werden [HP22].

Versteht man Transformation als einen Lernprozess, dann sollte hierbei dem Prozess des Verlernens als Form des intentionalen Vergessens nicht mehr nützlichen Wissens mehr Gewicht eingeräumt werden. Es ist definiert als das bewusste Loslassen von bestehendem Wissen, um die Aufnahme neuen Wissens zu begünstigen [FO17]. Verlernen kann auf vielfältige Weisen unterstützt werden [Di23a]. So haben [Ko22] in einer deutschlandweiten Online-Befragung von über 400 VM gezeigt, dass sich eine Lücke im Bereich E-Government-Kompetenzen auftut. Jedoch ähnelte kaum eine Kompetenz der Befragung konzeptionell der des Verlernens. [Pa06] haben das Potenzial von Verlernen bei Transformationsprozessen in internationalen E-Government-Projekten aufgezeigt. Durch Verlernen konnten bestehende, hemmende Annahmen und Glaubenssätze identifiziert und abgelegt werden, wodurch ein Wandel der Organisationskultur bewirkt wurde [Sc85]. In Praxis und Forschung zur Digitalisierung der öffentlichen Verwaltung ist bereits heute klar, dass bestehende Kompetenzen kontinuierlich angepasst und teils abgebaut werden müssen, um Raum für neue Zukunftskompetenzen zu schaffen. Umso wichtiger erscheint es daher, frühzeitig klare Kompetenzanforderungen zu identifizieren, bestehende Kompetenzmodelle zu erweitern [HP22] und so das Fundament für die erfolgreiche Kompetenzentwicklung von VM in der Phase der Ausbildung und der Weiterbildung [Og16] zu legen. Um die bisher fragmentarisch definierten Kompetenzanforderungen an VM im Kontext von E-Government zu präzisieren [Sc10], haben wir zwei Forschungsfragen (FF) adressiert: **FF1:** *Inwiefern berücksichtigen*

bestehende Kompetenzmodelle das Konzept des Verlernens? **FF2:** *Wie kann eine Kompetenz des Verlernens auf Basis bestehenden, theoretischen Wissens und zu erlangendem, empirischem Wissen formuliert werden?*

Dieser Beitrag ist wie folgt strukturiert: In Kapitel 2 erläutern wir den aktuellen Forschungstand zu E-Government-Kompetenzen und Verlernen. Danach definieren wir eine vorläufige Kompetenz des Verlernens (KdV). In Kapitel 3 beschreiben wir unser methodisches Vorgehen. In Kapitel 4 erläutern wir die Ergebnisse der Analyse bestehender E-Government-Kompetenzmodelle als Antwort auf FF1. Ebenso präsentieren wir zentrale Erkenntnisse aus den Interviews mit VM und die überarbeitete Kompetenzdefinition für eine KdV als Antwort auf FF2. In Kapitel 5 geben wir einen Überblick über mögliche Ansätze zur praktischen Entwicklung einer KdV für VM. Im letzten Kapitel reflektieren wir unsere Ergebnisse und ziehen ein Fazit.

2 Forschungshintergrund

Organisationen der ÖV besitzen oftmals eine charakteristische ‚Verwaltungskultur'. Nach Schein beschreibt **Organisationskultur** wesentliche, geteilte Annahmen und etablierte Muster der Mitarbeiter:innen einer Organisation, um mit Problemen umzugehen [Sc85]. Sind diese geeignet zur Problemlösung, werden sie als gültig betrachtet und neuen Mitarbeiter:innen als der ‚richtige Weg' gelehrt. Ergo ist die Organisationkultur wichtig zur Schaffung von Stabilität, aber auch für Veränderung. Das zeigt sich in einer ihrer Komponenten, die bestimmte, wiederkehrende, soziale Verhalten kodiert – **Routinen.** Feldman definiert sie als effiziente Ablaufstrukturen, die als Antwort auf häufig wiederkehrende, ähnliche Aufgaben von Mitgliedern der Organisation abgerufen werden [Fe00]. In der Verwaltung sind das insbesondere papierlastige Routineprozesse wie z. B. im Antrags- und Meldewesen. Abseits fester Routinen ermöglichen **Kompetenzen** es VM, auch unter dynamischen Bedingungen neue Herausforderungen zu meistern. Unter Kompetenz im Sinne der Kompetenzmanagement-Literatur verstehen Erpenbeck und Sauter *„in offenen, unüberschaubaren, komplexen, dynamischen und zuweilen chaotischen Situationen kreativ und selbstorganisiert zu handeln*." [ES15, S. 14] Hier spielen Einstellung und Werte eine große Rolle. Denn *„Werte ermöglichen ein Handeln unter […] Unsicherheit [und] ersetzen fehlendes Wissen […]"* [ibid., S. 15]. E-Government-Kompetenzen im engeren Sinne beziehen sich nach [He18] auf Kompetenzen zur kontinuierlichen Identifikation und Realisation von Innovationspotenzialen, die durch den Digitalen Wandel induziert werden und technologische, organisationale und kulturelle Aspekte umfassen. In Anlehnung an [ACB21] fassen wir E-Government-Kompetenzen als Querschnittskompetenzen auf, die nicht auf spezifische, technische IT-Fähigkeiten beschränkt sind. **Verlernen** bezieht sich im Rahmen eines umfassenden Lernprozesses auf die Reduktion des Einflusses bestehenden, teils störenden Wissens [GKK20], als Selbstzweck [Br15] oder um den Aufbau neuen Wissens zu begünstigen [TZ08]. Das können Werte und Überzeugungen

wie z. B. Stabilität und Sicherheit sein, ebenso Arbeitsroutinen, die VM nur schwer ablegen können. Auch soziale Normen oder geteilte Ansichten – z. B. *‚Das haben wir schon immer so gemacht.‘* – sind möglich.

Auf Basis dieser Konzepte formulieren wir die **vorläufige Definition für eine KdV**: „*Verlernkompetenz bezieht sich auf die Fähigkeit und Bereitschaft einer Person oder Organisation, bestehende Denk- und Verhaltensmuster bewusst zu erkennen, zu überdenken und abzulegen, um Raum für neue Perspektiven, Fähigkeiten und Wissensinhalte zu schaffen.“* Sie fußt auf der Annahme, dass Lernen nicht nur auf den Aufbau neuer Kompetenzen fokussiert sein, sondern auch das kritische Hinterfragen und Überwinden veralteter Annahmen, Routinen und Gewohnheiten umfassen sollte. So kann die Entwicklung neuen Wissens begünstigt werden.

3 Methodisches Vorgehen

In der **Analyse bestehender Kompetenzmodelle für E-Government** haben wir auf Basis unserer vorläufigen Definition untersucht, inwiefern eine Auswahl zentraler Quellen bereits Konzepte des Verlernens berücksichtigen. Dabei haben wir neben inhaltlicher Passung auch eine Zuordnung auf die Teilprozesse des Verlernens nach [FO17] zum Verlernen organisationaler Routinen vorgenommen, welches aus drei Teilprozessen besteht: Destabilisieren, Experimentieren, Loslassen. Im Anschluss daran haben wir ähnlich wie [RR21] **Interviews** mit sechs VM aus der niedersächsischen ÖV geführt, die Erfahrungen mit der Umsetzung diverser E-Government-Maßnahmen haben. Diese haben beurteilt, inwiefern eine KdV zur Bewältigung von wissensbezogenen Hindernissen in der ÖV im Kontext von E-Government nützlich (gewesen) wäre und wie diese künftig kultiviert werden kann. Auf Basis der Interviews haben wir die Definition einer KdV nochmals überarbeitet. Abschließend haben wir sechs **praktische Ansätze zur Entwicklung einer KdV** auf Basis von Reflexion unserer Ergebnisse abgeleitet.

4 Ergebnisse

4.1 Ergebnisse der Analyse bestehender E-Government-Kompetenzmodelle

Quelle	Verlernprozess			Rolle	
	Destabilisieren	Experimentieren	Loslassen	Fach	Führ.
[ACB21]		x		x	
[Be16]		x		x	x
[Pa17]	x	x	x	x	x
[RNG17]	x			x	x
[HS13]	x	x	x		x
[SB20]	x	x	x	x	x

Tab. 1: Überblick über analysierte Quellen

Wir haben sechs Kompetenzmodelle und Ansätze aus [ACB21] und [SB20] mit Bezug zu E-Government nach dem Modell von [FO17] analysiert (vgl. Tab. 1).

[ACB21] nennen in ihrem erweiterten Kompetenzmodell für die digitale Verwaltung E-Kompetenzen und Digitale Kompetenzen. Relevant für Verlernen im Bereich Problemlösung erscheinen die E-Kompetenzen *„Change Management“* und *„Lernbereitschaft“* [ibid., S. 7] – ebenso die digitalen Kompetenzen *„Innovationsorientierung [,] Kreativitätstechniken [und] Innovationsmethoden (Design Thinking)“* [ibid.]. Da die Kompetenzen nicht näher erläutert wurden, ist eine Zuordnung zu anderen Prozessphasen als ‚Experimentieren‘ – siehe Kreativitätstechniken und Innovationsorientierung – nicht möglich.

[Be16] haben in der Studie ‚E-Kompetenz‘ im Auftrag des IT-Planungsrates als Managementkompetenz *„Changemanagement“* [ibid., S. 14] genannt. Weiter nennen sie als gestalterische Fähigkeiten: *„Gestaltungswille [,] Kreativität [,] Innovationsbegeisterung [,] Veränderungsbereitschaft [und] Weiterbildungsbereitschaft“* [ibid., S. 15]. Als persönliche Fähigkeiten nennen sie *„Flexibilität [,] Frustrationstoleranz* [,] *Risikobereitschaft [sowie] Problemlösekompetenz“* [ibid., S. 16]. Die Kompetenzen sind nicht weiter definiert, weswegen eine Phasenzuordnung eher schwierig ist. Jedoch bietet das Kompetenzmodell die Möglichkeit zur Erweiterung in sog. Steckbriefen [ibid.].

[Pa17] beziehen sich in ihrer Analyse von Kompetenz- und Qualifizierungsbedarfen im Bereich des öffentlichen Dienstes stark auf Routineprozesse, die sich im Wandel befinden und daher *„Veränderungsbereitschaft und Anpassungsfähigkeit“* bei VM fordern [ibid., S. 38]. Indirekt ist die Notwendigkeit einer Verlernkompetenz angezeigt, da sich IT-Systeme kontinuierlich weiterentwickeln. VM müssen sich also auf durchgehendes Verlernen einstellen, auch wenn keine Kompetenz dies bisher so erfasst.

[RNG17] betonen den Charakter ständiger Herausforderungen, u. B. durch die Anpassung an neue Programme. Daher müssen VM *„lernen, mit ständig neuen Technologien und geänderten Verfahren umzugehen."* [ibid., S. 2]. In Bezug auf die Organisationskultur in der ÖV sollen hinderliche Faktoren identifiziert und beseitigt werden, um eine Kultur der stetigen Veränderung etablieren zu können [ibid.]. Die Bereitschaft zu kontinuierlicher Veränderung aufgrund diverser Trigger ist gefordert, es wird hierfür jedoch keine konkrete Kompetenz für Fach- oder Führungskräfte genannt.

[HS13] definieren diverse E-Government-Teilkompetenzen, die für Verlernen relevant sind. Dazu gehört *„Reflexion"* [ibid., S. 7] zur Identifikation von Veränderungspotenzialen. Ebenso erwähnen sie *„Kreativität"*, wodurch VM in der Lage sind, auch in unbekannten, instabilen Umgebungen zu agieren. *„Designkompetenzen"* unterstützen VM beim Analysieren, Neudenken und Gestalten von IT-basierten Prozessen und Strukturen der ÖV [ibid.]. *„Veränderungskompetenzen"* helfen VM dabei, einmal abgelegte Routinen nachhaltig zu verlernen [ibid.].

[SB20] decken mit Qualifica Digitalis über verschiedene Teilkompetenzen den gesamten Verlernprozess ab. Ein *„digitales Mindset"* [ibid., S. 22] hilft VM bei der Initiierung von Veränderungsprozessen und *„Kreativität und Innovativität"* [ibid., S. 20] bei der Erkundung neuer Herangehensweisen. *"Interdisziplinäres Verständnis"* [ibid., S. 23] versetzt VM in die Lage, *„übergreifende Zusammenhänge zu erkennen, Denk- und Handlungsweisen aus verschiedenen Disziplinen zusammenzubringen und vorhandenes Silodenken zu überwinden."* Übergreifend helfen *„Innovationskompetenz und Veränderungsbereitschaft"* [ibid., S.24] sowie *„Transformationskompetenz"* [ibid., S. 25] bei der Bewältigung von Veränderungsaufgaben.

Auch wenn die hier analysierten Kompetenzmodelle teilweise oder komplett den Verlernprozess adressieren, haben wir keine konkrete Kompetenz identifizieren können, die klar das Verlernen von bestehendem, hinderlichem Wissen fokussiert.

4.2 Ergebnisse der Interviews mit Verwaltungsmitarbeiter:innen

Wir haben eine ehemalige VM (T1) und fünf aktuelle VM (T2-T6) zur Umsetzung von E-Government-Maßnahmen befragt (vgl. Tab. 2). Diese haben über konkrete Umsetzungen (z. B. OZG, E-Akte) berichtet. Dann haben sie Probleme dabei erläutert und beschrieben, wie sie und die Organisation darauf reagiert haben. Anschließend haben wir die Definition einer KdV und zugrundeliegende Annahmen präsentiert und nach deren potenziellen Nutzen im Falle der geschilderten Umsetzungserfahrung gefragt. Abschließend haben wir gefragt, wie die KdV in Aus- und Weiterbildung gefördert werden kann, um langfristig eine KdV in der Verwaltung zu kultivieren.

#	Rolle	**Rollentyp** Fach- oder Führungskraft	**Art der Verwaltung**	**Ebene der Verwaltung**	**Erfahrung** (Jahre[2])	**Dauer des Interviews** (Minuten)
T1	Smart City Manager Senior Consultant	Führungskraft Fachkraft	Stadt /	Kommune /	5/6 1	60
T2	Stellvertr. Dezernatsleitung	Führungskraft	Amt für regionale Landesentwicklung	Land	7/24	60
T3	Personalberatung	Fachkraft	Arbeitsagentur	Bund	8/14	55
T4	Berufsberatung	Fachkraft	Arbeitsagentur	Bund	3/3	49
T5	Stellvert. Teamleitung Ausbildung	Fachkraft	Arbeitsagentur	Bund	4/35	53
T6	Fachassistentin	Fachkraft	Arbeitsagentur	Bund	5/5	32

Tab. 2: Übersicht der interviewten Verwaltungsmitarbeiter:innen und weitere Details

Die Erfahrungen mit E-Government waren vielfältig. Von der Umsetzung der **E-Akte** und des **OZG** haben T1 und T2 berichtet. T3 hat Erfahrungen mit **E-Recruiting-Prozessen** geteilt. T4, T5 und T6 schilderten Erfahrungen mit dem Umstieg auf **digitale, videobasierte Telefonie**, z. B. Skype.

Die vorgestellte Definition und Beschreibung der KdV wurde überwiegend positiv durch alle Teilnehmenden aufgefasst und als nützlich empfunden. T2 unterstrich die Notwendigkeit der KdV, da *„völlig neue Kompetenzen wichtig werden, die wir heute nicht kennen und nicht Teil der Ausbildung sind“.* T3 beurteilte die KdV als *„sehr interessant“* angesichts der häufigen Aussage in der ÖV: *„Das haben wir immer schon so gemacht.“* T4 sagte, die KdV sei vor allem dort nützlich, wo man *„individuell auf neu aufkommende Bedarfe eingehen muss und alte Herangehensweisen eher blockieren.“* Jedoch wurden auch Überarbeitungsbedarfe angezeigt (T1, T3, T5). So sagte T1, dass die Definition grundsätzlich zutrifft, jedoch für den Einsatz in der Ausbildung angepasst werden müsste, damit junge Erwachsene diese verstehen können. T3 erschien die KdV nicht *„positiv belegt zu sein.“* und regte eine Umformulierung an. T5 sagte, sie würde sich eine Verlernkompetenz wünschen, um *„alte Zöpfe abzuschneiden […] umzudenken, sich neu auszurichten und Gewohntes abzulegen.“* T5 erwähnt jedoch auch, dass *„man sie positiv beschreiben“* muss, wenn die KdV von den VM akzeptiert werden soll.

Um eine KdV zu fördern hatten die Teilnehmenden diverse Ideen. T1 schlägt **Wirtschaftspraktika** vor, in denen VM *„neue Perspektiven von außen erhalten und dann*

[2] Lesehilfe: n/m, n = Jahre in konkreter Rolle als VM, m = Beschäftigungsdauer in ÖV insgesamt

nach innen tragen [und so] einfach einmal anderes Arbeiten sehen.“. Mit Bezug zu **übergreifendem Austausch** nannte T1 interkommunale ‚Change Projekte' mit VM aus verschiedenen Kommunen. T2 griff mit **Netzwerken** eine ähnliche Idee auf. Sie können hilfreich sein zur Förderung einer KdV, insbesondere durch organisationsübergreifende Zusammenarbeit und die dabei gewonnenen, neuen Einblicke und den Erfahrungsaustausch. T1 plädierte stark für „*geschützte Räume, um über strukturelle Optimierungsmaßnahmen nachdenken [zu] können.“* T3 betonte den Nutzen dieser **praktischen Freiräume**, die Raum und Zeit für Fehler außerhalb der eigenen Organisation *„erfahrbar und erlebbar“* machen. Der *„Kontakt zu anderen Teams“* kann neue Perspektiven eröffnen. Diese praktischen Experimentierräume sind wichtig für VM, da Verlernkompetenz eine *„learning-by-doing-Kompetenz“* zu sein scheint, wie es T4 erwähnte. T1 brachte die Idee von **Veränderungsberater:innen** – intern wie extern – ein, die wichtige Impulse zur Identifikation und Behebung struktureller Schwächen im Sinne einer *„Hilfe zur Selbsthilfe*“ leisten können. Diese könnten als **Coaches** VM individuelle Unterstützung beim Verlernen bieten, um *„Platz für neues [zu] schaffen“* (T4). Diese können durch Feedback den Prozess der Entwicklung einer KdV begleiten und **Feedback** geben. Formate der **offenen Innovation** können sinnvoll sein, bei denen motivierte VM identifiziert werden können, die dann – z. B. in Innovationswettbewerben – wichtige Kompetenzen wie Kreativität *„als einen wesentlichen Bestandteil, dass ich Verlernkompetenz überhaupt aufbauen kann“,* trainieren (T1). Allen Teilnehmenden erscheinen **Workshops** und **Schulungen** von Vorteil, z. B. allgemein zu Change Management, um Bewusstsein und Akzeptanz zu schaffen, bevor konkrete Umsetzungsmaßnahmen wie die E-Akte erfolgen. T2 betont, dass Vorteile vorab konkret und einfach kommuniziert werden sollten. T4 sieht in Workshops eine gute Möglichkeit, um sich neue Sachen zu erarbeiten. T5 merkt kritisch an, dass *„nur Online-Workshops hier nur bedingt geeignet sind [und] eher Präsenz hier gut wäre.“* Im Nachgang könnten ergänzend digitale Angebote hilfreich sein, um den Fortschritt zu sichern. Schließlich ist **Feedback** – von Kolleg:innen, Führungskräften, externen Coaches – ein motivierendes, erleichterndes Element, das bei der Entwicklung einer KdV helfen kann.

4.3 Finale Definition einer Kompetenz des Verlernens

Auf Basis der Reflexion der Ergebnisse aus der Analyse der Kompetenzmodelle und der Interviews haben wir folgende, finale Definition für eine KdV formuliert, die für den direkten Gebrauch mit VM gedacht ist: „*Erneuerungskompetenz bezieht sich auf die Fähigkeiten und Bereitschaft einer Person oder Organisation, bestehende Denk- und Verhaltensmuster bewusst zu erkennen, zu überdenken und abzulegen, um Raum für neue Perspektiven, Fähigkeiten und Wissensinhalte zu schaffen.“* Die neue Version trägt dem Feedback der Teilnehmenden Rechnung, d. h. sie ist positiver formuliert, damit VM möglichst nichts Negatives damit assoziieren. Die ursprüngliche Definition (vgl. Kap. 2) erscheint uns für den wissenschaftlichen Gebrauch dennoch weiter nützlich, da sie direkt das zugrundeliegende Konzept des Verlernens reflektiert.

5 Ansätze zur praktischen Entwicklung einer Verlernkompetenz

Wir stützen uns auf [Di23a] und präsentieren sechs konkrete Ansätze zur praktischen Entwicklung einer KdV für Mitarbeiter:innen der öffentlichen Verwaltung **[A1-A6]**.

[A1] Frühzeitige Identifikation von hinderlichen Denkweisen und störenden Routinen [MN17] kann VM dabei helfen, diese aktiv abzubauen, bevor sich diese in größeren Barrieren manifestieren, die schwerer zu beheben sind.

[A2] Veränderungsberater:innen – sog. ‚Change Consultants' [GKK20] – können das Verlernen hinderlicher Routinen unterstützen. Beispielsweise können Führungskräfte als interne ‚Disruptoren' aktiv ein Hinterfragen bestehender Verwaltungsprozesse im eigenen Team anstoßen. Externe Berater:innen können als Coaches [ES15] kontinuierliches Verlernen, z. B. durch Reflexionsworkshops und Einzelgespräche, mittels gezieltem Feedback fördern und so beim stetigen Verlernen helfen.

[A3] Verlern-Räume [CSC11] können, physisch oder digital, VM beim Experimentieren mit neuen Technologien unterstützen. So können sie besser den Nutzen eines neuen Ansatzes ‚im Kleinen' verstehen, bevor dieser tatsächlich in der eigenen Verwaltung umgesetzt wird. Denn *„die zentralen Orte der Kompetenzentwicklung [sind] heute die Arbeitsprozesse selbst […]"* [ES15, S. 19]. Angst vor Veränderung kann reduziert und über Chancen und Risiken reflektiert werden. Verlern-Räume schaffen *„Rahmenbedingungen, die Möglichkeiten zum Ausprobieren und Experimentieren erlauben."* [SS22, S. 150]. Dazu haben [Kl21] mit dem ‚Open Government Labor' ein interessantes Format erprobt, das sich Konzepte des Design Thinking zu eigen macht.

[A4] Netzwerke [ES15] – formale und informelle – bieten VM aus verschiedenen Verwaltungen die Möglichkeit zum Austausch von Erfahrungswissen. In ‚interkommunaler Zusammenarbeit' [Ha21a], z. B. ‚Communities of Practice' [ES15], können sie sich in sicherer Umgebung öffnen [GK17] und erhalten Feedback von Gleichgestellten. So wird ‚peer unlearning' und Vernetzung [Bi18] ermöglicht.

[A5] Innovationswettbewerbe können ein Format zur Förderung von Verlernen sein [Di23b]. Um bestehende Strukturen, Prozesse und Produkte in der öffentlichen Verwaltung neuzudenken, können Hackathons [GMS18] dienen, in denen VM zeitlich befristet die Vorteile neuer Ideen und Technologien praktisch erfahren können.

[A6] Präventionsmaßnahmen gegen einen Rückfall in alte Muster [MN17] können dabei helfen, Verlernerfolge zu sichern. So könnten Routinen zur Reflexion bestehender Muster im Team etabliert oder Anreizstrukturen, z. B. Belohnungen für identifizierte, hemmende Praktiken oder Ideen für neue Ansätze [SB09], geschaffen werden.

6 Reflexion, Fazit und Ausblick

Für das Gelingen der Digitalen Transformation in der öffentlichen Verwaltung (ÖV) muss sich diese für Veränderung öffnen. Verwaltungsmitarbeiter:innen (VM), insbesondere Führungskräfte, müssen ihr Denken und Handeln stets hinterfragen und anpassen. Hindernisse wie ineffiziente Prozesse müssen abgebaut werden. Verlernen kann hier Abhilfe schaffen, um Strukturen und Prozesse der ÖV kontinuierlich zu erneuern. Auf Basis einer vorläufigen Definition für eine Kompetenz des Verlernens (KdV) haben wir Lücken in bestehenden Kompetenzmodellen für E-Government identifiziert und deren Einfluss auf Aus- und Weiterbildung von VM aufgezeigt. Diese Definition haben wir in sechs Interviews mit VM nachgeschärft. Schließlich haben wir sechs Ansätze zur praktischen Entwicklung dieser KdV im Kontext der ÖV präsentiert, die als Orientierungshilfe in der Aus- und Weiterbildung von VM dienen können. Trotz möglicher Einschränkungen unserer Vorgehensweise bietet unser Beitrag relevante Erkenntnisse für Forschung und Praxis. So kann die von uns entwickelte Definition für eine KdV als übergreifende Kompetenz bestehende Kompetenzmodelle erweitern. Ferner schaffen wir mit unserer KdV die Basis für die Gestaltung und Beschaffung von Aus- und Weiterbildungsprogrammen mit Fokus auf Unterstützung von Verlernen [Di23c]. Wir hoffen mit unserem Beitrag VM auf ihrem *„Weg zu einer innovativen Verwaltung“* [Og16, S. 13] zu unterstützen.

7 Danksagungen

Wir danken dem Europäischen Sozialfonds (ESF+) und dem Land Niedersachsen (NBank) für die teilweise Förderung dieser Forschung im Rahmen des Forschungsprojekts 'ProXHybrid' (ZAM 3-87002690). Ebenso danken wir der Agentur für Arbeit in Niedersachsen und der Protiviti GmbH für die Zusammenarbeit.

Literaturverzeichnis

[ACB21] Auth, G.; Christ, J.; Bensberg, F.: Kompetenzanforderungen zur Digitalisierung der öffentlichen Verwaltung: Eine empirische Analyse auf Basis von Stellenanzeigen. In: Proc. der 16. Int. Tagung Wirtschaftsinformatik 2021 (WI21), Duisburg-Essen, Deutschland, 2021.

[AFL19] Anke, J.; Fischer, U.; Lemke, R.: Integration digitaler Sprachassistenten in den Kundenservice am Beispiel der Stadtwerke Leipzig. Digitalisierung von Staat und Verwaltung, S. 25-36, 2019.

[Be16] Becker, J. et.al.: E-Government-Kompetenz. Studie im Auftrag des IT-Planungsrats. Berlin, München, Münster, Siegen, 2016.

[Bi18] BitKom. Digitale Kompetenzen in der Verwaltung stärken. Impulspapier, 2018.

[Br15] Brook, C. et.al.: On stopping doing those things that are not getting us to where we want to be: Unlearning, wicked problems and critical action learning. Human Relations, 69/2, S. 369–389, 2015.

[BMI06] Bundesministerium des Inneren. Zukunftsorientierte Verwaltung durch Innovationen. Regierungsprogramm, 2006.

[CSC11] Cegarra-Navarro, J. G.; Sánchez-Vidal, M. E.; Cegarra-Leiva, D.: Balancing exploration and exploitation of knowledge through an unlearning context: An empirical investigation in SMEs. Management Decision, 49/7, S. 1099-1119, 2011.

[Di23a] Di Maria et al.: Practical Support for Unlearning – A Systematic Review to Organize the Field. In: Proc. of the 31st Eur. Conf. on Information Systems 2023 (ECIS23), Kristiansand, Norwegen, 2023.

[Di23b] Di Maria et al.: Design-Challenges im virtuellen Raum – Ein Erfahrungsbericht und Handlungsempfehlungen. HMD Praxis der Wirtschaftsinformatik, 60. S. 738-753, 2023.

[Di23c] Di Maria et al.: Designing Unlearning Support Systems: A Requirements Catalog. In: Proc. der 18. Int. Tagung Wirtschaftsinformatik 2023 (WI23), Paderborn, Deutschland, 2023.

[ES15] Erpenbeck, J.; Sauter, W.: Wissen, Werte und Kompetenzen in der Mitarbeiterentwicklung: Ohne Gefühl geht in der Bildung gar nichts. SpringerGabler, Wiesbaden, 2015.

[Fe00] Feldman, M. S.: Organizational routines as a source of continuous change. Organization science, 11/6, S. 611-629, 2000.

[FO17] Fiol, C. M.; O'Connor, E. J.: Unlearning established organizational routines–Part II. The Learning Organization, 24/2, S. 82-92, 2017.

[GK17] Grisold, T.; Kaiser, A. Leaving behind what we are not: Applying a systems thinking perspective to present unlearning as an enabler for finding the best version of the self. Journal of Organisational Transformation & Social Change, 14/1, S. 39-55, 2017.

[GKK20] Grisold, T.; Klammer, A.; Kragulj, F.: Two forms of organizational unlearning: Insights from engaged scholarship research with change consultants. Management Learning, 51/5, S. 598–619, 2020.

[GMS18] Guenduez, A. A.; Mergel, I.; Schedler, K.: Making cities smarter: Which work practices are need to drive smart city transformation?. Universität Konstanz OPAS-Plattform Serie, Nr. 002018, 2018.

[Ha21a] Halsbenning, S.: Digitalisierung öffentlicher Dienstleistungen: Herausforderungen und Erfolgsfaktoren der OZG-Umsetzung in der Kommunalverwaltung. HMD Praxis der Wirtschaftsinformatik, 58/5, S. 1038-1053, 2021.

[Ha21b] Handke, S.: Digitalisierung der öffentlichen Verwaltung: Öffentlichkeit als Reformkatalysator. Gemeinschaften in neuen Medien, Dresden, S. 256-274, 2021.

[He18] Heuermann, R.: Digitalisierung der Verwaltung – Ziele und Organisation. In (Heuermann, R., Tomenendal, M., und Bressem, C., Hrsg.): Digitalisierung in Bund, Ländern und Gemeinden – IT-Organisation, Management und Empfehlungen. S. 13–29. Gabler Verlag, Wiesbaden, 2018.

[HP22] Handke, S.; Pidun, T.: Fit fürs Amt: Notwendigkeit und Ansätze der Schärfung von Kompetenzanforderungen und Ausbildungsprofilen für die Digitalisierung der Verwaltung. FIfF-Kommunikation, 3/2022, S. 22-28, 2022.

[HS13] Hunnius, S.; Schuppan, T.: Competency Requirements for Transformational E-Government. In: Proc. of the 46th Hawaii Int. Conference on System Sciences 2013 (HICSS13), S. 1664-1673, 2013.

[KG20] Kersting, N.; Graubner, D.: Die digitale Transformation der deutschen Verwaltung Analysen zu Marktversagen und Daseinsvorsorge in Zeiten der Covid-19-Pandemie. In (Roters, W.; Gräf, H.: Wollmann, H., Hrsg.): Zukunft denken und verantworten. Springer VS, Wiesbaden, S. 231-252, 2020.

[Kl21] Klein, H. C. et.al.: Design Thinking als Werkzeug für Co-Kreation und Co-Design – Ein Erfahrungsbericht in 5 Thesen. HMD Praxis der Wirtschaftsinformatik, 58/5, S. 1148-1162, 2021.

[Ko22] Koddebusch, M. et.al.: The Increasing e-Competence Gap: Developments over the Past Five Years in the German Public Sector. In: HCI in Business, Government and Organizations: Proc. 9th Int. Con. HCIBGO 2022, Part of the 24th HCI Int. Con., HCII 2022, Virtual Event, 26. Juni – 1. Juli, Springer International Publishing, Cham, S. 73-86, 2022.

[LLW22] Lai, L. L.; Lin, S. C.; Wang, H. C.: Transforming Cultural Heritage -A Digital Humanity Perspective with Virtual Reality. In: HCI in Business, Government and Organizations: Proc. 9th Int. Con. HCIBGO 2022, Part of the 24th HCI Int. Con., HCII 2022, Virtual Event, 26. Juni – 1. Juli, Springer International Publishing, Cham, S. 87-96, 2022.

[Li19] Lindgren, I. et.al.: Close encounters of the digital kind: a research agenda for the digitalization of public services. Government Information Quarterly. 36/3, S. 427–436, 2019.

[Mi22] Mikalef, P. et.al.: Enabling AI capabilities in government agencies: A study of determinants for European municipalities. Government Information Quarterly, 39/4, 101596, 2022.

[MN17] Morais-Storz, M.; Nguyen, N.: The role of unlearning in metamorphosis and strategic resilience. The Learning Organization, 24/2, S. 93-106, 2017.

[Og16] Ogonek, N. et.al.: Auf dem Weg zu einer innovativen Verwaltung: Rollen und Kompetenzen der Verwaltung im E-Government-Kontext. In: Digitale Transformation: Methoden, Kompetenzen und Technologien für die Verwaltung 2016, Dresden, Deutschland, S. 13-24, 2016.

[Pa17] Patscha, C. et.al.: Kompetenz- und Qualifizierungsbedarfe bis 2030: Ein gemeinsames Lagebild der Partnerschaft für Fachkräfte. 2017.

[Pa06] Pan, G. et.al.: Escalation and de-escalation of commitment: a commitment transformation analysis of an e-government project. Information Systems Journal, 16/1, S. 3-21, 2006.

[RNG17] Räckers, M.; Nelke, A.; Gilge, S.: E-Kompetenz im öffentlichen Sektor Eine Positionsbestimmung. IT-Planungsrat, Gesellschaft für Informatik e. V. und Nationales E-Government Kompetenzzentrum, 2017.

[RR21] Redmann, J.; Rückel, D.: Die digitale Transformation kommunaler Einrichtungen – Herausforderungen und Erfolgsfaktoren. HMD Praxis der Wirtschaftsinformatik, 58/5, 2021.

[SB09] Srithika, T. M.; Bhattacharyya, S.: Facilitating organizational unlearning using appreciative inquiry as an intervention. Vikalpa, 34/4, S. 67–77, 2019.

[SB20] Schmeling, J.; Bruns, L.: Kompetenzen, Perspektiven und Lernmethoden im digitalisierten öffentlichen Sektor. Fraunhofer Institut für Offene Kommunikationssysteme (FOKUS), Berlin, 2020.

[Sc10] Schuppan, T.: E-Government Competencies. Looking Beyond Technology. In: (Shea, C.M.; Garson, G.D., Hrsg.): Handbook of Public Information Systems, 3. Auflage, Taylor & Francis, Boca Raton, S. 353-370, 2010.

[Sc85] Schein, E. H.: Organizational culture and leadership. Jossey-Bass, San Francisco, 1985.

[SGF19] Schedler, K.; Guenduez, A. A.; Frischknecht, R.: How smart can government be? Exploring barriers to the adoption of smart government. Information Polity, 24/1, S. 3-20, 2019.

[SS22] Schorlemmer, J.; Steffen, A.: Umgang mit Angst in Veränderungsprozessen der öffentlichen Verwaltung in Deutschland–Psychologische Grundlagen und praktische Ansätze. In (Richenhagen, G.; Dick, M., Hrsg.): Public Management im Wandel: Auf dem Weg zur Agilität in der öffentlichen Verwaltung. SpringerGabler, Wiesbaden, S. 147-169, 2022.

[TZ08] Tsang, E. W.; Zahra, S. A.: Organizational unlearning. Human relations, 61/10, S. 1435-1462, 2008.

[Ze23] Zeuge, A. et.al.: Crisis-driven digital transformation as a trigger for process virtualization: Fulfilling knowledge work process requirements for remote work. International Journal of Information Management, 70, 102636, 2023.

Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
42 Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023

On the Search for Trust: Self-Sovereign Identity and the Public Sector

Daniel Richter[1], Anna-Magdalena Krauß[2], Sarah Ebert[3], Stefan Handke[4]

Abstract: Trust in the government can be seen both as a prerequisite as well as an outcome for public sector digitization. Recently, Self-sovereign Identity (SSI) has been pursued as a means to provide an infrastructure for the secure exchange of digital credentials to public services. To enable SSI's potentially trust-enhancing properties in digital public services, we gather necessary design factors from the perspective of the system's user experience (UX) and the governance of technical artifacts and users. We provide a concretization of generic antecedents to trust found in the literature by using them as an analytical lens for the case of a digital public service utilizing SSI: the implementation of the direct-democratic instrument of the citizen's initiative ("Bürgerbegehren") in the city of Dresden, Germany. We highlight gaps in the case and literature and give recommendations concerning both the UX and credential governance to foster trust-enhancing implementations of SSI in public services.

Keywords: Trust, Self-Sovereign Identity, Digital Identity Wallet, User Experience, Governance, Acountability, Public Sector, Public Administration, E-Government, E-Democracy

1 Introduction

Low trust in government has long been seen as a trigger for increasing public service performance. However, the causality between the increase in trust and the modernization of the public sector has been challenged [vB03]. In e-government, trust is seen as an important prerequisite for the adoption of digital services by citizens [Ca16]. In this respect, "trust is a cause, an objective, a driver, and a leverage of public sector reform. It is important to keep trust on the reform agenda in an explicit way. […] Improving service

[1] HTWD - University of Applied Sciences, Digital Service Systems Group, Friedrich-List-Platz 1, 01069 Dresden, daniel.richter@htw-dresden.de
[2] HTWD - University of Applied Sciences, Digital Service Systems Group, Friedrich-List-Platz 1, 01069 Dresden, anna-magdalena.krauss@htw-dresden.de
[3] HTWD - University of Applied Sciences, Digital Service Systems Group, Friedrich-List-Platz 1, 01069 Dresden, sarah.ebert@htw-dresden.de
[4] HTWD - University of Applied Sciences, Chair of Public Management, Friedrich-List-Platz 1, 01069 Dresden, stefan.handke@htw-dresden.de

doi:10.18420/rvi2023-024

delivery is necessary but not sufficient for trust. Good performance does not necessarily lead to more trust, but bad performance certainly will erode trust" [Bo12].

Besides evaluating the general system of governance, citizens can base their trust in public services on the cooperation with street-level bureaucrats. Such an interpersonal relationship is the origin of any discussion on trust. Trust can be defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" [TPH14]. The nature of control is also crucial for digital relationships and online interactions. Since "[t]he Internet was built without a way to know who and what you are connecting to" [Ca05], *digital* public services suffer from the same fundamental trust-related shortcomings as any other digital transaction involving a non-marginal risk component [BJS10].

Emerging from the intersection of public key cryptography, blockchain technology, and traditional identity management [Se22], self-sovereign identity (SSI) is a set of technologies often referred to as being capable of inducing trust into digital interactions [Sc23]. By providing an infrastructure for the exchange of digitally verifiable credentials, SSI is therefore a valuable component for public sector digitization [JRA22]. This is reflected in a growing number of public digitization projects relying on SSI internationally. Most notably, the European Commission has initiated a revision of the 2014 Regulation on Electronic Identification, Authentication and Trust Services (eIDAS) by drawing from SSI's main principles. The proposed amendments aim at supplying EU citizens with certified digital identity wallets for more user-friendly and privacy-respecting data sharing in both the public and private sectors [Eu21].

Whether and how SSI can meet these expectations is not yet clear. Recent research underlines deficiencies in SSI's core conceptual foundations which inhibit practical implementation projects [LKA21]. Among them is the phenomenon of trust which in most publications is oversimplified and quite arbitrarily taken for granted by implementing the so-called "trust triangle" between a digital credential's issuer, holder, and verifier, e.g. [Eh21]. However, the alignment of this diverse set of actors in practice is found to be one of the most important challenges in SSI projects [LKA21]. We argue that the implementation of SSI in such a critical area as the public sector requires a more profound understanding of the mechanisms underlying its trust-enhancing properties. Therefore, the research question guiding this study can be formulated as: "Which socio-technical factors in an SSI system are relevant to trustworthy digital public services delivery?"

To answer this question, we specifically focused on two perspectives. First, user experience is an important influencing factor for trust in information systems, especially when the user has no alternative service choices, as prevalent in the public sector [AK12]. Second, we took a governance perspective as (digital) administrative action should follow the principle of legality and governance has been identified as an important building block for SSI's trust-providing features [Da19]. As a methodological starting point, we reviewed

the scientific literature on trust taking these perspectives, and generating a set of generic trust-building factors. We then applied these factors as a lens for analyzing a case of a digital public service using SSI. Access to that case was provided as part of a German government initiative to test SSI solutions in public and private services. We chose the case of the citizens' initiative ("Bürgerbegehren") in the Saxon state capital Dresden, which as an instrument of direct democracy allowed us to examine the identified factors in an area where trust is of high importance. The analysis led to a set of trust-building factors in the areas of user experience and governance specified to the scope of a digital public service using SSI. We therefore provide actionable insights for practitioners and a foundation for future research.

2 Theoretical background

2.1 The kaleidoscope of trust research

Trust is an easily accessible concept as everyone can find situations relying on it in daily life. This broad spectrum of situations wherein we can identify trust, however, is also one of the reasons why a clear definition of the concept is so hard and why the term tends to be used imprecisely. Trust has consequently been studied from a variety of different scientific angles. In this paper, we focus on the socio-psychological tradition of trust research. A widely cited definition of trust is based on a meta-analysis consolidating competing views [Ro98]: "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another." In this light, trust is seen as relational and contextual. The contextual component of a trusting relationship is referred to as so-called institutional trust, which consists of an assessment of the normality of a situation and the existence of structural assurances such as contracts, or the rule of law [MCC98]. Further, a trusting relationship is often explicated in a dyadic role model with a trustor who trusts a trustee, e.g. [Ro98]. The degree of trust by a trustor is determined by a set of beliefs about the trustee. These are influenced by their type. To trust a human-like actor, beliefs of competence, benevolence, and integrity are more important than beliefs about functionality, helpfulness, and reliability in the case of more system-like actors [LMT15].

These beliefs need to be formed based on information about the trustee. In digital interactions, typical sources of information such as appearance or previous conduct are often not available, so "second-hand information" from other trusted sources must be used [Sz03]. The provision of such informational cues by "proof sources" [MF88] in the form of verifiable credentials is at the heart of SSI. Both the technical artifacts and the institutional context wherein they are embedded must signal trustworthiness to users for the claim "SSI leads to more trustworthy digital interactions" to be valid. The respective foundations of this trust signaling are considered in the following sections.

2.2 Self-sovereign identity as trust-enhancing technology?

The roots of the claim that SSI can lead to more trust in digital interactions can be traced back to an influential blog post by identity expert Christopher Allen, wherein he lays out the basic principles of the identity management approach [Al16]. Besides a comparison with the e-mail encryption scheme PGP, no further details are given about the exact mechanisms of trust establishment. Using the vision of self-sovereign data management described in that blog post, research and practice have since then more clearly defined the components of an SSI system. One of the most important facets of SSI is the promise of interoperability of identity information across a variety of domains. At the heart of SSI's interoperability initiatives lies the W3C verifiable credentials data model. This standard document is also the source of the trust model, which is most often used to explain the core mechanisms of SSI:

An issuer creates a verifiable credential (VC) and sends it to the wallet application of a holder, which now can determine to send a presentation of that credential to a verifier. To accept the credential as valid, the verifier needs to trust the issuer to provide truthful information during the issuance process. Additionally, all parties must trust a data registry for the provision of identifiers and schemas.

The Trust Over IP (ToIP) Foundation, a Linux Foundation project, gives recommendations on how this trust between the actors can be established. The goal of the foundation is to provide a solution for the internet's missing trust layer [Tr20]. Its main contribution to that goal is reflected in the so-called ToIP stack. It aligns SSI's main technical components, decentralized identifiers, digital wallets, and VCs, in a layered architecture. Each layer is supported by specific governance frameworks, which serve as the regulatory foundation of trust thereon [Da19]. In addition to the three technical layers, the ToIP stack provides an overarching fourth layer, which describes the application ecosystem the SSI implementation is embedded. Governance frameworks at this layer need to regulate technical and usability standards according to the requirements of the use cases in a specific application domain [Re21]. The trust created at this layer stems from the authoritative position of governing actors to assign roles, rights, and responsibilities in such domain. For SSI to be able to provide trust in digital public services, the organization of private and public actors around existing and new regulatory provisions is necessary. Research in this direction is still in its infancy, e.g., defining only the contents of physical and digital credential governance [RPA23].

2.3 The rule of law as the basis for trust in the public sector

When the arguments presented above all come together, we must answer the question, of which role the state can play in creating trust in digital spheres. It is crucial to distinguish between the various categories of statehood that generate the citizens' trust, be it the political sphere, the public administration, or the law. In Germany, the prevailing focus of digitization is on interacting with public authorities. Looking at the role of public

administration from a functionalist perspective, its main output is legally binding decisions. Following Max Weber's classical notion, this role is played through a rationalization mechanism. This means that all public activities can be managed according to the principle of expediency. Thus, it is particularly possible and desirable to fully automate routine procedures. Automated decisions based on the simple application of legal norms can be expected to be accepted by citizens, provided that such decisions bring the same degree of legal reliability as non-automated ones [SA23]. Still, this raises the question of how trust, the state, and the law are linked.

Trust in public institutions is not solely based on the state's power as an authority. Rather, trust in *what the state does* is only achieved when the logic of an interpersonal relationship of trust (see 2.1) is reproduced. The willingness to accept information asymmetry and the belief that there is no disadvantage arising from sharing personal data is based on the ability to penalize improper actions. Thus, trust in public institutions is based on a state under the rule of law. A state alone is by no means a sufficient basis for the development of trust; democratic principles and the recognition of legal provisions are required as well [Sz03]. Only with the institutionalized limitation of the state's power, trust in a state can be fully established. This suggests that it is not so much the dynamic framework of politics and government that is the anchor of trust in the state, but rather the permanent structures of the administration and its commitment to the law. This observation outlines a prerequisite for the emergence and perpetuation of trust. In addition other supporting factors are sufficient requirements for the trust mechanism. Some of these elements are highlighted in the following section.

2.4 The link between trust and user experience

This chapter examines the relationship between user experience and trust in information systems. Research in this direction frequently mentions usability and user experience as key factors influencing trust in digital systems, e.g. [Ba17]. In addition, usability is also found to be an even more important factor in situations where users *must* use a particular system or their only alternative is not to use it, such as in governmental contexts [AK12]. In cases where other alternatives to a particular system are available for use, the reputation of the system provider is often found to be of greater importance in influencing trust [AK12]. Furthermore, several dimensions and guidelines describe the impact of user experience on trust. Dimensions provide abstract considerations, while guidelines offer concrete instructions and design patterns.

Zieglmeier and Lehene [ZL21] identified three different dimensions in an extensive literature review: purpose, process, and performance. Wang and Emurian [WE05], Seckler et al. [Se15], and Backhaus [Ba17] also made categorizations in this context, most of which can be assigned to the dimensions of Zieglmeier and Lehene [ZL21]. In contrast to the other studies, Seckler et al. [Se15] investigated not only the influence of usability on

trust but also usability factors that generate mistrust. It is important to note that meeting these criteria does not guarantee trust but leads to users not distrusting the system [Se15].

Purpose: According to Zieglmeier and Lehene [ZL21], this dimension describes the purpose of the system, which depends on the intended use. Three trustworthiness factors in this dimension convey users' perception of the designer's intentions during system interaction [ZL21]. Benevolence refers to users' belief in the system's care and respect for their data and actions. Credibility is established when the system is perceived as honest and sincere. Perceived security is solely determined by users' perceptions, shaping their sense of security. Backhaus [Ba17] adds that perceived data security and privacy play an important role in user trust, as they can have serious consequences. Accordingly, users with special privacy and security requirements have lower trust in systems. In general, lack of privacy is often cited as a factor contributing to distrust [Se15].

Process: This dimension outlines the system functionality based on users' perception of the system design's appropriateness for its stated purpose [ZL21]. Integrity plays a vital role, as it reflects users' impressions of the system's underlying values. Predictability is crucial for users, as they seek consistency in the system's behavior and design, enabling them to predict its future actions. Transparency is important in informing users about the system's purpose and functionality. Familiarity with the system helps users to better understand and interact with it. Effective communication by the system actively engages users. Usability is another critical factor, encompassing the quality of the tool in enabling users to use it. Backhaus [Ba17] mentioned that good usability enhances trust by enabling easy operation, conveying security, and evoking positive emotions.

Performance: This dimension maps the degree of the system's ability to solve tasks by encompassing factors, that collectively influence users' assessment of the system's task-solving capabilities and overall satisfaction [ZL21]. Users evaluate the system based on the factor competence, which indicates the system's capability to achieve tasks efficiently and with high quality. Wang and Emurian [WE05] and Seckler et al. [Se15] add that structure and accessibility of displayed information ensures that users can easily find the information they need. The reliability of the system also plays a crucial role in fostering trust, as the consistency of the functions contributes to its predictability [ZL21]. Furthermore, low reliability can lead to reduced validity, affecting users' trust. Thereby, validity refers to the extent to which the system completes tasks according to the user's intentions. Backhaus [Ba17] emphasizes in the context of the performance dimension that a lack of trust implies that the system has no benefit for the user and does not deliver what it promises. It is further argued that trust increases expectations of system performance [Ba17].

Graphic Design: In addition to the dimensions already mentioned, Wang and Emurian [WE05] and Seckler et al. [Se15] covered another dimension, which refers to the visual factors that create a first impression on users [Ba17].

In several contributions, recommendations for the design of user interfaces are formulated or these are summarized as the result of a literature review [Sh00], [WE05], [Se15], [Fa17] [ZL21]. However, some of them focus primarily on e-commerce use cases. Therefore, only the guidelines that are also suitable for a government use case were considered for this work. They can serve as a guide for designing user interfaces that foster trust and enhance the user experience of digital public services.
A frequently mentioned recommendation relates to the visual design and the graphic aspect of user interfaces (UI). Here, it is often emphasized that trust is increased by considering aesthetic design [WE05], [Se15], [ZL21]. Therefore, it is recommended to follow a clear design structure [WE05], to maintain consistency in design, and to follow established design patterns and metaphors to evoke users' familiarity [ZL21]. Through the latter, the credibility dimension is also addressed, in the sense of aligning the interface with users' expectations and mental models [ZL21]. Furthermore, it is suggested to display organization-related information, such as the logo [WE05], [Se15]. In addition, typography and color schemes can positively influence users' trust [Fa17], [ZL21].

In terms of navigation, it is recommended to ensure ease of navigation and user guidance [WE05], [Fa17], [ZL21]. This component seems to be crucial for trust and serves the overall usability of the application [Fa17], [ZL21]. Another factor in this regard is to focus on the ease of use, to make the application easily accessible, and to reduce the cognitive effort required [ZL21]. Additionally, there must be a focus on learnability by clarifying the system functionality [ZL21]. In terms of transparency and predictability, it is recommended to provide comprehensive, correct, consistent, and up-to-date information about the system's state, available actions, potential risks, and limitations [Se15], [ZL21]. Furthermore, privacy and security policies should be easily accessible and enforceable [Sh00], [WE05], [Se15].

To enhance perceived security, it is recommended to acquire certifications from trusted third parties and display these seals of approval or certificates [Sh00], [WE05], [Se15], [ZL21]. This suggests an ethics code or value system and thus can improve users' sense of security [ZL21]. In addition, it is suggested to use the relevant web address and domain name [WE05], [Se15]. It is also recommended to provide other security sign cues or display security details, such as lock symbols, encryption, data verification, and data usage [Se15], [ZL21]. These aspects raise the users' awareness and increase their perceived security [ZL21].

3 Case analysis

3.1 Case description

The public service used for analysis in this study comprises the procedures for a so-called citizens' initiative (CI, German “Bürgerbegehren”) of Dresden, the capital of the German state of Saxony. A CI is an instrument of direct democracy in Germany at the municipal level. It is a request by citizens to the municipal council to hold a citizens' referendum (“Bürgerentscheid”). The CI can be used, e.g., to correct city council resolutions or to enforce measures of general interest. The legal basis is given by § 24 and § 25 of the Saxon Municipal Code (“Sächsische Gemeindeordnung”).

A CI can be divided into three subsequent steps. First, during initiation, two to three people are involved in the application for the CI with the city administration, which needs to check for formal criteria. These are the identity and the minimum age of the CI’s counterpersons as well as a budget plan. After successful initiation, members of the CI can start to gather signatures of supporters. To reach the next stage in the process, the CI needs to be able to convince at least 5 % of Dresden’s citizens to sign. Endorsers must have lived in Dresden for at least 3 months, be at least 18 years old, and have EU citizenship. During the last stage of a CI, the manually gathered signatures are sent to the municipal administration for another check of formal criteria. Civil servants manually count each declaration of support and cross-check them with data in the electronic citizens' register. If all formal criteria are met, the city council decides either to enforce the CI’s claims directly or to plan a referendum.

Currently, the electronic processing of CIs is prohibited in the state of Saxony. In the scope of the research program this study is embedded into, the processes for initiation and support of a CI have been prototypically implemented using SSI technology for research purposes. In this setup, the city administration offers a portal for conducting CIs. Using SSI wallets, initiators and supporters of the CI can provide their data from trustworthy issuers in a machine-readable form, allowing for automatic verification.

3.2 Verifiable credentials and public governance

In its current state, the analyzed digital service can be accessed by three groups of actors: initiators and supporters of CIs as well as municipal staff, the latter of which was out of scope for this study. Everyone must provide specific information to the service for authentication and the legal processing of a CI. For this purpose, VCs are to be presented by each actor using a personal wallet application. These credentials need to be obtained first by using a second issuing application also offered by the city of Dresden. After the presentation of the necessary VCs, the CI system verifies the semantic correctness of the included data by reference to a credential type, which needs to be specifically configured

beforehand. Similarly, the identifier of the issuing organization of the credential must be added to a local whitelist, to be accepted. For initiators, two valid options are presented for the transmission of their legal identity and age.

The first is an electronic version of a confirmation of registration following § 24 of the Federal Act on Registration ("Bundesmeldegesetz"). German municipalities issue this document type to citizens after registration therein. Since there is no semantic standard nor a list of public keys used by German municipalities for the signature of VCs, the municipal administration of Dresden can at this stage only rely on its infrastructure to identify valid credentials.

The second option, which is also available to supporters of the CI, is a planned verifiable credential based on data available to the municipality through access to the citizens' registry. It is planned to be available to citizens authenticating themselves with the national electronic identity solution. The corresponding legal basis for the issuance of this credential can be found in § 10 of the Federal Act on Registration, which itself refers to the right of access by the data subject as proclaimed in Art. 15 of the GDPR. During the timeframe of this study, the systems for the issuance of this credential were still in development. However, it is an example of how a municipality can use federal as well as European Union law to provide trustworthy information as input to their digitization efforts. Still, to avoid abuse, legal foundations must be created for the practical use of this registry credential. This includes the definition of formal administrative processes in the citizens' office and socio-technical peculiarities such as the revocation of credentials following a change of its source data in the registry. This requires ongoing cooperation between the IT and functional departments in Dresden's municipal administration, but also with technology providers for SSI and public registry software.

In both cases, the municipality of Dresden acts as both the source as well as verifier of the accepted credentials, turning SSI's decentralized "trust triangle" into a closed system. This is a natural result of the goal of providing reliable information from a trusted source for administrative processes and the lack of an overarching governance framework, making issuing municipalities identifiable electronically.

3.3 UX and trust in SSI

To foster a good UX and trust in an SSI-based use case, it is important to not solely focus on the digital service website (in this case the CI platform) but to widen the view and consider the wallet in process and UI design. Taking this holistic view and considering the trustworthiness factors mentioned in section 2.4 will be the next step in developing the CI pilot. Therefore, in this section, we will provide recommendations based on the guidelines regarding the interface design.

Some recommendations apply in general, regardless of which process step a user is in. For instance, to ensure transparency and predictability, users should be provided with

comprehensive, correct, consistent, and up-to-date information [Se15], [ZL21]. Furthermore, the ease of use of the system should be supported by intuitive navigation [WE05], [Fa17], [ZL21] and step-by-step instructions to provide user guidance [Se15], [ZL21] and to convey prerequisites the digital service requires [Sh00]. Additionally, user actions should result in appropriate visual feedback from the system [ZL21]. At each step of the process, users should have the option to cancel the interaction or undo their action so as not to give them the impression that they are being forced to do something they do not want to do [Se15]. To credibly convey to users that it is the city of Dresden that offers this digital service, it is important to use the city's official logo, corporate identity, and appropriate domain [WE05], [Se15]. Giving users the option to reach out to a contact person in the relevant department, e.g., via a chat in their wallet, could also help foster trust [WE05], [Se15].

The process of initiating or supporting a CI via the website based on SSI starts with a contact initiation. Therefore, the user scans a QR code with their wallet or clicks a button (deep link) to initiate it. As a result, the user gets a contact request in their wallet. Regarding this request, it is important to indicate who the counterpart is (City of Dresden) and whether it is trustworthy, e.g., by a green icon like a check mark, if Dresden has a relevant certificate [Sh00], [WE05], [Se15], [ZL21]. Further information regarding the contact and the verification should be available for users [Sh00], [WE05], [Se15], [ZL21]. Based on the security information, users should be recommended action [ZL21].

If the user approves the contact request, the verifier (city of Dresden) automatically sends a proof request to the user's wallet. Here, only the data should be requested that is needed to initiate or support a CI, and the user should be able to decide if they want to share them or not [Se15]. Hereby, the security cues in terms of the contact (city of Dresden) should also be visible [Sh00], [WE05], [Se15], [ZL21]. In addition, for users to make informed decisions, both the website and the wallet should clearly state what data is needed, for what reason, and what happens to the data afterward [Sh00], [WE05], [Se15]. Further information could be provided to users in the form of easily understood and accessible privacy and security policies [Sh00], [WE05], [Se15].

For users to support a CI, information regarding its duration, contact persons, and names of the initiators must be displayed centrally to foster trust [Se15], [ZL21]. Furthermore, the support of a CI must be reversible, and this option must also be made visible to the users [Se15].

4 Discussion and conclusions

In this paper, we address the role of trust as both a precondition and desired effect in public sector digitization. We aim to shed light on the mechanisms underlying the often-cited trust-enhancing properties of SSI. To that end, we consulted a wide array of trust literature to identify the factors that play into these mechanisms on two levels of analysis: a) the

rule of law in public services and its influence on the design of verifiable credentials, as well as b) user experience effects on the perceived trustworthiness of the solution. In the second step, we used these factors as a lens for the analysis of the case of a digital citizens' initiative utilizing SSI.

On a theoretical level, we highlight how trust in a digital public service depends on both the design of the technical subsystem as well as organizational measures and the institutional framework. We show that contemporary SSI technology only covers partial aspects of these factors. We encourage scholars to further research the interplay between wallets and the digital services, they are utilized in.

Practitioners in public service digitization can benefit from our research in analyzing the constraints for the use of SSI more holistically. This includes the integration of relevant stakeholders in digitization projects. Further, we give guidelines for the definition of governance frameworks and the design of a trust-evoking user experience, which can be adapted to other cases.

As our research presents a single case, our findings come with the limitation that they may be only applicable to the German public context. Also, the rapid development of SSI needs to be considered. Future research could build on our analysis to formalize the identified factors for building trust and conduct qualitative measurements of trust in cases, where our identified factors are being used as a design guideline.

The project on which this publication is based was funded by the German Federal Ministry of Economics and Climate Protection (Grant number 01MN21001A).

References

[AK12] Acemyan, C. Z.; Kortum, P.: The Relationship Between Trust and Usability in Systems. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 1/56, pp. 1842–1846, 2012.

[Al16] Allen, C.: The Path to Self-Sovereign Identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html, accessed 15 Apr 2020.

[Ba17] Backhaus, N.: Nutzervertrauen und –erleben im Kontext technischer Systeme. Technische Universität Berlin, 2017.

[BJS10] Beldad, A.; Jong, M. de; Steehouder, M.: How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in Human Behavior 5/26, pp. 857–869, 2010.

[Bo12] Bouckaert, G.: Trust and public administration. Administration 1/60, pp. 91–115, 2012.

[Ca05] Cameron, K.: The Laws of Identity. Kim Cameron's Identity Weblog. https://www.identityblog.com/?p=352, accessed 11 Aug 2020.

[Ca16] Carter, L. et al.: Citizen Adoption of E-Government Services: Exploring Citizen

Perceptions of Online Services in the U. Information Systems Management 2/33, pp. 124–140, 2016.

[Da19] Davie, M. et al.: The Trust Over IP Stack. https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0289-toip-stack, accessed 24 Feb 2021.

[Eh21] Ehrlich, T. et al.: Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. HMD Praxis der Wirtschaftsinformatik, 2021.

[Eu21] European Commission: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, Brussels, 2021.

[Fa17] Faisal, C. M. N. et al.: Web Design Attributes in Building User Trust, Satisfaction, and Loyalty for a High Uncertainty Avoidance Culture. IEEE Transactions on Human-Machine Systems 6/47, pp. 847–859, 2017.

[JRA22] Jürgenssen, O.; Richter, D.; Anke, J.: Selbstbestimmte digitale Identitäten in der Smart City. Potenziale und Grenzen. In (Köhler, T. et al. Eds.): Gemeinschaften in Neuen Medien. 25. Workshop GeNeMe '22 Gemeinschaften in Neuen Medien. TUDpress - Verlag der Wissenschaften, Dresden, pp. 148–158, 2022.

[LKA21] Laatikainen, G.; Kolehmainen, T.; Abrahamsson, P.: Self-Sovereign Identity Ecosystems: Benefits and Challenges: 12th Scandinavian Conference on Information Systems. Living in a digital world? Association for Information Systems, Orkanger, Norway, 2021.

[LMT15] Lankton, N.; McKnight, D. H.; Tripp, J.: Technology, Humanness, and Trust: Rethinking Trust in Technology. Journal of the Association for Information Systems 10/16, pp. 880–918, 2015.

[MCC98] McKnight, D. H.; Cummings, L. L.; Chervany, N. L.: Initial Trust Formation in New Organizational Relationships. The Academy of Management Review 3/23, pp. 473–490, 1998.

[MF88] Milliman, R. E.; Fugate, D. L.: Using Trust-Transference As A Persuasion Technique: An Empirical Field Investigation. The Journal of Personal Selling and Sales Management 2/8, pp. 1–7, 1988.

[Re21] Reed, D.: SSI governance frameworks. In (Preukschat, A.; Reed, D. Eds.): Self sovereign identity. Decentralized digital identity and verifiable credentials, pp. 248–270, 2021.

[Ro98] Rousseau, D. M. et al.: Not So Different After All: A Cross-Discipline View Of Trust. Academy of Management Review 3/23, pp. 393–404, 1998.

[RPA23] Richter, D.; Praas, C. R.; Anke, J.: Beyond Paper and Plastic. A Meta-Model for Credential Use and Governance: ECIS 2023 Research Papers, 2023.

[Sc23] Schäfer, F. et al.: Unleashing The Potential of Data Ecosystems: Establishing Digital Trust through Trust-Enhancing Technologies: ECIS 2023 Research Papers, 2023.

[Se15] Seckler, M. et al.: Trust and distrust on the web: User experiences and website characteristics. Computers in Human Behavior 45, pp. 39–50, 2015.

[Se22] Sedlmeir, J. et al.: Transition pathways towards design principles of self-sovereign identity: ICIS 2022 Proceedings, p. 4, 2022.

[Sh00] Shneiderman, B.: Designing trust into online experiences. Communications of the ACM 12/43, pp. 57–59, 2000.

[Sz03] Sztompka, P.: Trust: A Sociological Theory. Cambridge University Press (CUP), New York, 2003.

[TPH14] Tenzer, H.; Pudelko, M.; Harzing, A.-W.: The impact of language barriers on trust formation in multinational teams. Journal of International Business Studies 5/45, pp. 508–535, 2014.

[Tr20] Trust Over IP Foundation: Introducing The Trust over IP Foundation. https://trustoverip.org/wp-content/uploads/sites/98/2020/05/Introducing-The-Trust-over-IP-Foundation-V1.pdf, accessed 31 May 2023.

[vB03] van de Walle, S.; Bouckaert, G.: Public Service Performance and Trust in Government: The Problem of Causality. International Journal of Public Administration 8-9/26, pp. 891–913, 2003.

[WE05] Wang, Y. D.; Emurian, H. H.: An overview of online trust: Concepts, elements, and implications. Computers in Human Behavior 1/21, pp. 105–125, 2005.

[ZL21] Zieglmeier, V.; Lehene, A. M.: Designing Trustworthy User Interfaces. In (Buchanan, G.; Davis, H.; Muñoz, D. Eds.): 33rd Australian Conference on Human-Computer Interaction. ACM, New York, NY, USA, pp. 182–189, 2021.

Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 55

Predictive Policing

Eine kritische Bestandsaufnahme am Beispiel der Dimension Raum

Caroline Mehner[1], Yannick Fernholz[2], Benjamin Fabian[3], Tatiana Ermakova[4]

Abstract: Dieser Beitrag bietet eine kritische Bestandsaufnahme des Predictive Policing am Beispiel der Dimension Raum. Unter Berücksichtigung der aktuellen Entwicklungen des europäischen AI-Acts werden Maßnahmen und Methoden beleuchtet und aus ethischer Perspektive reflektiert und diskutiert. Das methodische Fundament bildet eine systematische Literaturanalyse anhand einer Korpusanalyse zu Techniken des Predictive Policing. Es werden vorhandene wissenschaftliche Vorarbeiten vorgestellt und ethische Fragestellungen im Zusammenhang mit der Verwendung von Daten für Predictive Policing untersucht. Der Beitrag eröffnet wichtige Fragen, die es weiter zu erforschen gilt. Die aktuellen Entwicklungen im Rahmen des AI-Acts bestätigen die Relevanz der Thematik.

Keywords: Predictive Policing, Raum, Künstliche Intelligenz, Literature Review, KI-Ethik

1 Einleitung

Es ist eine kleine Sensation: „MEPs ready to negotiate first-ever rules for safe and transparent AI" [YO23]. Unlängst verhandelt das Europäische Parlament über Regeln für sichere und transparente Künstliche Intelligenz. Davon sind neben der Erhebung von biometrischen Echtzeitdaten auch Methoden zur biometrischen Kategorisierung „using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation)" betroffen. Besonders interessant: Der Einsatz von Predictive Policing

[1] Universität Leipzig, Ritterstraße 26, 04109 Leipzig, caroline.mehner@googlemail.com
[2] Weizenbaum Institut e.V., Hardenbergstraße 32, 10623 Berlin, yannick.fernholz@weizenbaum-institut.de
[3] EDIH pro_digital TH Wildau, Hochschulring 1, 15745 Wildau, benjamin.fabian@th-wildau.de
[4] HTW Berlin, Treskowallee 8, 10318 Berlin, tatiana.ermakova@htw-berlin.de

doi:10.18420/rvi2023-015

Systemen, die sich auf Daten des „profiling, location or past criminal behaviour" beziehen, wurde auf die Liste der zu bannenden KI-Praktiken gesetzt [YO23].

Inwieweit aber haben die Entwicklungen im Zusammenhang mit dem AI-Act Einfluss auf bestehende Praktiken im Zusammenhang mit Predictive Policing? Der Artikel führt dazu zunächst in Methoden des Predictive Policings ein eröffnet die aktuelle Diskussion im Zusammenhang mit dem europäischen AI-Act. Im Zuge dessen werden Maßnahmen und Methoden prediktiven Polizierens insebsondere unter dem Aspect der „location" systematisiert dargestellt und auf ethische Fragestellungen hin geprüft. Basierend auf einem Literature Review nebst Korpusanalyse zu Techniken des Predictive Policings werden wissenschaftliche Vorarbeiten vorgestellt sowie ethischen Fragestellungen im Zusammenhang mit der Verwertung von Daten für Predictive Policing nachgespürt. Kapitel 2 stellt die begriffliche und inhaltliche Grundlage für den weiteren Verlauf dar, die in Kapitel 3 durch die Einführung in das Systematic Literature Review methodisch ergänzt wird. Kapitel 4 diskutiert die inhaltlichen Ergebnisse der Recherche anhand der Dimension Raum, im folgenden Kapitel 5 werden daraufhin ethische Implikationen des Predictive Policing reflektiert.

2 Predictive Analytics und Predictive Policing

Die methodische und technische Grundlage für Predictive Policing als konkreten Anwendungsfall für die Vorhersage und Prävention von Kriminalität stellt *Predictive Analytics* dar.

Predictive Analytics umfassen datenbasierte Techniken zur Vorhersage (insbesondere menschlichen) Verhaltens. Der Fokus liegt dabei auf der Sammlung und Bereitstellung größerer Datenmengen sowie deren Auswertung. Die datengestützte Auswertung und Beurteilung von Informationen sind zwar seit jeher Grundlage menschlicher Interaktion. Jedoch erhöht die im Informationszeitalter gestiegene Verfügbarkeit von Daten auch deren Sammlung mit dem Ziel, sie so in Beziehung zu setzen, dass sich daraus allgemeingültige Aussagen sowie Vorhersagen zukünftiger Ereignisse ableiten lassen [SK11, Fi14]. Auch im Zusammenhang polizeilichen Agierens haben Techniken des Data Minings und datengestützter und prädiktiver Analysen zugenommen. Die zum Einsatz kommenden Methoden werden unter dem Begriff des Predictive Policing gefasst.

2.1 Predictive Policing

Predictive Policing bezeichnet demnach die datengestützte Analyse zur Bewertung polizeilicher Interventionsmaßnahmen, die Bewertung potenzieller Gefahrenlagen sowie von Präventionsmaßnahmen. Ziel des Einsatzes prädiktiver (und vorbeugender) Methoden in der Polizeiarbeit ist „[…] to work more proactively with limited resources

[...] to develop effective strategies that will prevent crime or make investigation efforts more effective" [Pe13].

Zugleich werden sie auch als „[…] ein technisches Hilfsmittel zur Unterstützung der polizeilichen Intuition und des kriminalistischen Gespürs" [Kn16, S. 6] erachtet. Diesem Zitat folgend, erführe Polizeiarbeit also lediglich eine technische Erweiterung. Predictive Policing ziele auf eine datengestützte Erhöhung der Glaubwürdigkeit, indem „[a]lles, was intransparent ist, was un- oder nur halb bewusst geschieht, […] explizit gemacht werden [muss]"[Kn16,S.6].
Als Datengrundlage für Predictive Policing dienen polizeiliche Vorgangsdaten, häufig in Verbindung mit nicht-polizeilichen Daten (z.B. Daten zur Wetterlage, der Wohnlage oder der Entfernung zur nächstgelegenen Autobahn). Für deren weitere Analyse ist es also wichtig, dass alle ausgewählten Daten geografisch referenziert werden können, sodass ein einheitlicher, maschinell verarbeitbarer Datensatz vorliegt [Bo17]. Insbesondere die Möglichkeit ihrer geographischen Referenzierung macht daher die Dimension Raum für Maßnahmen des Predictive Policings zum geeigneten und im Weiteren zentralen Untersuchungsgegenstand.

Datengestützte polizeiliche Interventionen sind vor allem aus den USA und hier im Zusammenhang mit Gangkriminalität bekannt. Mit [Bs20] liegt überdies eine „Bestandsaufnahme für den deutschsprachigen Raum" vor. Eine weitere Quelle stellte eine Studie der Bertelsmann Stiftung von 2016 über den Einsatz von Techniken Predictive Policings in einzelnen Bundesländern Deutschlands dar [Kn16], die die Bestandsaufnahme für Deutschland ergänzt.

Mittels einer systematischen Literaturanalyse (systematic literature review) wurde daher zunächst die vorhandene Literatur im Feld bis 2021 untersucht und Praktiken und Mechanismen in Anwendung exemplarisch vorgestellt.

2.2 Zum polizeilichen Inventar

Maßnahmen und Methoden im Bereich Predictive Policing adressieren unterschiedliche Kategorien polizeilicher Interessensgegenstände. Eine umfangreiche Quelle stellt die von [Pe13] vorgelegte Studie dar, die, wie im Literature Review bestätigt wird, Ausgangspunkt einer Vielzahl ihr historisch folgender Untersuchungen im Feld ist. Sie wurde daher als Startpunkt identifiziert und infolge einer immanenten Recherche zugrundeliegender Quellen als geeignete Referenz für die Analysen bestätigt.

Die folgende Tabelle orientiert sich an den nach [Pe13] zusammengestellten Informationen, die als Grundlage eines *Law Enforcements* und daraus folgend der Durchsetzung von Maßnahmen zur Verbrechensbekämpfung dienen.

Es handelt sich dabei um eine aus der Literatur zusammengeführte Auswahl an Methoden, die im Zusammenhang mit Predictive Policing zum Einsatz kommen.

Problem	**Predictive Analytics**
Predicting Crimes: Identify areas at increased risk	
Using historical crime data	Advanced hot spot identification models, risk terrain analysis
Using a range of additional data (e.g., 911 call records, economics)	Regression, classification, and clustering models
Accounting for increased risk from recent crimes	Near-repeat modeling
Identifying geographic features that increase the risk of crime	Risk terrain analysis
Predicting Offenders	
Finding a high risk of violent outbreak between criminal groups	Near-repeat modelling (on recent intergroup violence)
Identify individuals who may become offenders	Regression and classification models using risk factors
Prediction Perpetrator Identities	
Identifying suspects using a victim's criminal history or other partial data (e.g., plate number)	Computer-assisted queries and analysis of intelligence and other databases
Determining which crimes are part of a series (i.e., most likely commited by the same perpetrator)	Statistical modeling to perform crime linking
Finding suspects using sensor information around a crime scene (GPS tracking, license plate reader)	Computer- assisted queries and analysis of sensor database
Predicting Crime Victims	
Identifying groups likely to be victims of various types of crime (vulnerable people)	Advanced models to identify crime types by hot spot, risk terrain analysis

Identifying people at risk for victimization (e.g., people engaged in high-risk criminal behavior)	Advanced data mining techniques used on local and other accessible crime databases or identify repeat offenders at risk
Identifying people at risk of domestic violence	Computer- assisted database queries of multiple databases to identify domestic and other disturbances involving local residents when in other jurisdictions

Tab. 1: Übersicht von Maßnahmen im Bereich des Predictive Analytics [Pe13]

Die Tabelle verdeutlicht einen ersten Zugang zum Feld und bietet eine Übersicht potenzieller, im folgenden Systematic Literature Review untersuchten Techniken, die bereits auf die Relevanz der Dimension Raum für Maßnahmen im Predictive Policing hindeutet.

3 Systematic Literature Review

Der methodische Zugang des Systematic Literature Reviews beschreibt eine zeitgemäße, systematisch betriebene Literaturrecherche, um das Feld plausibel zu eröffnen. Forschungsfragen können spezifischer und Kriterien geleitet und diskutiert werden. So werden für einen Schwerpunkt relevante Quellen, umfänglich erschlossen und „[…] a vital contribution to the relevance and rigour of research" [Br09, S. 4] geleistet. In verschiedenen Schritten werden systematisch Vorwärts- sowie Rückwärtssuchen [Sc17, S. 7] vorgenommen, um die inhaltliche Felderschließung durch Forschende auf Plausibilität und Richtigkeit zu prüfen und um nachzuvollziehen, anhand welcher Kriterien genutzte Literatur ausgewählt wurde [Br09, S. 4].

In der folgenden tabellarischen Darstellung wurden die Kategorien nach [Bo16, S. 101f.] zugunsten des Fokus auf Predictive Policing beschränkt. Die Methodik der Literaturrecherche und Qualitätsbewertung musste leider informativ verkürzt werden. Der Bewertung zugrunde lag aber zunächst eine allgemeine Schlagwortsuche in gängigen Suchmaschinen und dann die thematische Begrenzung vorgenommen. Insgesamt wurden im Rahmen des Literature Reviews nach dessen Reduktion auf die unter 2.2. identifizierten, polizeilichen Techniken im Raum 38 Artikel analysiert, unter den Schlagworten „Geographic Profiling", „Hot Spot (Identification)", „Risk Terrain Analysis" sowie „Spatiotemporal Analysis".

Arbeitsschritt	**Kurzbeschreibung**
Hintergrund (*Background*)	Hintergrund des Reviews: Analyse von Techniken und Methoden für das Predictive

	Policing unter der Berücksichtigung der Dimension „Raum“
Ziele (*Objectives*)	Ziele und Fragestellungen, die erarbeitet werden sollen: - Techniken im Zusammenhang mit Predictive Policing unter der Berücksichtigung räumlicher Repräsentation; inwiefern sind sie im Korpus der analysierten Literatur vertreten? - Kommen sogar verschiedene Techniken zum Einsatz, wenn ja, gibt es zu berücksichtigende Besonderheiten?
Auswahlkriterien (*Criteria for inclusion and exclusion of studies*)	Kriterien, die dem Ein- oder Ausschluss von Literatur dienen sollen: - Beschränkung auf Begriffe, die in der von [Pe13] vorgeschlagenen Systematik verwendet wurden - Beschränkung auf die Dimension Raum, räuml. Repräsentation
Studienarten (T*ypes of studies*)	Arten von inkludierten Studien: - Es wird hier im engeren Sinne nicht von Studien zu sprechen sein, da im Korpus sowohl Literature Reviews als auch den Gegenstand essayistisch beschreibende Publikationen berücksichtigt werden - Den Publikationen ist gemein, dass sie peer-reviewed wurden - Alle mittels Stichwörter identifizierten Publikationen Gegenstand der Untersuchung
Bestandsdefintion (*Types of populations*)	Refokussierung des Bestands andhand der Forschungsfragen: - Erfolgt immanent in der Beschreibung und infolge einer Methodenkritik
Bestandsbegrenzungen (*Types of interventions or exposure*)	- Die Bestandsbegrenzung erfolgt anhand der vorgenommenen und dokumentierten Einschränkungen vor Hintergrund der Forschungsfragen

Erwartungshorizont (*Types of outcome measures*)	- Es sollen Techniken und Methoden des Predictive Policings im Zusammenhang mit räumlichen (Interventions-)Maßnahmen nachvollzogen werden - Ggf. sollten weitere Einschränkungen und Differenzierungen vorgenommen werden - Es sollen im Zusammenhang mit dem Korpus ersichtlich werdende Herausforderungen herausgearbeitet werden.
Kontext (*Setting/context*)	Einschränkung des Kontextes: - Predictive Policing wird auf den Kontext räumlicher Intervention beschränkt.

Tab. 2: Review Protocol Template zum Korpus "Predictive Policing"

4 Predictive Policing am Beispiel der Dimension Raum

Im sogenannten AI-Act erfährt der Aspekt des Einsatzes von Predictive Policing Systemen die präzisierende Ergänzung: „based on profiling, location or past criminal behaviour". Location oder Raum als Untersuchungsgegenstand, so konnte im Literature Review gezeigt werden, kommt im Zusammenhang mit vorhersagender Polizeiarbeit eine besondere Relevanz zu: Die Fokussierung auf das Thema Raum als Untersuchungsgegenstand und zugleich Handlungsrahmen polizeilichen Wirkens sowie auch das wissenschaftliche Interesse an einer *geography of crime* ist nicht neu [Va17, S. 1]. Die Analyse der Entität Raum im Zusammenhang mit Verbrechen und Kriminalität sowie die Kriminalistik als strukturierter Zugang zu den Ursachen und dem Wesen von Verbrechen selbst findet ihren Anfang in der Mitte des 19. Jahrhunderts. In den USA erfuhr hier insbesondere die strukturierte Auswertung von (Kriminalitäts-)Räumen seit den 1970er Jahren Relevanz. Die USA (und wie zu zeigen sein wird auch der deutschsprachige Raum) haben ihr Programm seither systematisch erweitert [Ta16, S. 7f.; AP 20, S.60].

Die hier zusammengestellte Übersicht gibt einen ersten Eindruck der gängigsten Methoden und Zugänge amerikanischer Polizeiarbeit seit den 1970er Jahren:

Standard model of policing *Herkömmliche Polizeiarbeit*	***Reaktive Gesetzesdurchsetzung*** "The standard model of policing uses law enforcement in a reactive manner." ● Analysemethoden dienen der zeitlich- und räumlich effizienten Planung des Einsatzes von Polizeikräften
Community policing *(Sozial-)Bereichs-Polizeiarbeit*	***Einbezug lokaler Akteure*** "Community policing strategies benefit from partnership and collaboration of the community to understand and solve the problem." ● Anwohner:innen und Geschäftstreibende werden in die Planung und Durchführung der Polizeiarbeit einbezogen
Disorder policing *Polizeiarbeit an identifizierten Gefahrenorten*	***Proaktive Polizeiarbeit in Gefahrenlagen*** „Disorder policing or broken window policing is applying strict law enforcement procedures to minor offences to prevent happening of more serious crimes." ● Analysemethoden dienen der Bewertung von Maßnahmen zur Störung von Verbrechen
Problem-oriented policing *Problemorientierte Polizeiarbeit*	***Präventives, problembasiertes Handeln*** "In problem-oriented policing the goal is diagnosing problems within the community and developing appropriate responses which solve the cause of the problems." ● Analysemethoden werden zur Bewertung von Ursachen und Maßnahmen eingesetzt
Hotspot policing *Schwerpunktpolizieren*	"Hotspots policing is a location-based policing in which the police resources are allocated to different areas proportional to crime rate of each area." ● Analysemethoden dienen dem Finden und Identifizieren von Hotspots

Tab. 3: amerikanische Polizeiarbeit seit den 1970er Jahren (Übersicht), eigene Darstellung mit Erläuterungen basierend auf [Ta16, S. 8]

4.1 Exemplarische Darstellung von Techniken

[AP20] unterscheiden für die Polizeiarbeit zwischen exploratory (explorative) und predictive (prädiktive) analytics (Auswertung). Während explorative Zugänge eher zur retrospektiven Auswertung krimineller Aktivitäten und mittels Mappings und strategischer Auswertung der Identifikation potenzieller Gefahrenorte oder Hotspots dienten, nutzten prädiktive Analysen bereits identifizierte Orte, um „forecasting models on micro-locations of crimes called prospective or dynamic hot spots“ zu erstellen [AP20].

Insbesondere der Aspekt mikrogeografischer Analysen erscheint dabei zentral: „Predictive policing is characterized mainly using increasingly complex statistical methods such as machine learning models (see infra), and using micro geographic levels of analysis, in practice generally a raster grid consisting of equally sized grid cells. The micro geographic level is more suitable and accurate as it better reflects the existing variability at that level of both crime and socioeconomic variables and provides more predictable crime patterns compared to higher geographic units of analysis such as census tracts, neighborhoods, or districts" [HR18].

Um räumliche (und sozialgeographische) Dimensionen abzubilden, eignen sich traditionell visuelle Zugänge in Form von Karten. Das Konzept des Mappings hat hier eine doppelte Bedeutung. Zum einen werden verschiedene Datensätze in Verbindung gesetzt und daraus relevante Indikatoren abgeleitet. Hier findet ein theoretisches Übereinanderlegen von Kriminalitätsdaten, z. B. mit demographischen Informationen statt. Zum anderen werden diese Daten mit ihrer räumlichen Verortung in Verbindung gebracht und es findet eine Modellierung potenzieller „risk locations“ statt [HR18, S. 205].

4.2 Big Data und Intelligence-led Policing

In der Regel geht der polizeilichen Intervention die Sammlung und Auswertung von Daten voraus. In Zeiten einer erhöhten Verfügbarkeit und immer größerer Datensätze findet bereits eine Zusammenführung verschiedener Datenquellen und Datensätzen und deren automatisierte Durchsuchung nach Mustern oder Patterns statt. Insbesondere Datamining helfe in der Polizeiarbeit von einem re- zu einem proaktiven Problemverständnis [Sh18, S. 253]. [Sh18] sprechen sich insbesondere für die erweiterte Suche nach Patterns zur (zukünftigen) Zusammenführung verschiedener Polizeidatenbanken zu einem Big Data-Netzwerk aus. Als Datenquellen könnten neben Einsatzberichten und Falldatenbanken IoT-Devices, die an öffentlichen Orten automatisiert Verbrechen detektierten, dienen [Sh18, S. 256]. In Data Fusion Centern würden Informationen von Strafverfolgungseinrichtungen und nicht an der Strafverfolgung beteiligten Akteuren, z. B. anhand von Social Media-Daten zusammengeführt: „[…] as a collaborative effort of multiple law enforcement and non-law enforcement entities that combine resources and information with the intent to “fuse” disparate pieces of information in an attempt to prevent or mitigate threats” [Ca12, S. 70]. Weitere Datenquellen liefert die Polizei selbst:

„Police authorities have been building their expertise on surveillance and monitoring technologies in the wake of 9/11, for example, CCTVs, smart phones, automated number plate readers, dash-board cameras and body-worn video cameras. These real-time sensors can continuously collect large amounts of data in urban environments on the movement of people, traffic flows and violations and changes in environmental indicators like heat, sound or pollution" [AP20, S. 60].

Im Folgenden wird zu zeigen sein, wie diese Aspekte im AI-Act einer kritischen Revision unterzogen werden.

5 Ethische Fragestellungen

Objektiv betrachtet erscheint eine bei angemessener Verfügbarkeit und mit gebotener Sorgfalt erfolgte Verarbeitung von Daten zum Allgemeinwohl relevant und naheliegend. Wieso sollten einmal erschlossene Datenquellen nicht einer Weiterverarbeitung zur Verfügung stehen und potenzielle Erkenntnisse, die die Korrelation verschiedener Variablen mit sich bringen würden, ungenutzt bleiben? Dieser Fragestellung soll an dieser Stelle noch einmal genauer nachgespürt und verschiedene Aspekte sorgfältiger beleuchtet werden. Wie so oft bilden diese ethischen Fragestellungen die Grundlage zukünftiger, gesetzlicher Direktiven.

Wie bereits erörtert, wurde im untersuchten Korpus der Umgang mit Daten untersucht. Wie u. a. [Eg20], [Os18], oder [Sh18], verweist auch [Zw19] auf die Kontextgebundenheit der Daten. Diese werfen selten selbst Fragen auf, sondern es müssen ihre Verfügbarmachung, ihre Verarbeitung und die daraus folgenden Konsequenzen betrachtet werden [Zw19]. In Zusammenhang mit der hier beleuchteten Thematik können verschiedene Ebenen diskutiert werden: Wie und wo werden Daten generiert, welche Konsequenzen werden aus der Datenverarbeitung gezogen?

Auf jeder dieser Ebenen kommt man nicht umhin, sich mit Fragen der Angemessenheit von Maßnahmen zum Gewinn und zur Auswertung von Daten auseinanderzusetzen. Und im Falle des Predictive Policing (bei dem es infolge seines Einsatzes zu einer behördlichen Urteilsbildung kommt) muss zusätzlich deren Gerechtigkeit und sogar Rechtmäßigkeit hinterfragt werden [Zw19].

Zu den ersten beiden Punkten der Fragestellungen, wie Daten akquiriert und generiert werden, äußern sich [Bo17] in ihrem Aufsatz zu Qualitätsmetriken im Zusammenhang mit Predictive Policing. Sie problematisieren die generelle Erfassbarkeit und Beschreibbarkeit der im Prozess erhobenen Daten selbst: „Ein generelles Problem von Predictive Policing mittels automatischen Datenanalysemethoden betrifft zudem deren grundlegende Annahme, dass das Delikt, das Gegenstand der Analyse ist, mit den vorliegenden Daten hinreichend genau im Hinblick auf Einflussfaktoren wie Raum, Zeit oder lokale Gegebenheiten beschrieben ist. Diese ist Voraussetzung für deren Anwendung, denn Verfahren zur automatischen Datenanalyse bzw. des maschinellen Lernens setzen die

ausreichende Messbarkeit des analysierten Phänomens voraus" [Bo17]. Während es sich hier vordergründig um die Frage ihrer Verfügbarkeit handelt, kommt dennoch die ethische Frage auf, ob Daten, wenn sie nicht hinreichend beschrieben werden können, überhaupt erfasst und verarbeitet werden dürfen. Auch schließt sich die Frage, ob die Datenerhebung rechtmäßig und die Erfassung kontextueller Umstände zulässig erfolgt ist, an.

An diesem Punkt setzt auch die Liste des Europäischen Parlaments an, die aufführt, welche KI-gestützten Praktiken im Rahmen des AI-Acts verboten werden sollen. So werden Techniken, die hier im Abschnitt 4.2 erfasst worden sind, als diskriminierend eingestuft. Verboten wird in diesem Zusammenhang konkret „untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases (violating human rights and right to privacy)" [YO23]. In diesem Zusammenhang verboten werden sollen zudem der Einsatz von KI zu Zwecken des Profilings, für räumliche Bewertungen sowie prädiktive Vorhersagen zu Personen anhand früherer Delikte. Alle hier diskutierten Aspekte werden im Zusammenhang mit Prädiktive Policing eher im Kontext einer Tätervermutung und des Targetings verwendet, wohingegen die eigentliche Unschuldsvermutung in den Hintergrund rückt.

Dem Verbieten bestimmter Praktiken stehen Ansätze gegenüber, ethische Konzepte in die Anwendung von Predictive Policing zu integrieren. [As19] liefert eine praktische Bewertung von Maßnahmen des Predictive Policings im Raum und schlägt zwei konkrete Ansätze vor: Das bewertende Konzept der *Models of Threat*, welches eher auf dem Targeting potenzieller Gefahrenquellen basiert auf der einen Seite. Dem gegenüber steht das Prinzip der *Ethics of Care*, welches eine durchaus datengestütze proaktive Integration von Personengruppen in Sozialprogrammen vorsieht [As19, S. 46-49]. Zusammengefasst benennt [As19] den holistischen Ansatz der Ethics of Care als konkrete Handlungsmaxime. Dieser basiert auf folgender Aussage: „interpersonal relationships form the basis for normativity, and should be guided by benevolence"[As19, S. 44]). Somit legt der Beitrag von [As19] eine konkrete Implementierung ethischer Aspekte in Maßnahmen vorbeugender Kriminalisierung vor und bietet einen ersten, ganzheitlichen Ansatz, den es weiter auszubauen und zu verbessern gilt.

6 Fazit

(Wie) Gelingt eine ethisch reflektierte Erhebung und Verwertung von Daten für die Polizeiarbeit und inwieweit ist sie nach dem Europäischen AI-Act möglich? Sicher ist zunächst, dass Techniken des Predictive Policings nach dem AI-Act weitestgehend gebannt werden dürften. Zwar liegen laut Quellenlange wesentliche Untersuchungen zum Einsatz von Techniken des Predictive Policings für die USA vor, jedoch konnten auch in Europa und Deutschland Szenarien für den Einsatz in der Polizeiarbeit nachgewiesen werden. Ihre Ergebnisse und Nutzung dürften nach dem AI-Act auf dem Prüfstand stehen. Für den juristischen Bereich eröffnet sich ggf. zudem die Frage, wie mit Personen, die basierend auf Maßnahmen aus dem Bereich behandelt wurden, umzugehen ist.

Der Artikel eröffnet interdisziplinär eine erste Diskussion und bietet das Rüstzeug für die Erschließung des Gegenstandes. Dazu wurde in einem ersten Zugang der theoretische Kontext zur Datenerhebung eingeordnet. Anhand des Literature Reviews wurden Methoden des Predictive Policing im Raum nachvollzogen. Abschließend wurden die so eröffneten Problematiken um das Feld ethischer Fragestellungen erweitert. Gezeigt werden konnte so, dass räumliche Verortung im Feld eine hohe Relevanz hat. Im Zusammenhang mit dem AI-Act werden derzeit eben diese Fragen einer kritischen Revision unterzogen und neu bewertet. Dieser Beitrag zeigt auch dass das Thema weiterer Untersuchungen und Klarstellungen bedarf und auch im zukünftigen Verwaltungshandeln miteinbezogen werden sollte. Die Diskussion um prädiktive und KI-gestützte Vorhersagen und ihre Regulierung ist noch immer sehr jung. In Zukunft wird sich zeigen, ob und wie auf aufgeworfene ethische Fragen, vielleicht gesetzliche Direktiven folgen werden.

Literaturverzeichnis

[AP20] Afzal, M. and Panagiotopoulos, P.: Smart policing: A critical review of the literature. In Electronic Government: 19th IFIP WG 8.5 International Conference, EGOV 2020, Linköping, Sweden, August 31–September 2, 2020, Proceedings 19 (pp. 59-70), Springer International Publishing, 2020.

[As19] Asaro, P. M.: AI Ethics in Predictive Policing: From Models of Threat to an Ethics of Care. IEEE Technology and Society Magazine, 38(2), S. 40–53, 2019.

[Bo17] Bode, F., Stoffel, F., & Keim, D.: Variabilität und Validität von Qualitätsmetriken im Bereich von Predictive Policing, 2017.

[BS20] Bode, F. & Seidensticker, K., Verlag für Polizeiwissenschaft.: Predictive Policing eine Bestandsaufnahme für den deutschsprachigen Raum, 2020.

[Bo16] Booth, A., Sutton, A., & Papaioannou, D.: Systematic approaches to a successful literature review (Second edition). Sage, 2016.

[Br09] Brocke, J. vom, Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process, 2009.

[CC12] Carter, J., & Chermak, S.: Evidence-Based Intelligence Practices: Examining the Role of Fusion Centers as a Critical Source of Information. In C. Lum & L. W. Kennedy (Hrsg.), Evidence-Based Counterterrorism Policy (S. 65–88). Springer New York, 2012.

[Eg18] Egbert, S.: About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany. European Journal for Security Research, 3(2), 95–114, 2018.

[Eg20] Egbert, S.: Datafizierte Polizeiarbeit – (Wissens-)Praktische Implikationen und rechtliche Herausforderungen. In D. Hunold & A. Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung (S. 77–100). Springer Fachmedien Wiesbaden, 2020.

[Fi14] Finlay, S.: Predictive analytics, data mining and big data: Myths, misconceptions and methods. Palgrave Macmillan, 2014.

[HR18] Hardyns, W., & Rummens, A.: Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. European Journal on Criminal Policy and Research, 24(3), 201–218, 2018.

[Kn16] Knobloch, T.: Vor die Lage kommen:Predictive Policing in Deutschland. Bertelsmann-Stiftung, 2016.

[Os18] Ostermeier, L.: Der Staat in der prognostischen Sicherheitsgesellschaft. In J. Puschke & T. Singelnstein (Hrsg.), Der Staat und die Sicherheitsgesellschaft (S. 101–121). Springer Fachmedien, 2018.

[Pe13] Perry, Walter L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S.: Predictive Policing. RAND Corporation; JSTOR, 2013.

[Sc17] Schryen, G., Benlian, A., Rowe, F., Gregor, S. D., & Larsen, K. R.: Literature Reviews in IS Research: What Can Be Learnt from the Past and Other Fields? Communications of the Association for Information Systems, 41, 759–774, 2017.

[Sh18] Sherer, J. A., Sterling, N. L., Burger, L., Banaschik, M., & Taal, A.: An Investigator's Christmas Carol: Past, Present, and Future Law Enforcement Agency Data Mining Practices. In H. Jahankhani (Hrsg.), Cyber Criminology (S. 251–273). Springer International Publishing, 2018.

[SK11] Shmueli, G., & Koppius, O. R.: Predictive Analytics in Information Systems Research. MIS Quarterly, 35(3), S. 553–572, 2011.

[TG16] Tayebi, M. A., & Glässer, U.: Social Network Analysis in Predictive Policing: Concepts, Models and Methods (1st ed. 2016). Springer International Publishing, 2016.

[YO23] Yakimova, Y.; Ojamo, J.: MEPs ready to negotiate first-ever rules for safe and transparent AI, https://www.europarl.europa.eu/news/en/pressroom/20230609-IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai, 2023-06-14, abgerufen 2023-06-17.

[VB17] Vandeviver, C., & Bernasco, W.: The geography of crime and crime control. Applied Geography, 86, 220–225, 2017.

[Zw19] Zweig, Katharina: Ein Algorithmus hat kein Taktgefühl: Wo künstliche Intelligenz sich irrt, warum uns das betrifft und was wir dagegen tun können. Heyne Verlag, 2019.

Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
68 Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023

Auf dem Weg zur datenbasierten Fallakte – ein Open-Source-Ansatz mit dem Digitalisierungswerkzeug samarbeid

Michael Prilop[1], Lutz Maicher [2]

Abstract: Die Digitalisierung der Fallbearbeitung führt häufig zu dokumentenzentrierten Fallakten. Auch außerhalb von Fachverfahren in der öffentlichen Verwaltung wird fallbasiert gearbeitet, bspw. bei der Klientenarbeit in Beratungsstellen oder in Anwaltskanzleien, bei Begutachtungen durch Sachverständigenbüros, im Bereich der sozialen Arbeit oder auch im Fördermittelsystem und Technologietransfer. Für eine Steigerung von Effektivität, Ablauf- und Ergebnisqualität im Fallmanagement sind datenbasierte Fallakten notwendig. Wichtige Basisanforderungen an digitale Akten sind Vertraulichkeit, Authentizität und Integrität, Revisionssicherheit, Verbindlichkeit, Verfügbarkeit, Schutz personenbezogener Daten, Langzeitarchivierung sowie Aktenrelevanz. Wir zeigen, dass in datenbasierten Fallakten die Steuerung und die Speicherung der Daten eine Einheit bilden müssen. Samarbeid ist ein Open-Source-Werkzeug für die Digitalisierung der Fallbearbeitung das diese Anforderungen adressiert und das Konzept der datenbasierten Fallakte implementiert.

Keywords: Fallakte, Digitalisierung, digitale Akte, Fallbearbeitung, Workflow, Fallmanagement

1 Einleitung

Verwaltungshandeln wird über die Bearbeitung von Vorgängen strukturiert. Ein Vorgang ist eine Abfolge von Tätigkeiten zur Erbringung einer Verwaltungsleistung. Dabei werden Dokumente erstellt, die dann zur Entstehung einer Vorgangsakte führen. Neben standardisierten Vorgängen (bspw. Ummeldung beim Bürgeramt) sind im Kontext von Fachverfahren [He18] häufig weniger standardisierte Vorgänge anzutreffen (bspw. komplexe Genehmigungsverfahren). Diese Vorgänge sind in ihrem Ablauf weniger

[1] Friedrich-Schiller-Universität Jena, Fakultät für Mathematik und Informatik, "Werkstatt" for digitization in the sciences, Ernst-Abbe-Platz 2, 07743 Jena, michael.prilop@uni-jena.de
[2] HTWK Leipzig, Professur für Digitalisierte Geschäftsprozesse und Geschäftsmodelle, Fakultät für Wirtschaftswissenschaft und Wirtschaftsingenieurwesen, D-04277 Leipzig, lutz.maicher@htwk-leipzig.de, https://orcid.org/0000-0002-9196-5742

doi:10.18420/rvi2023-008

vorstrukturiert, aber auch durch vielfältige Normen reglementiert. Gerade in diesen Fachverfahren entstehen umfangreiche Fallakten.

Viele Fallakten werden auch heute noch in Papierform geführt. Wird die Aktenführung digitalisiert, wird häufig der „mittlerweile jahrhundertealte Grundablauf jeden Verwaltungshandeln[s digitalisiert. …] In diesem Prozess dreht sich alles um Dokumente – um Anträge, Vermerke und Bescheide“ [He18]. Somit wird die „dokumentenzentrierte Verwaltungsarbeit einfach nur elektronisch nachgebildet“ [He18].

Die Kritikpunkte an dieser Dokumentenzentrierung sind offensichtlich „Es reicht eben nicht, Papier abzuschaffen, aber weiterhin dokumentenzentriert zu organisieren. […] Man kann und sollte heute zwischen Trägermedium (analoges oder digitales Dokument) und dem darin transportierten Inhalt unterscheiden. […] ‚Content‘ muss […] vom Dokument gelöst werden, um als Steuerungsinformation in IT-Systemen (d.h. als Information, die von Algorithmen verarbeitet werden kann) zur Verfügung zu stehen.“ [He18]. Vereinfacht gesagt: das Dokument soll aus der Aktenführung nicht verschwinden, sondern es muss zu einer Koexistenz von Dokumenten und Daten in der Aktenführung kommen (siehe hierzu auch Kap 4.3 in [MM22]). Wir sprechen dabei von der *datenbasierten Fallakte*.

Das grundsätzliche Prinzip der Aktenführung findet sich nicht nur innerhalb, sondern auch in vielen Bereichen außerhalb der öffentlichen Verwaltung. Beispiele sind die Klientenarbeit in Beratungsstellen oder in Anwaltskanzleien, Begutachtungen durch Sachverständigenbüros, viele Aspekte der sozialen Arbeit ([Ku19]) oder auch im Fördermittelsystem und Technologietransfer. Auch viele der dort aktiven Akteure haben erkannt, dass die Digitalisierung der Fallbearbeitung ein wichtiger Schlüssel zur Steigerung der Effizienz, aber auch der Ablauf- und Ergebnisqualität ist.

In ihrer Charakteristik sind diese Fälle wissensbasierte Dienstleistungen. Sie zeichnen sich durch hohe Wissensintensität und Komplexität aus. Sie sind zumeist personenbezogen und haben einen Schwerpunkt in Dispositionsbeziehungen [Bö06]. Dies bedeutet, dass zumeist eine Kooperation unter Bezug auf den „Gegenstand“ (bspw. das Gutachten) der Dienstleistung stattfindet. Wobei zumeist ein hierarchisches Verhältnis – zumindest aber eine Experte–Hilfsbedürftiger-Beziehung – zwischen den Kunden und den Erbringern der Dienstleistung existiert. Bei der Arbeit an den Fällen muss häufig eine Vielzahl an Regularien zum Vorgehen und/oder zur Dokumentation (Berichtswesen) eingehalten werden. Häufig haben diese Fälle Schnittstellen zu öffentlichem Verwaltungshandeln. Dies kann die Unterstützung der Klienten in Verwaltungsvorgängen sein; aber auch verpflichtendes Ergebnisreporting für die Statistik oder zu Abrechnungszwecken.

Fallbearbeitung ist zumeist eine kollaborative Tätigkeit. Mehrere Mitarbeitende sind in die Leistungserbringung für die Klienten eingebunden. Darüber hinaus sind oft externe Stakeholder (öffentliche Verwaltung; Gutachter; etc.) in die Fälle eingebunden.

Die Digitalisierung der Fallbearbeitung umfasst drei Felder: (1) Unterstützung der *Ablauforganisation der Fälle*, (2) die *Dokumentation der Fälle* (die Fallakte im engeren

Sinne) und (3) die Unterstützung der *Zusammenarbeit* aller an der Fallbearbeitung beteiligten. Eine besondere Herausforderung dabei ist, dass die oben skizzierten fallbearbeitenden Organisationen außerhalb der öffentlichen Verwaltung häufig klein sind und geringe oder keine IT-Kompetenzen besitzen. Zudem sind für viele Aufgabenfelder keine Fachanwendungen verfügbar. Im Folgenden stellen wir einen Lösungsansatz für die Digitalisierung der Fallbearbeitung vor, der besonders kleine, fallbasiert arbeitende Organisationen mit geringen IT-Kompetenzen adressiert.

Samarbeid[3] ist eine Open-Source-Lösung, welche die Digitalisierung der Fallbearbeitung für diese Organisationen ermöglicht. Samarbeid vereint die drei zentralen Funktionsbereiche der Fallbearbeitung in einem System:

- **Steuerung** - es vereint *flexibles* Aufgaben- und Prozessmanagement für die Fallbearbeitung, und unterstützt dabei gleichzeitig Struktur, ermöglicht Abweichungen und ist ohne IT-Kenntnisse anpassbar.
- **Kollaboration** – es ermöglicht integrierte, aufgabenzentrierte Zusammenarbeit und Kommunikation in der Organisation sowie mit Kunden und Externen.
- **Dokumentation** - Erfassung, Vernetzung und Wiederverwendung aller in den Aufgaben und Prozessen entstehenden Daten, Dokumente und organisationalen Wissen als datenbasierte Fallakte.

Bei der Realisierung einer datenbasierten Fallakte ist es notwendig Steuerung und Datenhaltung als Einheit zu verstehen. Gleichzeitig ist die Flexibilität der Steuerung wichtig, denn gerade im Kontext von Fachverfahren ist jeder Fall zwar ähnlicher Struktur, aber von unterschiedlicher Ausprägung. Weber fasst diese Herausforderung folgendermaßen zusammen: „Der zunehmende Einsatz von Fachsoftware zur Falldokumentation unterliegt dem Spannungsverhältnis zwischen der einzelfallorientierten Darstellung und der Subsumtion der Fälle unter Kategorien und Schemata.“ [We17]. Um dies zu ermöglichen implementiert samarbeid für die *Steuerung* eine Adaption des Case-Handling-Paradigma [VW+05]. Dieses Paradigma greift die Schwächen klassischer Workflow-Ansätze bei der Realisierung von Fällen auf und ermöglicht eine Lösung, die gleichzeitig Struktur und Flexibilität bietet. Dies wird in Abschnitt 0 im Detail beschrieben.

Eine datenbasierte Fallakte sollte die Basisanforderungen an eine digitale Akte erfüllen. In Abschnitt 3 werden diese Anforderungen – aus einer dokumentenzentrierten Perspektive kommend – beschrieben und in den Kontext einer datenbasierten Fallakte übertragen. In Abschnitt 4 wird samarbeid als Werkzeug für die Steuerung, Kollaboration und Dokumentation im Fallmanagement beschrieben. In Abschnitt 5 diskutieren wir, inwieweit samarbeid bereits heute die Implementierung einer datenbasierten Fallakte darstellt – sowie die noch bestehenden Lücken.

[3] https://www.samarbeid.org/

2 Case-Handling-Paradigma

Klassische Workflow-Management-Systeme haben gerade für die Digitalisierung der Fallbearbeitung (also bei wissensintensiven Fachverfahren) einige Schwächen, die durch [VW+05] folgendermaßen zusammengefasst werden:

- In Workflow-Systemen muss die Arbeit in Aktivitäten verpackt und verteilt werden. Diese Aktivitäten müssen unabhängig voneinander abgearbeitet werden können, da sie immer unterschiedlichen Bearbeitenden zugewiesen werden können. Bei dieser „Atomisierung" der Aufgaben besteht das Risiko, dass eigentlich zusammenhängende Aufgabenkomplexe in Teilaktivitäten zerlegt und damit Kontext verloren geht (*context tunneling*).
- Das Zuweisen einer Aufgabe impliziert in einem Workflow-System gleichzeitig *Verantwortung für die Abarbeitung* und *Berechtigung (Sichtbarkeit)*. In Fällen ist es auch sinnvoll, wenn ein Fallbearbeitender nur die Aufgaben „auf dem Schreibtisch" hat, für die er aktuell verantwortlich ist. Aber unabhängig davon, sollte er zusätzlich auch Berechtigungen (oder mindestens Sichtbarkeit) für die anderen Aufgaben innerhalb des Falles haben.
- Die ausschließliche Sichtbarkeit von Aufgaben, für die die Bearbeiter gerade verantwortlich sind, fokussiert diese ausschließlich auf die Aktivitäten, die gemacht werden *müssen* und nicht auch auf die Aktivitäten, an denen situationsbezogen auch gearbeitet werden kann.

Basierend auf diesen Schwachstellen schlagen [VW+05] das Case-Handling-Paradigma vor, dessen zentrale Eigenschaften sind:

- *Trennung von Verantwortung und Sichtbarkeit.* Damit sind grundsätzlich alle relevanten Informationen eines Falls für den Fallbearbeiter verfügbar. Das vermeidet *context tunneling*.
- *Aktivitäten* werden umgesetzt, wenn relevante Informationen verfügbar sind und nicht ausschließlich auf Basis der Ablauflogik des Falles.
- *Alle berechtigten Nutzer dürfen Daten bearbeiten* unabhängig davon, ob die zugehörige Aktivität gerade ausgeführt wird oder nicht.
- *Daten und Prozesse werden als gleichwertig betrachtet*. In klassischen Workflow-Systemen dominieren Aufgaben, in Fällen wird das Abarbeiten von Aufgaben und das Erstellen fall-relevanter Daten als eher gleichwertig betrachtet.

Für eine ausführliche Darstellung des Case-Handling-Paradigmas sei auf [VW+05], [Mh+13] verwiesen. Das Paradigma hat zudem Eingang in die Standardisierung der CMMN (Case Management Model and Notation)[4] der OMG gefunden.

[4] https://www.omg.org/spec/CMMN

3 Basisanforderungen an eine digitale Akte

Schriftlichkeit, und die damit einhergehende Nachvollziehbarkeit und Einklagbarkeit von Verwaltungsbescheiden, ist ein zentraler Vorteil dokumentenorientierten Verwaltungshandelns. Dies muss auf datenorientiertes Verwaltungshandeln übertragen werden. Leibenger et al. [LP+15] beschreiben die folgenden Anforderungen an digitale Akten, die hier in den Kontext einer datenorientierten Fallakte gesetzt werden.

Vertraulichkeit bedeutet, dass „wer nicht berechtigt ist, soll nicht auf Informationen zugreifen können". Dies betrifft sowohl den direkten Zugriff auf die Gesamtakte, sowie einzelne Datenpunkte innerhalb der Gesamtakte, als auch das Wissen über die Existenz der Akte sowie einzelner Datenpunkte innerhalb der Akte. Das zeigt, dass Berechtigungen auf verschiedenen Ebenen einer digitalen Akte festlegbar sein sollten. Zudem können sich Berechtigungen einzelner Personen im Zeitverlauf ändern, bspw. wenn Mitarbeiter neue Funktionen übernehmen oder aus der Bearbeitung des Falls ausscheiden.

Authentizität und Integrität. Unter Authentizität wird verstanden, dass es nachgewiesen ist, dass ein Datenpunkt von dem behaupteten Autor stammt. Integrität bedeutet, dass der Datenpunkt nicht unerkannt verändert werden kann. Es also sichergestellt ist, dass ein Datenpunkt genau in der gespeicherten Art und Weise durch den authentischen Autor erstellt wurde. Authentizität und Integrität kann jedoch nicht nur auf Ebene eines Datenpunktes, sondern auch auf Ebene einer ganzen Akte gefordert sein.

Revisionssicherheit ist die „Integrität der Versionsgeschichte" [LP+15] der Akte. Das bedeutet, dass es für die Gesamtakte und für jeden Datenpunkt in der Gesamtakte möglich sein muss, diese auf einen bestimmten Zeitpunkt „zurückzusetzen". Und dass sichergestellt ist, dass diese „zurückgesetzte" Version dem tatsächlichen Zustand zu diesem Zeitpunkt entspricht.

Verbindlichkeit bedeutet, „dass ein Dokumentautor seine Autoreneigenschaft nicht erfolgreich abstreiten kann" [LP+15]. Digitale Signaturen sind ein probates Mittel, um die Verbindlichkeit einer Autorenschaft für einen Datenpunkt zu erhöhen.

Verfügbarkeit bedeutet, dass alle Nutzer, die die Berechtigung haben eine Akte oder einen Teil einer Akte einzusehen, jederzeit Zugriff auf diese Daten haben sollen.

Schutz personenbezogener Daten. Sowohl in den Daten der Akten, als auch in den Metadaten der Akten, werden personenbezogene Daten gespeichert. Dies muss konform zu den in dem Kontext der Aktenführung geltenden Rechtsnormen passieren. [LS+18] illustriert, dass gerade die dadurch mögliche Transparenz (bspw. zur Arbeitseffektivität) durch die Fallbearbeitenden durchaus kritisch gesehen werden kann.

Langzeitarchivierung. [LP+15] unterstreichen, dass alle oben genannten Ziele „von der erstmaligen Anlage der Akte über den rechtskräftigen Abschluss des Verfahrens" erreicht werden müssen. Das kann Aufbewahrungsfristen von mehreren Jahrzehnten umfassen. Auch die Rekonstruierbarkeit einer Akte muss über diese Zeiträume gewährleistet sein.

Konzept der *Aktenrelevanz*. Daten, die im Rahmen von Kollaborationsaktivitäten entstehen und sich nicht direkt auf die Dokumentation des Falls beziehen, sollen auch nicht in der digitalen Akte erscheinen. Es muss also eine Unterscheidung zwischen aktenrelevanten Daten und nicht-aktenrelevanten Daten existieren.

Die Wichtigkeit von Authentizität, Integrität und Revisionssicherheit (aber auch einer sicheren Langzeitarchivierung) illustriert [Gr21] im Kontext medizinischer Fallakten. „Die Dokumentation darf keinesfalls nachträglich geändert werden da ihre Vollständigkeit und Richtigkeit in fast jedem Prozess umstritten ist“ [Gr21]. „Denn deren Beweiswert wäre schon beeinträchtigt, wenn bei ihr theoretisch nachträgliche Änderungen entgegen der Vorgabe des § 630f Abs. 1 S. 2 u. 3 Bürgerliches Gesetzbuch gar nicht erst erkennbar wären. Es muss zumindest systemseitig aus den Metadaten ersichtlich bleiben, wann welcher Eintrag getätigt und eventuell doch verändert wurde. Selbst wenn keine Änderung an einer solchen elektronischen Dokumentation erfolgt, diese Gewähr aber technisch nicht bestünde, käme ihr schon nicht mehr die volle Indizwirkung für festgehaltene Maßnahmen oder nicht festgestellte Befunde zu. Dies hat aktuell der Bundesgerichtshof (BGH) nochmals bestätigt (Urt. v. 27.4.2021, VI ZR 84/19).“ [Gr21]

4 Datenbasierte Fallakte mit samarbeid

Mit samarbeid stellen wir eine Open-Source-Lösung vor, welche die Digitalisierung der Fallbearbeitung für kleine Organisationen mit geringen IT-Kompetenzen ermöglicht. Samarbeid wird derzeit von sechs Pilotorganisationen in der operativen, täglichen Arbeit genutzt. Diese Organisationen arbeiten fallbasiert, jedoch außerhalb der öffentlichen Verwaltung. Einige der Organisationen haben enge Austauschbeziehungen zu öffentlichem Verwaltungshandeln, andere nur peripher.

Im Folgenden sollen die drei Kernkonzepte von samarbeid *Prozesse*, *Aufgaben* und *Dossiers* vorgestellt werden. Abb. 1 stellt die Zusammenhänge zwischen diesen Kernkonzepten dar.

Fälle werden in samarbeid durch Prozesse abgebildet. Die Datenstruktur eines individuellen Prozesses ist gleichzeitig die Grundlage für die datenbasierte Akte dieses Falls. Im Regelfall basiert ein Prozess auf einer Prozessvorlage.[5] Die Prozessvorlage legt die Grundstruktur eines Prozesses zum Startzeitpunkt fest. Zur Laufzeit kann jeder Prozess flexibel – sowohl um Aufgaben als auch um Datenfelder – erweitert werden. So kann der Lebenszyklus jedes Falls flexibel abgebildet werden und gleichzeitig ein Mindestmaß an Struktur (welches sich bspw. aus regulatorischen Vorgaben ableiten kann) und somit Vergleichbarkeit sichergestellt werden.

[5] Samarbeid unterstützt darüber hinaus auch Prozesse ohne Prozessvorlage sowie Einzelaufgaben. Da dies jedoch keinen Einfluss auf die hier vorgestellte Nutzung von samarbeid als datenbasierte Fallakte hat, werden diese Spezialfälle im Weiteren nicht besprochen.

Die Struktur eines Prozesses definiert zum einen die im Prozess verfügbaren Datenfelder. Datenfelder haben eine Benennung und einen Datentyp[6]. Ein möglicher Datentyp ist Dokument. Somit werden in den Datenfeldern Daten und Dokumente gleichwertig behandelt, was den Übergang von der dokumentenzentrierten Fallakte zur datenzentrierten Fallakte ermöglicht. Ein weiterer spezieller Datentyp sind Referenzen zu Dossiers, die weiter unten im Detail beschrieben werden.

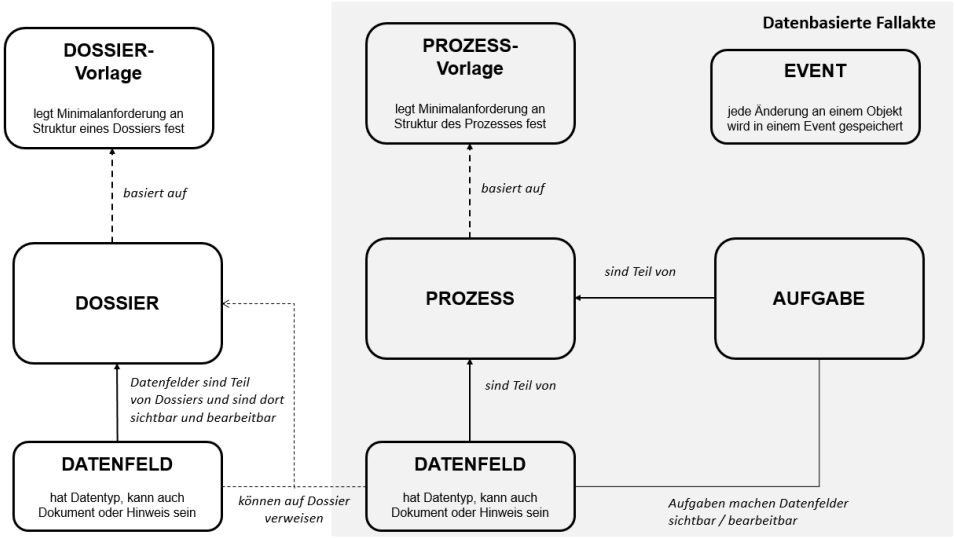

Abb. 1 Übersicht über die Kernkonzepte von samarbeid

Neben den Datenfeldern definiert die Prozessstruktur auch die Aufgaben innerhalb eines Prozesses. Aufgaben sind die Container, in denen die Datenfelder des Prozesses für die Nutzer verfügbar gemacht werden. Für jede Aufgabe kann festgelegt werden, welche Datenfelder des Prozesses angezeigt werden sollen – und ob diese innerhalb der Aufgabe bearbeitbar sein sollen. Darüber hinaus kann spezifiziert werden, für welche Datenfelder einer Aufgabe ein Wert vorliegen muss, damit die Aufgabe abgeschlossen werden kann.

Innerhalb eines Prozesses ist die Ablaufstruktur der Aufgaben festgelegt, wobei eine deutlich geringere Komplexität als bei BPMN oder eEPK möglich ist. Grund für diese bewusste Komplexitätsreduktion ist, dass die Ablaufstruktur auch durch Nutzer mit geringer Digital- und Modellierungskompetenz erstellt und modifiziert werden kann. Im Standardfall ist der Ablauf innerhalb eines Prozesses sequentiell. Durch die Nutzung von sogenannten Blöcken können Bereiche der parallelen Aktivierung von Aufgaben definiert

[6] Einen Überblick über alle derzeit unterstützten Datentypen gibt:
https://www.samarbeid.org/support/samarbeid-verwenden/datenfelder/

werden. Blöcke können zudem Eingangsbedingungen haben (die auf Basis von Datenfeldern ausgewertet werden), so dass auch bedingte Abläufe möglich sind.

Aus dieser Ablaufstruktur leitet sich auch das Statusmodell der Aufgaben innerhalb von samarbeid ab. Aufgaben können die Status erstellt, aktiv, zurückgestellt, übersprungen und abgeschlossen haben. Aktive Aufgaben „liegen“ auf dem Schreibtisch der für die Aufgaben verantwortlichen. Jedoch kann jeder Nutzer jederzeit auch alle anderen Aufgaben bearbeiten, die für ihn sichtbar sind. Damit wird ein zentrales Element des Case-Management-Paradigmas umgesetzt.

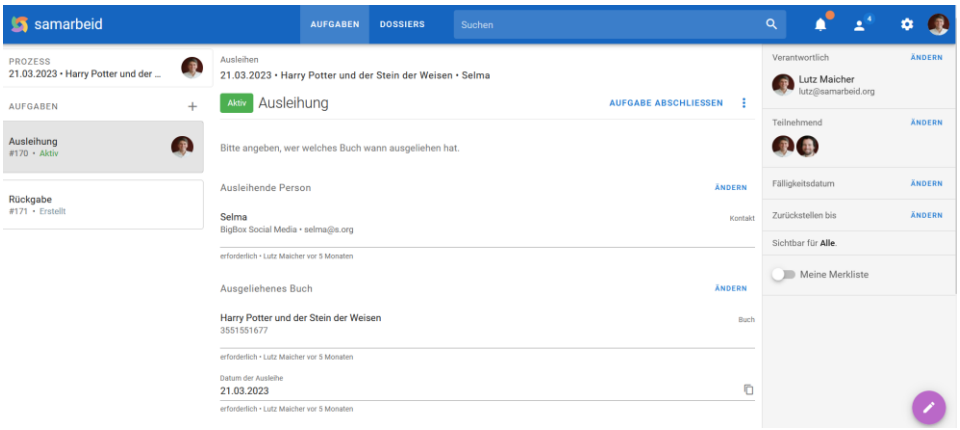

Abb. 2 Die Aufgabe Ausleihung in einem Prozess im Demo-System[7] von samarbeid.

Verantwortlichkeit ist ein wichtiges Konzept in samarbeid. Dabei wird zwischen *Verantwortlich* und *Teilnehmend* unterschieden. Durch unterschiedliche Ansätze versucht samarbeid sicherzustellen, dass alle aktiven Prozesse einen Verantwortlichen haben. Der Verantwortliche hat den Prozess „auf seinem Schreibtisch“ und wird über alle relevanten Änderungen informiert. Dieser Nutzer ist maßgeblich dafür verantwortlich, dass der Prozess rechtzeitig und in der geforderten Güte abgeschlossen wird. Für die Aufgaben innerhalb des Prozesses kann derselbe Nutzer verantwortlich sein. Die Verantwortlichkeit von Aufgaben kann aber auch an andere Nutzer weitergegeben werden. Hier gilt wieder das Prinzip: der für eine Aufgabe verantwortliche Nutzer hat diese „auf seinem Schreibtisch“ und ist für den Abschluss der Aufgabe verantwortlich. Aufgaben können darüber hinaus auch Teilnehmende haben. Das sind Nutzer, die bei der Realisierung der Aufgabe unterstützen oder über diese informiert werden.

Die Sichtbarkeit eines Prozesses oder einer Aufgabe für einen Nutzer ist von dem Thema Verantwortlichkeit getrennt. Die Sichtbarkeit wird über die Prozessvorlage gesteuert. Ein

[7] Diese Aufgabe im Demo-System von samarbeid ist unter https://try.samarbeid.org/tasks/170 erreichbar. Details zum Einloggen in das Demo-System finden sich unter: https://www.samarbeid.org/ueber-samarbeid/du-willst-samarbeid-ausprobieren-so-geht-es/

Nutzer kann (über seine Zugehörigkeit zu einer Gruppe) einer Prozessvorlage zugeordnet werden. Wenn das der Fall ist, dann sieht er alle Prozesse und Aufgaben, die aus dieser Prozessvorlage abgeleitet sind. In samarbeid umfasst die Sichtbarkeit Lese- und Schreibrechte. Dies ist sehr weitgehend. Ein Nutzer kann in allen Prozessen, die er sieht, die Werte aller Datenfelder ändern – und darüber hinaus auch die Struktur aller Prozesse. Diese umfassenden Rechte sind für die Sicherstellung der Flexibilität notwendig.

Eingehegt werden diese Rechte durch ein hohes Maß an Transparenz und Nachvollziehbarkeit. Für alle Änderungen an Daten und Strukturen werden Events erzeugt. Diese Events speichern wer was wann verändert hat und werden unveränderbar im Journal abgelegt. Einige Events werden als Benachrichtigungen an verantwortliche Nutzer ausgespielt, damit diese direkt über Änderungen informiert werden.

Benachrichtigungen sind auch für die aufgabenzentrierte Kommunikation innerhalb von samarbeid wichtig. Jede Aufgabe oder Prozess hat einen Kommentarbereich. Hier können die Nutzer relevante Themen direkt im Kontext der Aufgabe besprechen und Ergebnisse der Diskussion dokumentieren. Mit einem einfachen Referenzierungsmechanismus kann leicht gesteuert werden, an wen (Nutzer oder Gruppen) ein Beitrag gelenkt werden soll. Dieses Kommunikationssystem ist wichtig für die Kollaboration innerhalb des Falls.

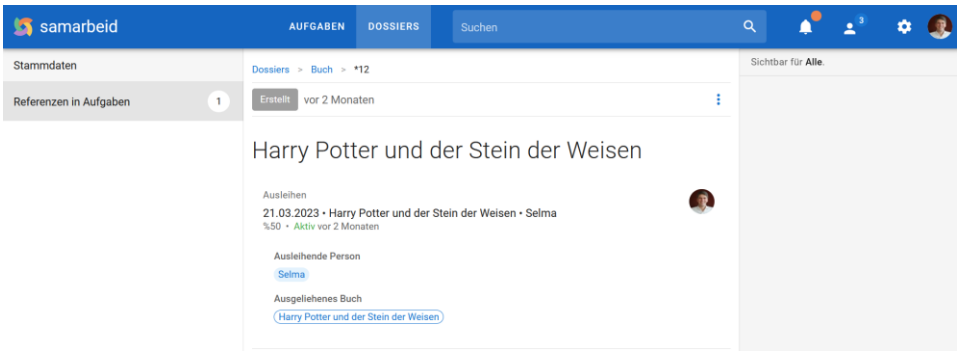

Abb. 3 Ausschnitt aus dem Dossier für das Buch Harry Potter und der Stein der Weisen im Demo-System (https://try.samarbeid.org/dossiers/12/task-references)

Neben Prozessen und Aufgaben sind Dossiers das dritte zentrale Konzept in samarbeid. Die meisten Daten werden in samarbeid innerhalb der einzelnen Prozesse gespeichert – da sie vollständig dem Fall zuordbar sind und nur für den Fall Relevanz haben. Es gibt aber auch „Dinge“, die in verschiedenen Fällen „genutzt“ werden (z.B. die Stammdaten für einen Klienten). Um für diese Daten einen „single point of truth“ zu schaffen und Redundanzen zu vermeiden, werden Dossiers genutzt. Ein Dossier kann in unterschiedlichen Aufgaben referenziert werden. In dem Dossier werden (ebenfalls in Datenfeldern) bspw. die Stammdaten einer Person gespeichert (Name, Telefonnummer etc.). In den Aufgaben wird über eine Referenz gespeichert, was mit dieser Person im

Kontext der Aufgabe gemacht wurde. Im Dossier entsteht dabei automatisch ein 360°-Blick auf alle Aktivitäten, die mit dieser Person realisiert wurden.

Beispiel: In Abb. 2 existiert in der Aufgabe „Ausleihe“ ein Datenfeld „Ausgeliehenes Buch“. Hier kann referenziert werden, welches Buch in dieser Aufgabe ausgeliehen wurde. Für das Buch existiert ein Dossier, welches in Abb. 3 zu sehen ist. Durch die Nutzung des Dossiers in der Aufgabe „Ausleihe“ wird in dem Dossier automatisch sichtbar, dass es im Kontext dieser Aufgabe genutzt wurde – und zudem einen Bezug zu dem Dossier „Selma“ hat. Denn dies ist das Dossier der ausleihenden Person.

Abschließend ist hervorzuheben, dass Prozesse in samarbeid *abgeschlossen* sind. Hier setzt samarbeid das in [Ma07] beschriebene Konzept um, dass jeder Prozess als in sich abgeschlossene Einheit die Beschreibung seiner Ablaufstruktur, das Datenmodell aller Datenfelder, alle individuellen Falldaten incl. Kommentare sowie alle zugehörigen Ereignisse speichert. Diese Abgeschlossenheit ermöglicht es, diese Prozesse als eigenständige datenbasierten Fallakten zu speichern.

5 samarbeid als Umsetzungsoption der datenbasierten Fallakte

Eine aus unserer Sicht notwendige Voraussetzung für die Umsetzung einer datenbasierten Fallakte ist, dass die *Ablauforganisation eines Falls* und seine *datenbasierte Dokumentation* eine abgeschlossene Einheit bilden. Auf Grund der Variabilität der Fälle – auf der einen Seite – und der Notwendigkeit von Regelkonformität – auf der anderen Seite – muss der Ansatz zugleich Struktur und Flexibilität zulassen. Zudem fokussiert sich der hier vorgestellte Ansatz auf kleine Organisationen mit geringer Digitalkompetenz.

Für die Umsetzung einer strukturierten und gleichzeitig flexiblen Ablauforganisation setzt samarbeid eine adaptierte Form des Case-Handling-Paradigmas (siehe Abschnitt 2) um. Dabei trennt samarbeid konsequent Verantwortung und Sichtbarkeit. Diese Trennung wird von zwei Ansätzen begleitet, die den Pilotnutzern besonders wichtig waren: (1) Samarbeid versucht sicherzustellen, dass alle aktiven Prozesse und alle aktiven Aufgaben immer einen Verantwortlichen haben und unterstützt proaktiv alle Verantwortlichen dabei, die Aufgaben und Prozesse „auf ihrem Schreibtisch“ im Blick zu behalten. (2) Um Flexibilität sicherzustellen ist Sichtbarkeit bei samarbeid mit weitgehenden Schreibrechten verbunden. Das wird jedoch flankiert mit sehr detaillierter Transparenz, so dass alle Aktionen und die zugehörigen Nutzer leicht nachvollzogen werden können.

Samarbeid verhindert *context tunneling*. Durch die flexible Nutzung von Datenfeldern innerhalb von Aufgaben (mit und ohne Schreibrechten) können in der Struktur der Aufgaben alle notwendigen Informationen vorgegeben werden, welche für die erfolgreiche Abarbeitung der Aufgabe notwendig ist. Wenn dies nicht reicht, können sich die Nutzer einen breiten Überblick über alle Aufgaben und Daten des Falles verschaffen.

Die Prozesse und deren Datenhaltung ist in samarbeid so konzipiert, dass sie in sich abgeschlossene Einheiten bilden. Vereinfacht gesagt: es ist konzeptuell möglich, einen Prozess separat zu speichern und diesen in einer anderen samarbeid-Instanz ohne eine Vorkonfiguration zu laden und mit seinen Daten auszuführen. Dies bildet die technische Grundlage für die Nutzung von Prozessen in samarbeid als datenbasierte *Fallakte*. Im Folgenden werden die oben skizzierten Anforderungen an eine digitale Akte im Kontext der samarbeid-Umsetzung gesetzt.

Vertraulichkeit ist in samarbeid über die oben beschriebenen Sichtbarkeitsregeln sichergestellt. Diese können auf Ebene der Prozessvorlage gesteuert werden. Dies bedeutet, dass in der derzeitigen Implementierung die Steuerung der Sichtbarkeit einzelner Datenpunkte nicht möglich ist. Die technische Architektur von samarbeid würde dies jedoch grundsätzlich ermöglichen. Hierfür haben wir bereits das Konzept der *Zuarbeit* entwickelt, welches jedoch noch nicht implementiert ist. Das Problem der Veränderung von Berechtigungen im Zeitverlauf ist in samarbeid gelöst. Nutzer können Sichtbarkeiten verlieren, ihre Beiträge innerhalb eines Falls bleiben jedoch erhalten.

Authentizität und Integrität. Mit den fein-granularen Ereignissen hat samarbeid einen Mechanismus, um Integrität sicherzustellen. Jede Änderung an Datenfeldern (oder an der Prozessstruktur) wird als unveränderbarer Event gespeichert. Damit kann Integrität auf Ebene von Datenfeldern, Aufgaben oder ganzen Prozessen (und damit Fallakten) sichergestellt werden. Dieser Mechanismus ist derzeit noch lückenhaft implementiert, d.h. es existieren Änderungen, die „unbemerkt" vorgenommen werden können. Diese Lücken werden schrittweise geschlossen. Authentizität ist in der Weise sichergestellt, dass alle Änderungen einem Nutzerprofil zugeordnet werden.

Revisionssicherheit. Der Mechanismus der Ereignisse ist auch die Grundlage für eine zukünftige Revisionssicherheit, d.h. der „Integrität der Versionsgeschichte" [LP+15]. Derzeit ist es noch nicht möglich, die Gesamtakte oder auch nur einen Datenpunkt auf einen bestimmten Zeitpunkt „zurückzusetzen". Die technischen Grundlagen sind dafür jedoch gelegt.

Verbindlichkeit ist derzeit nur rudimentär umgesetzt. Durch den Ereignis-Mechanismus ist jede Änderung einem Nutzer zugeordnet. Auf Grund der fehlenden Revisionssicherheit ist jedoch beispielsweise nicht nachvollziehbar, wer einen bestimmten Wert in ein Datenfeld gespeichert hat. Wie bereits oben diskutiert, sind die architektonischen Grundlagen vorhanden, so dass Verbindlichkeit auf Ebene der Datenfelder, Aufgaben oder Prozesse umgesetzt werden kann.

Verfügbarkeit ist umgesetzt. Samarbeid ist ein serverbasiertes System, was somit von allen internetfähigen Endgeräten aus genutzt werden kann. Zudem ist samarbeid Open Source. Es kann durch die Anwendungsorganisationen selbständig und vollkommen unabhängig von einem Anbieter betrieben werden.

Schutz personenbezogener Daten ist nicht nur eine technische, sondern eine organisationale Herausforderung. Die Organisation, die samarbeid nutzt, legt fest, welche personenbezogenen Daten in ihren Fällen erhoben und gespeichert werden sollen. Hier muss die Organisation über Regelkonformität entscheiden. Darüber hinaus werden personenbezogene Daten der Nutzer bei der Arbeit mit samarbeid gespeichert. Dies geschieht insbesondere innerhalb der Ereignisse, die die Nachvollziehbarkeit (und damit Authentizität, Integrität und Revisionssicherheit) sicherstellen. An dieser Stelle muss anwendungs- und organisationsspezifisch zwischen der Notwendigkeit einer rechtssicheren Akte und dem Schutz personenbezogener Daten abgewogen werden.

Langzeitarchivierung. Aufbewahrungsfristen von mehreren Jahrzehnten und die langfristige Gewährleistung der Rekonstruierbarkeit sind für alle digitalen Formate eine große Herausforderung. Eine wichtige Grundlage hierfür ist die Abgeschlossenheit der Fallakten. In samarbeid beinhaltet ein Prozess sowohl die Beschreibung seiner Ablaufstruktur als auch alle in ihm gespeicherten Daten, sowie die zugehörigen Ereignisse. Er ist somit in sich vollkommen abgeschlossen und kann als abgeschlossene Einheit archiviert und später rekonstruiert werden.

Aktenrelevanz ist noch eine Herausforderung in der aktuellen Architektur von samarbeid. Konzeptuell unterstützt samarbeid direkt die Kollaboration im Kontext der Fälle. Derzeit wird jedoch jeder Datenpunkt (also auch jeder Kommentar) Teil der Prozessdaten. Um samarbeid als integriertes Kollaborationswerkzeug zu etablieren (was aus unserer Sicht für die erfolgreiche Nutzung zur digitalen Fallbearbeitung notwendig ist), und gleichzeitig das Konzept der Aktenrelevanz zu unterstützen, wird es notwendig sein, Kollaborationsmöglichkeiten „außerhalb“ der Akte zu etablieren. Von Vorteil ist dabei, dass bereits heute in samarbeid alle Aufgaben, Prozesse und Dossiers – ähnlich des Konzepts des Zettelkastens - leicht referenziert werden können. Somit ist die Grundlage geschaffen, den Kollaborationsbereich von den eigentlichen Falldaten zu trennen und gleichzeitig stark mit dem Kontext des Falls zu vernetzen.

6 Zusammenfassung und Ausblick

Ausgangspunkt ist, dass die Digitalisierung der Fallbearbeitung nicht zu dokumentenzentrierten Fallakten führen darf. Für Lösungen, die zu einer Steigerung von Effektivität sowie Ablauf- und Ergebnisqualität führen, ist es notwendig, dass Dokumente und in den Anwendungen entstehende Falldaten gleichwertige Bestandteile der Fallakte werden - eine datenbasierte Fallakte. Wichtige Basisanforderungen an digitale Akten sind Vertraulichkeit, Authentizität und Integrität, Revisionssicherheit, Verbindlichkeit, Verfügbarkeit, Schutz personenbezogener Daten, Langzeitarchivierung sowie Aktenrelevanz. Um dies auch in datenbasierten Fallakten zu ermöglichen ist es notwendig, die Steuerung und die Speicherung der Daten als abgeschlossene Einheiten zu betrachten.

Besonders kleine, fallbasiert arbeitende Organisationen mit geringer IT-Kompetenz haben keine Möglichkeiten passende Individualsoftware für die Digitalisierung ihrer Fallbearbeitung zu erstellen. Häufig ist auch keine passende Fachsoftware am Markt verfügbar. Mit samarbeid stellen wir ein Open-Source-Werkzeug für Digitalisierung der Fallbearbeitung in diesen Organisationen vor. Wir zeigen, dass samarbeid bereits viele Voraussetzungen erfüllt, um das Konzept der datenbasierten Fallakte umzusetzen. Einige Aspekte sind bisher nicht implementiert, jedoch konzeptuell vorbereitet.

Wir führen mit den aktuell sechs Pilotorganisationen systematisch, regelmäßig und engmaschig Feedbackgespräche durch. Die gewonnenen Erkenntnisse fließen kontinuierlich in die Weiterentwicklung von samarbeid ein. In einem nächsten Schritt planen wir – wenn 10 Pilotorganisationen gewonnen werden konnten - eine strukturierte Nutzerstudie durchzuführen, in der wir ein umfassendes Bild der Pilotnutzung von samarbeid zeichnen werden (Nutzen, Aufwände, Barrieren, Onboarding, etc.).

Literaturverzeichnis

[Bö06] Böhle, F. (2006): Typologie und strukturelle Probleme von Interaktionsarbeit. In: Böhle, F., Glaser, J. (Hrsg.): Arbeit in der Interaktion — Interaktion als Arbeit. VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-90505-1_18

[Gr21] Greiff, M.: Beweiswert der (elektronischen) Dokumentation, HNO-NACHRICHTEN 2021;51 (6), S. 53, 2021.

[He18] Herzberg, J.: Wird die Bedeutung der eAkte für die Digitalisierung der Verwaltung überschätzt? In: Verwaltung und Management 24. Jg, Heft 2, S. 96-99, 2018

[Ku19] Kutscher, N.: Digitalisierung der Sozialen Arbeit. In: Rietmann, S., Sawatzki, M., Berg, M. (Hrsg.): Beratung und Digitalisierung. SpringerVS (2019)

[LP+15] Leibenger, D.; Petrlic, R.; Sorge, C.; Vogelgesang, S.: Elektronische Akten: Anforderungen und Technische Lösungsmöglichkeiten. Proceedings of the 18th Legal Informatics Symposium IRIS 2015, S. 271–279, 2015.

[LS+18] Löbel, S.; Schuppan, T.; Dozenko, C.: Ein Blick in die Praxis: Akzeptanz der eAkte im Bereich SGB II. In: VM Verwaltung & Management 24.6 (2018): 299-306.

[Ma07] Maicher, L.: Autonome Topic Maps. Zur dezentralen Erstellung von implizit und explizit vernetzten Topic Maps in semantisch heterogenen Umgebungen. Universität Leipzig, Diss, 2007.

[MH+13] Marin, M.; Hull, R.; Vaculín, R.: Data centric bpm and the emerging case management standard: A short survey. In: Business Process Management Workshops: BPM 2012 International Workshops, Tallinn, Estonia, September 3, 2012. Revised Papers 10. Springer Berlin Heidelberg, 2013.

[MM22] Markus, H.; Meuche, T.: Auf dem Weg zur digitalen Verwaltung. Ein ganzheitliches Konzept für eine gelingende Digitalisierung der öffentlichen Verwaltung. SpringerGabler (2022)

[VW+05] Van der Aalst, W. M.; Weske, M.; Grünbauer, D.: Case handling: a new paradigm for business process support. Data & knowledge engineering, 53(2), 129-162, 2005.

[We17] Weber, J.: Softwarebasierte Falldokumentation im Balanceakt um die fallangemessene Darstellung [online]. KoPäd, 2017. Verfügbar unter: http://dx.doi.org/10.26041/fhnw-1110, 2017

Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
82 Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023

A Scoring Model for Public Administration Process Prioritization in Germany

Tim Pidun [1] and Dirk Müller [2]

Abstract. The German public administration still struggles on becoming digital though considerable effort has been made by accompanying laws and institutions and a good will to digitalize all user-centered processes. But still there is no structured prioritization of processes, and Stakeholders fear the ongoing rather ad-hoc processing of their digitalization tasks. This contribution aims to construct a suitable prioritization score by deriving domain-specific selective aspects along an IS evaluation approach and formulation of a score that relates to the priority of the service process. It can be used to sort a given amount of processes independently of the administrative level.

Keywords: Public Administration, Priority, Information Systems, Processes, Public Service, Score

1 Introduction

In Germany, there are some federal laws in place that demand the public administration to become more and more digital. The most prominent regulations are the "E-Government-Gesetz" (Law on the promotion of electronic administration, [Bu13]), the "Registermodernisierungsgesetz" (RegMoG, Law introducing and using an identification number in public administration and amending other laws, [Bu21]) and the "Onlinezugangsgesetz" (OZG, Act for the Improvement of Online Access to Public Services, [Bu17]). The EGovG obliges public administration internally to provide electronic access channels and payment, accessible ("open") data, the documentation of processes, fully digital promulgations as well as to replace the written form with digital documents, using digital input as well as output methods. The RegMoG is also an internal set of rules to install a central and common ID for most databases in public administration as well as the Once-Only principle, which stands for the demand to re-use datasets of citizens instead of keeping multiple copies for different purposes. Apart from that, the

[1] HTWD University of Applied Sciences, Chair of Information Systems/Digital Administration, Friedrich-List-Platz 1, 01069 Dresden, Germany, tim.pidun@htw-dresden.de,
https://orcid.org/0000-0003-1331-1732
[2] HTWD University of Applied Sciences, Chair of Software Technology/Operating Systems, Friedrich-List-Platz 1, 01069 Dresden, Germany, dirk.mueller@htw-dresden.de

doi:10.18420/rvi2023-019

OZG takes the view of the user; it is designed to empower citizens to interact with public administration in a digital way. Originally supposed to be fully implemented by the end of 2022, its regulations included the obligation for federal and state administration to offer administrative services online through a portal according to the "Einer für Alle" principle (EfA, One for all), which means that a public service process that has been set up already must also be re-used and not be set up again in different formats or instances. Due to the fact that in Germany constitutive law ("Grundgesetz", [Pa49]) separates administrative responsibilities very strictly, every cooperation between the federal level, the sixteen states and the executing 11,000 municipalities below has to be negotiated and put down to legal regulations individually. Hence, the implementation was rather slow and by October 2022, only about 6% of the service processes (33 of planned 575) were available fully digital. Hence, the OZG is currently subject to revision in order to overcome the drawbacks and implement the lessons learned, which were mainly the complicated coordination of all players, missing standardization and a lack of liability [Na22], p. 5. Moreover, every service process was considered to be as "digital-to-be" important as the others, which means that there was no common sense on prioritization and is still not yet addressed in the drafts of the OZG 2.0. Players and affected parties again are afraid of a failure [MF23, Me21, Se21]. In the domain of Business and Administrative informatics, it is very common to consider these service processes as well as their technical implementation as Information Systems (IS) in the meaning of a sociotechnical system that is built to automate tasks [GRB04]. In this domain, there are even more well-established evaluation approaches that could be used to prioritize the digitalization of public services, e.g. the Technology Acceptance or the IS Success Model.

Hence, this contribution aims to build an easy-to-use prioritization score aligned to the specific demands of public service in Germany along a well-established transporting evaluation approach in order to quickly gain an overview of the different priorities in a set of public service processes. The remainder of the paper therefore is as follows: Chapter 2 discusses the problem Background from the governmental, administrative and user perspective, Chapter 3 frames the search for the appropriate evaluative approach as well as the demands of the domain and the proposal of a score calculation. Chapter 4 concludes, reviews the results and gives outlooks for future research and evaluation.

2 Background

2.1 Governmental/political perspective

Germany is a strong country in terms of economy with industrial companies belonging to worldwide leaders in mechanical engineering, automotive and chemical industry. The German economy according to the metrics GDP (PPP), i.e. gross domestic product based on purchasing power parity, is the largest in Europe and ranks in the 5th place behind China, US, India and Japan in the world [In23]. On the other hand, in terms of degree of

digitalization, Germany is only ranked in the midfield of EU countries [Eu22]. Since the digitalization is widely considered as a key factor for future economical and social development, this discrepancy casts a shadow on the future development of Germany. Recent cases illustrating some problems are a 2-day delay of some final exams (Abitur) in the state North Rhine-Westphalia due to an insufficiently dimensioned server [Se23], the discontinuity of media sometimes increasing instead of decreasing the effort [Ti23], and a tiny online percentage of 0.6% in 2021 for online motor vehicle licensing [Ch23], a huge service with >20m annual cases. Reasons are an inadequate infrastructure, a narrowed view on processes intermixing real digitalization with simplistic digitization, and a lacking focus on cornerstones like digital identity cards for citizens with typical hurdles like usability and extra costs.

In this context, it is worth noting that the political institution "Normenkontrollrat" (regulatory control council) that reviews and controls the effectiveness and efficiency of laws and regulations in Germany strongly recommends timely and swift OZG review and execution [Mi23a] and even the German CIO, located at the Federal Ministry of the Interior and Community doubts the effectiveness of digitalization in case of lacking prioritization [Mi23b]. Taking these different viewpoints on "digitalization" into account, three different levels of execution can be addressed [Jö22]: First, the mere electronification of analog documents and processes in a digital form without adaption of organizational or process structures, thus just addressing the citizen as user of the service, second the digitalization of service structures and processes to implement a fully digital communication with the citizen, thus addressing both internal and citizen participants of the processes, and third a transformation of authorities by adaption of staff and qualification structures and institutional cultural change. As the transformative change level cannot be addressed mainly by an information systems approach, it will not be considered further in this contribution.

Hence, it is of importance to what extent digital change is desired and to what extent the "success" of the IS is defined: either the goal of electronification of access and administrative objects (as low level-objective) or the goal of digitalization, hence the offer of more or less fully digital citizen-faced-processes (as high level-objective). The biggest problem though - with interaction to all mentioned phenomena - is the expected lack of 140,000 IT specialists in Germany's public service in 2030. 1.5m IT workers will retire until 2030. Only part of their knowledge might be transferred to their successors. The total manpower shortage then might sum up to almost one million people [Mc23].

2.2 User(s)/working perspective

One of the key problems for the shortage of staff are the rather unattractive conditions in public administration compared to the private sector [HP22], p. 25 and the common notion of a rather bureaucratic, rigid, security-driven work structure [Fu22], p. 23. These obstacles are of organizational and legal shape, both formally and informally, [Pe17] p.

159 and hence cannot primarily be addressed by digitalization and appropriate information systems. Though, the same source also names technological and technology-acceptance-related obstacles and thus, this leads to the claim of a rather user-centric design of information systems in public administration [Pe17], p. 163 and the use of evaluation schemes such as [Pa85]. In Funke [Fu22], p. 23, the importance of a general public-service culture to motivate the user as well as the actual intention to use, supported by a user-centric design of public service processes is demanded. With the first again being rather of political-organizational quality (and therefore not in the scope of this contribution), the second claim is also backed up by Einhaus [Ju19] who highlights direct user participation to foster acceptance and usage. These thoughts point to the need to consider two different levels of technology acceptance in public service: The organizational and the individual level (see also [WCM07]), representing the professional users in administration (synonymously organizational key users, employees, officers) as well as the citizen users. Parasuraman et al. [Pa85] point to the individual level as the end-users/citizens need to evaluate the service, whereas common IS Success models do not distinguish between professional and citizen users; given the fact that traditionally, information systems are designed to automate the working tasks of the professional users.

In Germany, a maturity level for OZG service processes exists that also takes the perspective of the citizen user. It consists of five levels from 0 – no information available, 1 – service description and application form is available online as PDF (starting the electronification level, see Chapter 2.1), 2 – online application possible, documentations and notifications are being sent via mail (starting the digitalization level, see Chapter 2.1), 3 – application, document supply to as well as notifications from the authority all run fully digital and 4 – application via data supply according to the Once-Only-principle [Bu23].

Hence, it could be of specific interest if an analogue process should be initially lifted to level 1 first or if it would be of bigger impact to shift a process from level 2 to 3 to avoid mail traffic and gain time. Hence, we use two different user concepts in order to categorize the addressees of Information success; the professional user in public administration whose day-to-day tasks are about to be automated and the citizen user that occasionally uses information systems to interact with the public administration.

2.3 Administrative/service perspective

Whereas Ganswindt [Ti23] claims that one of the key problems of digitalization in public services would be the technical adaption and execution, most sources confirm the above-mentioned lack of staff as a key obstacle for successful digitalization, e.g. [RH20], p. 10. Though, the technical part of information systems (besides task and human [GRB04]) must not be unattended; both professional and citizen users rely on information technology to user public services. In this context, the professional users in administration should run appropriate application systems and infrastructural (Platform-) Hard- and Software, the latter comprising all classic architectural levels (Presentation, Business Logic and Data

Layer). The same is true to citizen users; they need appropriate and accessible infrastructure, e.g. their own mobile devices with access to the presentation layer of the publicly available application systems. Key drivers in this context could be the cost for administration and the citizen user, the savings related to time and money when digital services are being used, as well as a certain consideration of sustainability by means of fitness for multi and re-use of IT and IS systems.

Hence, the technical infrastructure/platform availability and usage of appropriate application systems must be taken into consideration when it comes to evaluating Information systems from the professional users' view. The citizen user needs private infrastructure and accessibility/usability of the public service presentation layer, which finally drives its recognition as successful Information system.

2.4 Summary

Summarizing the three perspectives of public service digitalization and adapting the problem to the IS model, following selective aspects for appropriate IS Success approaches can be stated (Table 1): The different concepts that need to be considered in the evaluation as well as potential prioritization drivers.

Application perspective	IS Structure	Selective Aspects					
		Considered concept			Prioritization drivers		
User(s)	Human	Process Executive					
		Citizen User	Professional User		Amount of annual cases	Amount of process participants	
Govern-mental	Task	IS Success Objective					
		Low-level electroni-fication	High-level digitalization		Importance or Impact	OZG level shift	
Adminis-trative	Tech-nology	IT Systems					
		Infra-structural Hardware	Infra-structural Software	Applic ation Sys-tems	Cost	Savings	Sustain-ability

Tab. 1. Selective aspects for IS evaluation approaches

3 Investigation

3.1 Review of Evaluation Approaches

From April to June 2023, we performed a structured review in multiple databases along the search terms (“IS” or “Information Systems”) and (“success” or “evaluation”) and (“public” or “administration”) that resulted in 29 papers which were supposed to give us an overview on the most common IS evaluation approaches used in public service. In a first review round, we screened the papers according to their abstracts and filtered seven matching contributions that could be considered as not too much specific by means of application of an evaluation approach to a specific country and administration domain. These seven papers were thoroughly reviewed according to their content and this resulted in a total of three studies that may act as reviews themselves, hence giving a good overview of the body of investigation.

The first meta study from 2021 [St21] features a review of 28 studies in which the type of evaluation model was determined. They found that in 55% of all cases, the DeLone and McLean IS Success (ISSM, [DM92]) was used; 4% (one occurrence in Gambia) used the Technology Acceptance Model (TAM) by Davis et al., [FRP89] 41% used combinations or refinements of ISSM and TAM and again 4% were represented by (one) new model from Turkey. A second review from 2023 [Vu23] found 72 papers with confirmatory results (ISSM 52%, TAM 1%, combined models 43% and new ones 4% along with their own setup that will be discussed a little later on). Nkanata [Nk13] also advocates the use of ISSM in public service. Summing up, most of the applications of IS evaluations in the public sector used the ISSM; we support this view and hence use the ISSM as model for further investigations and adaptions.

3.2 Application of Selective Aspects

The original edition of the ISSM [DM92] featured two, the latest updated model three success dimensions and all in all six success dimensions [DM03]. Its overall validity and reproducibility has been proved for many years. In this model, System, Information and Service Quality drive Intention to use and tightly connected, Use as well as User Satisfaction that ultimately contribute to Net Benefits. They are considered to act as dependent variables [DM92] and are driven themselves by success metrics according to the IS they are applied to. In the context of public administration, Nkanta investigated 34 Studies and found that most applications of ISSM in public service were not connected to all of the six dimensions as DeLone and McLean demanded, but would rather be restricted to Information and Service Quality as well as User Satisfaction constructs [Nk13, S. 299]; we therefore stick to the ISSM recommendations and keep on considering the entire set of success dimensions. The above-mentioned success metrics for the success dimensions have explicitly been described by Petter, DeLone and McLean ten years later as 43 independent variables or determinants of IS success that can be put down to four

categories: Task, User/People and Structure (which is divided into Project and an Organizational) [SWE13]. The categories are derived from the IS definition of Leavitt [LE65] and drive IS System Success on the right. Moreover, the categories directly match the model of the Information System [GRB04] and their structure of human, task and technology.

17 of the success metrics consistently relate to all the six success dimensions and therefore are considered to represent the connection clearest. The extent to which they contribute to the specific success dimensions is categorized into strong (90% of all 450+ cases) and moderate support (67-89%). [SWE13, S. 39]. We therefore limited ourselves to these strong supportive determinants in a first step (Explanations are from Petter et al.'s paper unless otherwise stated). If no direct or only moderate supporting determinants from the table on page 39 were noted, we retrieved all supported relationships from the extended tables A1-A5 on pages 54 to 61 in a second step and filtered them according to their strong impact on the overall IS Success according to Table 9. Results are shown in Table 2 on the following page. Due to space restrictions, exhaustive explanations and a derived causal ISSM model for public administration in Germany are given in [PM23].

In a last step, the resulting drivers were compared to the selective aspects in Table 1 along with the consideration of the generic explanations. Summing up, every success driver out of the literature could be backed up by one or more selective aspects of the considerations in Chapter 2.4. We therefore suggest using the ISSM as validated transporting model as well as the selective aspects to explain the input to as well as the output of IS Success (drivers) in the case of Public Administration in Germany.

3.3 Prioritization Approach

To form a prioritization approach, we operationalize the above collected selective aspects in order to evaluate their occurrence (cf. Table 3 on the following page). The aspects are abbreviated with single characters that are the variables of the calculation for the Indicator of Prioritization (Prio).

Success Dimension [SWE13]	Success Drivers [SWE13]	Explanation [SWE13]	Selective Aspects
System Quality	Self-efficacy	Belief of Capability to be able to perform tasks with an IS	Citizen User and Professional User
	Technology Experience	Capability to perform tasks with an IS	

Information Quality	IT Infrastructure	n/a	Low level electronification and high-level digitalization Infrastructural Software, Hardware and Application Systems
	Trust	n/a	
Service Quality	Ease of use [Al22]	the degree of which an individual believes that using a specific system would be free of effort [FRP89]	OZG level shift Low level electronification and high-level digitalization
	Utility [Al22]	the degree to which a user believes services were (…) beneficial [Al22, S. 10]	Importance or Impact
Intention to use	Extrinsic Motivation	Incentives or pressure by the organization to use the IS	Amount of annual cases
System Use	Organizational Competence	The knowledge possessed by the management of a firm about IS	Process participants
User Satisfaction	User expectations	n/a	Low level electronification and high-level digitalization
	Attitudes towards technology	user characteristics (…) toward technology (…) that can be influenced through setting proper expectations	
	Task compatibility	The consistency of the technology with the work processes or work styles	Citizen User and Professional User
Net Benefit	Management support	The willingness to allocate time, resources and encouragement for the use of an IS	Cost, Savings and Sustainability

Tab. 2. Application of selective aspects to the ISSM Success drivers

Considered Concept	Selective Aspects	Explanation	Proposed value
Input values			
Process Executive	Citizen User and Professional User (u)	If an IS is designed to serve the citizen user as well as the internal professional user, the impact and visibility of the process is much higher and hence the priority should rise	If only Professional User: multiply by 1. If Citizen Users affected: multiply by 2
	Amount of annual cases (e)	The more cases the process needs to cover, the higher the importance and automation potential of the process	Below 10: plus 0. Below 100: plus 1 etc. (e= int(lg(cases))).
	Process participants (p)	The more process participants, the more complex the process will be and hence the more potential for optimization and automation rises. This also covers processes that interact between state and federal level	Below 5: plus 0. Below 10: plus 1, below 15 plus 2, below 20 plus 3, above 20 plus 4
IS Success Objective	Low level electronification and high-level digitalization (d)	If the process is just set up to imitate the common analogue process, the effort and success are lower than the digitalized, customer-faced process	If only electronification: multiply by 1. If digitalization approach: multiply by 2
	Importance or impact (i)	This is the political adjusting screw that can be used to prioritize manually. It should be used in a conscious manner and only a balanced set of processes should be of high or critical prioritization	Normal: multiply by 1. High: multiply by 2. Critical: multiply by 3
	OZG level shift (o)	The delta between the initial OZG level of the process and its level after implementation	Add 0-4
IT Systems	Infrastructural Software, Hardware and Application Systems (t)	If infrastructural Soft- and Hardware as well as new Applications are needed, the project complexity rises, even more, if Hard- and Software for the citizen user is necessary.	Every functional entity: Add 1; if citizen users are involved: multiply by 2

Output values			
Prioritization drivers	Cost (c)	The projected (ex ante) or real cost (ex post) of the project implementation. Cost and Savings must both be compared from the same perspective and including all cost categories such as material, labor etc.	Amount in €
	Savings (s)	The projected (ex ante) or real savings (ex post) of the project implementation.	Amount in €
	Sustainability (y)	Does this project contribute to the "Once Only" or the "One for all" principle?	If yes, multiply savings by 2

Tab. 3. Proposed operationalization of process prioritization

The main goal of the prioritization is to form an indicator that can easily be put into an order to be compared to other processes. Hence, we argue to rise the indicator if input complexity rises as well as the ratio between savings and cost; both as addition put down to following formula:

$$Prio=Input+Output \quad (1)$$

$$Input = ((e + p) \cdot u) + (o \cdot i \cdot d) + (t \cdot u) \quad (2)$$

$$Output = \frac{s \cdot y}{c} \quad (3)$$

To initially test the plausibility of the prioritization approach, we performed two example calculations for typical administration processes in Munich and the Uckermark region. Due to space restrictions, they are set out in an accompanying document [PM23].

4 Conclusion and critical review

This contribution aimed to construct a prioritization approach that can be used to put specific public service digitalization projects in Germany into a meaningful order. To do so, we collected selective aspects of public service digitalization in Germany and performed a structured review for IS evaluation approaches from the domain of Business and Administrative Informatics with special consideration of their applicability to the set of aforementioned public service processes. We then operationalized the so found success drivers aligned to the success dimensions of the host success model and proposed a simple formula to calculate a prioritization score. We are clear that this model is designed especially for Germany, but the same approach can be used for other countries as well.

The main difference might be the application of different laws, resulting in the use of different selective approaches and drivers. The calculation of the score is our first attempt; we therefore welcome its review and challenge in practice.

Our next scientific approaches are the evaluation of the approach in real life along a process catalog and hence we are welcoming offers from public service. Furthermore, we will compare the success drivers that we claim to foster IS success to the success factors that Escobar et al. collected in their 2023 Study on Success drivers [EAV23]. These approaches could unfortunately not be included in this publication for reasons of space.

All in all, we rather gave preference to the relevance of the reviewed literature strongly related to public service instead of an exhaustive theoretical foundation [vo15]. Hence, we preferred the discussion of rather few specific contributions to a sensitive research with a high amount of relevant studies, but time-consuming selection [PR06] Moreover, due to still open license negotiations, it is still not possible to assess publications from Science Direct or Elsevier in various parts of Germany and so during this research, literature dating from 2019 on could not be retrieved from these publishers.

References

[Al22] Al-Rahmi, W. M. et al.: Validation of an Integrated IS Success Model in the Study of E-Government. Mobile Information Systems 2022, S. 1–16, 2022.

[Bu13] Bundestag: Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG); Electronic Administration Promotion Act), 2013.

[Bu17] Bundestag: Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG), 2017.

[Bu21] Bundestag: Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz - RegMoG), 2021.

[Bu23] Bundesministerium des Innern und für Heimat: Reifegradmodell. https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-reifegradmodell/info-reifegradmodell-node.html, Stand: 2023-05-22.

[Ch23] Christian Wölbert: Typisch deutsches Digitaldesaster: Die Online-Autozulassung i-Kfz. https://heise.de/-7547529, Stand: 2023-05-22.

[DM03] DeLone, W. H.; McLean, E. R.: The DeLone and McLean model of information systems success: a ten-year update. Journal of Management Information Systems 4/19, S. 9–30, 2003.

[DM92] DeLone, W.; McLean, E.: Information Systems Success: The Quest for the Dependent Variable. Information Systems Research 1/3, S. 60–95, 1992.

[EAV23] Escobar, F.; Almeida, W. H.; Varajão, J.: Digital transformation success in the public sector: A systematic literature review of cases, processes, and success factors. Information Polity 1/28, S. 61–81, 2023.

[Eu22] European Commission: The Digital Economy and Society Index (DESI), 2022.

[FRP89] Fred D. Davis; Richard P. Bagozzi; Paul R. Warshaw: User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science 8/35, S. 982–1003, 1989.

[Fu22] Funke, C.: DIGITIZATION, FAST AND SLOW; Comparing the creation of digital public services in Denmark, France and Germany. Phdthesis, 2022.

[GRB04] Grob, H. L.; Reepmeyer, J.-A.; Bensberg, F.: Einführung in die Wirtschaftsinformatik. Vahlen, 2004.

[HP22] Handke, S.; Pidun, T.: Fit fürs Amt. Notwendigkeit und Ansätze der Schärfung von Kompetenzanforderungen und Ausbildungsprofilen für die Digitalisierung der Verwaltung. FifF-Kommunikation 3/39, S. 22–28, 2022.

[In23] International Monetary Fund. Research Dept.: World Economic Outlook, April 2023: A Rocky Recovery. International Monetary Fund, 2023.

[Jö22] Jörg Bogumil et al.: Bürgernahe Verwaltung digital? Digitalisierung und Automatisierung im Praxistest. Bonn Friedrich-Ebert-Stiftung, 2022.

[Ju19] Juliane Einhaus: <Ohne Beteiligung sinkt immer die Akzeptanz>. https://www.vdz.org/digitalisierung-von-staat-verwaltung/ohne-beteiligung-sinkt-immer-die-akzeptanz, Stand: 2023-05-22.

[LE65] Leavitt H. J.: Applied Organizational Change in Industry, Structural, Technological and Humanistic Approaches. Handbook of Organizations 264, 1965.

[Mc23] McKinsey & Company: Studie: Im öffentlichen Dienst fehlen bis 2030 140.000 IT-Fachkräfte. https://www.mckinsey.de/news/presse/2023-01-25-it-talent-im-public-sector, Stand: 2023-08-25.

[Me21] Mergel, I.: 19. Digital Transformation of the German State. In (Kuhlmann, S. et al. Hrsg.): Public Administration in Germany. Springer International Publishing, Cham, S. 331–355, 2021.

[MF23] Mario Martini; Fedor Ruhose: Das Digitaldesaster liegt nicht am Geld - im Gegenteil. Wirtschaftswoche, May 2023.

[Mi23a] Michael Linden: Normenkontrollrat rügt Regierung wegen mangelnder Digitalisierung. https://glm.io/173639, Stand: 2023-05-22.

[Mi23b] Mitteldeutscher Rundfunk: Warnung vor falschen Prioritäten, Videotext, 24.04.2023, p. 119.1, 2023.

[Na22] Nationaler Normenkontrollrat: Jahresbericht 2022; Bürokratieabbau in der Zeitenwende; Bürger, Wirtschaft und Verwaltung jetzt entlasten, 2022.

[Nk13] Nkanata, M. G.: Applying DeLone and McLean information systems success model in the evaluation of e-government initiatives: a literature review. In (Neil, E.; Ocholla, D. N. Hrsg.): Proceedings of 13th annual IS conference. Empowering and inspiring current information studies worldwide. Department of Information Studies, University of Zululand, Kwadlangezwa, S. 287–312, 2013.

[Pa49] Parlamentarischer Rat: Grundgesetz für die Bundesrepublik Deutschland, 1949.

[Pa85] Parsu Parasuraman, Valarie Zeithaml, Leonard Berry: A Conceptual Model of Service Quality and its Implication for Future Research (SERVQUAL). The Journal of Marketing 49, S. 41–50, 1985.

[Pe17] Pereira, G. V. et al.: Categorizing Obstacles in E-Government: Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance. Association for Computing Machinery, New York, NY, USA, S. 157–166, 2017.

[PM23] Pidun, T.; Müller, D.: A Scoring Model for Public Administration Process Prioritization in Germany. Accompanying Explanations, Visualisations and Examples. http://dx.doi.org/10.13140/RG.2.2.27796.88964, Stand: 2023-08-25.

[PR06] Petticrew, M.; Roberts, H.: Systematic reviews in the social sciences. A practical guide. Blackwell, Oxford, 2006.

[RH20] Räckers, M.; Halsbenning, S.: E-Kompetenzen. In (Klenk, T.; Nullmeier, F.; Wewer, G. Hrsg.): Handbuch Digitalisierung in Staat und Verwaltung. Springer Fachmedien Wiesbaden, Wiesbaden, S. 1–13, 2020.

[Se21] Sebastian Płóciennik: Digitalisation in Germany: an overview and what lies behind the delays. OSW Commentary Number 417 22.11.2021. http://aei.pitt.edu/103779/, Stand: 2023-08-25.

[Se23] Sebastian Grüner: Serverüberlastung führte zu Abi-Chaos in NRW, https://glm.io/173615, Stand 2023-08-25.

[St21] Stefanovic, D. et al.: Information systems success models in the E-government: context: A systematic literature review: 2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH), S. 1–6, 2021.

[SWE13] Stacie Petter; William Delone; Ephraim R. Mclean: Information Systems Success: The Quest for the Independent Variables. Journal of Management Information Systems 4/29, S. 7–61, 2013.

[Ti23] Till Ganswindt: Warum die öffentliche Verwaltung mehr Digitalisierung braucht. https://www.mdr.de/nachrichten/deutschland/wirtschaft/fachkraeftemangel-digitalisierung-verwaltung-100.html, Stand: 2023-05-22.

[vo15] vom Brocke, J. et al.: Standing on the Shoulders of Giants. Communications of the Association for Information Systems 37, 2015.

[Vu23] Vuckovic, T. et al.: The Extended Information Systems Success Measurement Model: e-Learning Perspective. Applied Sciences 5/13, S. 3258, 2023.

[WCM07] Wimmer, M. A.; Codagnone, C.; Ma, X.: Developing an E-Government Research Roadmap: Method and Example from E-GovRTD2020. In (Wimmer, M. A.; Scholl, J.; Grönlund, Å. Hrsg.): Electronic Government. Springer, Berlin, Heidelberg, S. 1–12, 2007.

Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
96 Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023

Wer zwitschert denn da?

Autorenschaftsattribution mittels stilistischer Merkmale für kurze Social-Media-Nachrichtentexte

Katharina Luger[1] und Jörg Schmittwilken[2]

Abstract: Zur Bekämpfung von Computerkriminalität sowie zur Wahrung der Informationssicherheit ist es vielfach notwendig, die Autorenschaft von Texten zu kennen oder zu ermitteln. Gerade die Zuordnung anonymer Texte zu einer möglichen Autorin oder einem möglichen Autor ist in diesem Kontext ein häufig zu lösendes Problem. Beispielsweise muss im Rahmen der Ermittlungsarbeit zu Hass-Kommentaren die Menge möglicher Autor:innen bestenfalls auf eine Person reduziert werden. In diesem Beitrag wird ein Modell zur Autorenschaftsattribution vorgestellt, das mithilfe von maschinellem Lernen aus einem Datensatz mit den Tweets von 915 Twitter-Accounts gelernt wurde. Das Modell basiert auf Support-Vector-Machines. Der Fokus des Beitrags richtet sich auf das Feature-Engineering, also der Erstellung sowie der Auswahl von Merkmalen, auf denen das Modell basiert. Es werden Feature sowie andere Modellparameter vorgestellt, die eine Klassifikationsgenauigkeit von bis zu 63% erzielen.

Keywords: Informationssicherheit, Computerkriminalität, Autorenschaftsattribution, Maschinelles Lernen, Suppport-Vector-Machine, stilistische Merkmale

1 Motivation

Die Zuordnung der Autorenschaft eines Textes zu einer Person ist auch in vielen Kontexten der öffentlichen Verwaltung interessant und in Bezug auf die Informationssicherheit von höchster Bedeutung. So stehen beispielsweise Strafverfolgungsbehörden im Rahmen der Ermittlungsarbeit von Computerkriminalität häufig vor dem Problem, anonyme Texte einer Absenderin oder einem Absender zuordnen zu müssen – sei es bei anonymen oder extremistischen (Hass)postings in Internetforen

[1] Absolventin im Studiengang Verwaltungsinformatik der Hochschule des Bundes für öffentliche Verwaltung, katharina.luger@vit-bund.de
[2] Hochschule des Bundes für öffentliche Verwaltung, Studiengang Verwaltungsinformatik, Gescherweg 100, 48161 Münster, schmittwilken@vit-bund.de, https://orcid.org/0009-0009-4424-3008

doi:10.18420/rvi2023-025

[AC05], im Chatverlauf beschlagnahmter Smartphones oder gar bei der Analyse des Codes von Schadsoftware [Ka19].

Auch im Rahmen der Plagiatserkennung ist die Identifikation der Autor:in der Originalquelle eine hilfreiche Information. Ferner kann im Rahmen der Betrugsbekämpfung die Herleitung von Information über die Autorenschaft eines Textes (z. B. einer Phishing-Mail oder einer gefälschten Bewertung) bei der Verbrechensaufklärung helfen.

Diese Zuschreibung von Texten zu deren Verfasser:innen wird als Autorenschaftsattribution (engl. authorship attribution) bezeichnet und ist Gegenstand dieses Beitrags. Viele Arbeiten zur Autorenschaftsattribution verwenden Textkorpusse mit langen Texten wie Dokumenten, Reden, E-Mails o.ä. [Sc13; BMA13]. Diese eigenen sich aufgrund der Vielzahl der in den Texten enthaltenen Merkmale besonders gut und erzielen hohe Genauigkeiten bei der Zuweisung der Autor:innen.

Kennzeichnend für Social-Media-Nachrichten, die im Fokus dieses Beitrags liegen, ist jedoch ihre Kürze, das häufige Ignorieren grammatikalischer Regeln sowie die starke Verwendung von Emojis, sodass die Attribution der Autorenschaft bei diesen Texten schwieriger und weniger stark untersucht ist [Ro16; Sc13; BMA13].

Im Fokus dieses Beitrags steht die Forschungsfrage, ob geeignete Features konstruiert werden können, durch die eine Autorenschaftsattribution auch bei sehr kurzen Social-Media-Texten möglich ist.

Im Folgenden wird nach der Darstellung der verwandten Arbeiten in Abschnitt 2 ein auf Support-Vector-Machines basierendes Modell zur Autorenschaftsattribution vorgestellt, das für Texte des Kurznachrichtendienstes Twitter (s. g. Tweets) optimiert ist (Abschnitt 3). Der Fokus wird anschließend auf das Feature-Engineering, also die Auswahl der verwendeten Merkmale (Abschnitt 4) und die Güte der Klassifikation (Abschnitt 5) gelegt. In Abschnitt 6 wird die Arbeit zusammengefasst und es wird ein Ausblick gegeben.

2 Verwandte Arbeiten

Autorenschaftsattribution ist seit vielen Jahren Gegenstand der Forschung im Bereich des Maschinellen Lernens. In diesem Teilgebiet der künstlichen Intelligenz werden mithilfe von Lernalgorithmen Modelle aus Trainingsdaten gelernt. Diese Modelle können dann zur Klassifikation neuer Daten verwendet werden. Die Arbeiten im Bereich der Autorenschaftsattribution unterscheiden sich im Wesentlichen hinsichtlich der eingesetzten Lernmethode sowie der verwendeten Trainingsdaten. Zudem unterscheiden sich die Ansätze in Art, Anzahl und Umfang der verwendeten Feature. Eine Übersicht möglicher Verfahren zur Autorenschaftsattribution geben [Ro16; St09].

Etabliert sind für diese Anwendung insbesondere die leistungsfähigeren überwachten Lernalgorithmen wie Deep Learning auf Basis künstlicher neuronaler Netze, Random-

Forrests oder Support-Vector-Machines (SVM). Aber auch einfache statistische Ansätze wie Naive Bayes sowie N-Gramme werden zu diesem Zweck verwendet.

[BNJ03] stellen die *latent dirichlet allocation* (LDA) als generatives, probabilistisches Modell eines Textkorpus vor, das es ermöglicht, die latent im Text beinhalteten Themen zu identifizieren. Hierzu modellieren sie die Themen durch eine charakteristische, multinominale Verteilung von Worten.

[AMM17] zeigen ein Konzept zur Autorenschaftsattribution von Werken der arabischen Poesie. Sie setzen zur Klassifikation Naive Bayes sowie SVM ein. [Di03] wählen zur Identifikation der Autoren deutscher Zeitungsartikel ebenfalls SVM. Beim Feature-Engineering kommen unter anderem Part-of-speech-Tagging sowie N-Gramme zum Einsatz. Sie erzielen mit dem Ansatz eine Trefferquote von 60-80%. [Sc13] stellen die Konzepte der *signatur* sowie *flexible pattern* kurzer Social-Media-Nachrichten vor, mit deren Hilfe sie die Autorenschaft dieser Texte attributieren können. Sie schlagen die Verwendung dieser Metriken z.B. zur Klassifikation mithilfe von SVM vor und erzielen hiermit Genauigkeiten von bis zu 70%. [BMA13] stellen die Autorenschaftsattribution von Tweets im Rahmen forensischer Analysen vor. Hierzu verwenden sie insbesondere stilometrische Merkmale zur Klassifikation mit SVM und erzielen Genauigkeiten von bis zu 90%.

[CS03] vergleichen die Verwendung von N-Grammen und naive Bayes Ansätzen zur Autorenschaftsattribution sowie zur Bestimmung des Topics von langen Texten.

3 Methodik

Die Vorgehensweise folgt einem häufig anzutreffenden Vorgehen im Bereich der Autorenschaftsattribution. Als Datengrundlage kam eine Sammlung aller öffentlichen Tweets von 915 berühmten Twitter-Nutzer:innen zum Einsatz. Der User Ahmed Shahriar Sakib veröffentlichte diesen Datensatz unter der Lizenz „*for educational purposes only*“ [Sa22] auf der Internetseite Kaggle [Sa22].

Um die Arbeit mit dem vorliegenden Datensatz zu vereinfachen, werden einige Vorannahmen getroffen. Diese umfassen, dass jeder Tweet nur von einem Autor bzw. einer Autorin verfasst wurde, jeder Account nur von einer Person geführt wird und diese nicht versucht hat, den Schreibstil zu verfälschen.

3.1 Data Preparation

Zunächst wurde der Datensatz in einigen Schritten vorverarbeitet. Hierbei wurden unter anderem Zeichenketten, die nicht Teil des ursprünglichen Tweets sind, entfernt. Ein Beispiel hierfür ist der Zeitstempel der Veröffentlichung.

Zudem enthalten Social-Media-Nachrichten eine Reihe an domänenspezifischen Elementen wie Hashtags, Emojis, Hyperlinks und Referenzen, die einerseits Informationen über das Twitter-Verhalten einer Person liefern, andererseits durch detaillierte Analysen auch zu ungenaueren Ergebnissen führen können. [LWD] argumentieren beispielsweise, dass ein Großteil der Zeichen von Replies bereits vorgegeben ist, weshalb besonders bei kurzen Texten der Anteil an nicht selbst verfassten Zeichen sehr hoch sein kann. [Ro16] führen an, dass die Gefahr von Fehlzuordnungen von Tweets bei einer detaillierten Betrachtung sehr hoch ist, da überwachte Verfahren des maschinellen Lernens sehr viel Wert auf eine bestimmte User-Referenz legen, falls diese häufiger in Tweets vorkommt. Zudem fanden [LWD] bei ihren Untersuchungen zu Hashtags und Replies heraus, dass detaillierte Informationen der Hashtags kaum zur Verbesserung der Genauigkeit beitragen. Da derselbe Link meist nicht in mehreren Tweets vorkommt, werden alle Links bei [Ro16] und [Sc13] durch einen entsprechenden Tag ersetzt. Selbes gilt für Nummern, Datumsangaben und Uhrzeit [Ro16; Sc13]. Dieses Vorgehen soll auch hier Anwendung finden, indem alle eben genannten Komponenten durch die entsprechenden Tags `REF`, `HASH`, `URL`, `NUM`, `DATE` und `TIME` ersetzt wurden.

Besonders bei Emojis liegt die Vermutung nahe, dass Personen bestimmte Präferenzen bezüglich Art und Häufigkeit ihrer Verwendung besitzen. Diese Elemente sind im vorliegenden Datensatz in Form von UTF-8-Bytecode angegeben. Eine detaillierte Untersuchung der Emojis lag hier allerdings nicht im Fokus, weshalb auf eine aufwendige, differenzierte Betrachtung verzichtet wurde. Aus diesem Grund wurden hier alle alleinstehenden UTF-8-Bytecodes durch den Tag `EMOJ` ersetzt und somit nur ein Näherungswert der Verwendungshäufigkeit betrachtet.

Da nicht alle Tweets für eine Schreibstilanalyse relevant sind, mussten zudem einige Texte aus dem Korpus entfernt werden. Wie in verwandten Arbeiten wurde auf sämtliche Retweets verzichtet, da es sich hierbei üblicherweise um fremde Nachrichten handelt [Ro16; Sc13]. Zudem ist die Identifikation der Sprache nicht Teil der hiesigen Betrachtungen, weshalb auf eine entsprechende sprachliche Differenzierung verzichtet wurde. Um nur englische Tweets zu untersuchen, wurde ein Großteil der anderssprachigen Texte ausgeschlossen. [Ro16] sowie [Sc13] entfernen zudem kurze Nachrichten, die zu wenige Informationen über den Stil der verfassenden Person enthalten. Auch hier wurden deshalb alle Tweets gelöscht, die weniger als drei Komponenten beinhalten. Hierbei bilden Worte, Satzzeichen und Tags jeweils einzelne Komponenten.

Ebenfalls zu berücksichtigen ist der Zeitpunkt der Veröffentlichung, da sich der Stil einer Person mit der Zeit verändern kann. Um eine mögliche Stiländerung über die Jahre zu berücksichtigen, fanden nur Tweets der letzten 24 Monate Verwendung. Zuletzt wurden nur Profile verwendet, die nach der Vorverarbeitung noch mehr als 300 Tweets besitzen und sämtliche Usernamen mit einer Nummer ersetzt.

3.2 Text Representation Strategy

In der Stilanalyse werden aus einem Text sogenannte Features / Merkmale extrahiert (Feature-Extraktion). Diese stellen den Stil einer Person näherungsweise dar [HS14]. In der Literatur wird eine Vielzahl an möglichen Feature-Typen untersucht und diskutiert. Diese werden in der Regel in verschiedenen Kategorien zusammengefasst. [AC08] unterscheiden beispielsweise zwischen lexikalischen, syntaktischen, strukturellen, inhaltsspezifischen und idiosynkratischen Merkmalen.

Um ein möglichst genaues Modell zu erhalten, müssen geeignete Feature-Typen gewählt werden, da nicht alle für jeden Anwendungszeck sinnvoll sind. In der Regel werden mehrere dieser ausgewählt und in einem Feature-Set zusammengefasst.

Um die Eignung der Merkmale auch bei besonders kurzen Texten zu prüfen, wurden die gewählten Feature-Typen für jeden Text einzeln extrahiert und zu einem Vektor zusammengefasst. Hier wird also der sogenannte instanzbasierte Ansatz verfolgt, bei dem jeder Text einen Vektor bildet, der den Schreibstil der verfassenden Person repräsentiert [St09].

3.3 Feature-Selektion

Da einige Feature-Typen eine sehr hohe Anzahl an Dimensionen annehmen können, wird nach Erhebung der Vektoren in der Regel eine Feature-Selektion durchgeführt. Hierbei wird die Zahl an Features reduziert und somit die Performance eines Klassifikators verbessert [Sa20, S. 83].

Eine Strategie der Feature-Reduktion ist die Betrachtung der Auftrittshäufigkeit eines Merkmales, da besonders häufig auftretende Features besser in der Lage sind, stilistische Veränderungen zu erfassen. Bei Betrachtung der hier erhobenen Vektoren fällt auf, dass einige Feature-Typen eine besonders hohe Dimensionalität zur Folge haben, einige Merkmale aber kaum Aussagekraft aufweisen. Bei Funktionswörtern wurden deshalb alle Worte entfernt, die nicht oder nur einmal im gesamten Trainingsdatensatz vorkommen. [Ro16] entfernen bei N-Grammen sämtliche Features, die nur einmal im Datensatz zu finden sind, da diese in zukünftigen Texten wahrscheinlich nicht noch einmal auftauchen. Dieses Vorgehen wurde hier übernommen.

Bei Zeichen-N-Grammen wurde die Feature-Anzahl zusätzlich noch einmal auf die 10.000 am häufigsten vorkommenden Tetragramme reduziert. Dieser Feature-Typ hatte nach dem vorherigen Verarbeitungsschritt immer noch eine signifikant hohe Zahl an Dimensionen, was die zur Verfügung stehende Rechenkapazität zur Parameterwahl der Support Vector Machines und zum Erlernen des Klassifikators überstieg.

Insgesamt konnte eine Vielzahl an Merkmalen ausgeschlossen werden. Dabei mussten keine besonders relevant erscheinenden Informationen entfernt werden, insbesondere im Fall von Funktionswörtern, Wort- und Part-of-speech-N-Grammen.

3.4 Maschinelles Lernen

Im nächsten Schritt werden die erhobenen Vektoren einer Methode des maschinellen Lernens übergeben und somit ein Klassifikator erlernt. Analog zu u.a. [Ro16], [Sc13] und [BMA13] kamen auch hier SVMs zum Einsatz. [AC05; zitiert nach Zh06] führen an, dass sich SVMs für rauschende Daten eignen und mit hoch dimensionalen Vektoren umgehen können. Deshalb eignen sie sich besonders für die Analyse von Online-Nachrichten [AC05]. Verglichen mit Deep Learning, das vor allem in den letzten Jahren im Bereich der Autorschaftsanalyse zunehmend an Popularität gewann, eignen sich SVMs besser für den hier betrachteten Einsatzzweck. [Ro21] stellten bei ihren Untersuchungen an russischen Texten fest, dass SVMs besonders dann eine signifikant bessere Leistung erbringen, wenn nur eine begrenzte Textlänge zur Verfügung steht, da neuronale Netze mehr Trainingsdaten benötigen, um informative Merkmale aus dem Text zu extrahieren. Die verfügbaren Daten könnten in realen Situationen [Ro21] – wie auch in den hier durchgeführten Experimenten, in denen relativ wenige und besonders kurze Texte (max. 280 Zeichen) pro Autor:in verwendet werden – nicht ausreichen, um exakte Ergebnisse mit Deep Learning zu erzielen [Ro21].

Die SVM gehört zu den sogenannten überwachten Lernverfahren, welche sich dadurch auszeichnen, dass die Daten gelabelt sind, die Zuordnung von Autor:in und Text also bereits vorliegt [AC08]. Im Schritt des Lernverfahrens wird nun versucht, die Trainingsdaten optimal zu trennen. Im einfachsten Fall (2 Autor:innen) wird im zweidimensionalen Raum eine lineare Trennlinie gesucht, welche die Datenpunkte bzw. Textinstanzen der Personen teilt und somit zwei Klassen bildet [Sa20, S. 123]. Bei Prüfung unbekannter Instanzen, sollten diese vom Klassifikator idealerweise der richtigen Klasse zugeordnet werden.

Zum Trainieren und Testen der Modelle werden Datensätze üblicherweise in Test- und Trainingsdaten unterteilt. Um trotz kurzer Texte möglichst gute Ergebnisse zu erzielen und gleichzeitig noch genug Autor:innen mit einer ausreichenden Anzahl an Instanzen zu behalten, wurde ein Verhältnis von 4:1 (240 Trainings- und 60 Test-Tweets pro Account) festgesetzt.

4 Auswahl der Merkmale

In der vorliegenden Arbeit bestand der Fokus darin, Feature-Typen zu ermitteln, die für die Anwendung im Social-Media-Bereich besonders sinnvoll erscheinen. Eine Übersicht des erarbeiteten Feature-Sets ist in Tab. 1 abgebildet.

Lexikalische Merkmale, welche die Verwendung einzelner Worte und Zeichen bzw. Zeichenketten untersuchen, scheinen besonders im Bereich von Social Media sinnvoll. Aufgrund der weniger strengen Vorgaben bezüglich Grammatik und Rechtschreibung, wurden hier besonders große Unterschiede und Eigenheiten zwischen Personen vermutet.

Satzzeichen werden teils versehentlich falsch verwendet oder vergessen, aber von einigen Autor:innen auch bewusst als Stilmittel genutzt. So finden sich in manchen Tweets Auffälligkeiten wie z.B. „*!!!!*“. Aus ähnlichen Gründen wurde das Verhältnis zwischen Groß- und Kleinschreibung berücksichtigt. Daneben ist die durchschnittliche Wortlänge in der Literatur ein häufig aufgeführter Feature-Typ. Der Anteil an langen Worten entscheidet in der Regel mit darüber, wie komplex ein Text wirkt und ist auch von der Intention der verfassenden Person abhängig [Sa20, S. 31]. Da diese Faktoren auch im Social-Media-Bereich eine Rolle spielen, floss dieser Feature-Typ ebenfalls in die Betrachtung ein. Umgesetzt wurde dieser analog zum Ansatz von z.B. [We21] und [AC08], in welchem die durchschnittliche Anzahl an Zeichen pro Wort herangezogen wird.

Merkmalskategorie	**Feature-Typen**
Lexikalisch	· Verhältnis Satzzeichen zu Zeichen gesamt · Durchschnittliche Wortlänge · Verhältnis Groß- zu Kleinschreibung · Zeichen-Tetragramme (*n=4*)
Syntaktisch	· Häufigkeit Funktionswörter · POS-Monogramme (*n=1*) · POS-Bigramme (*n=2*)
Strukturell	· Anzahl Worte pro Nachricht · Anzahl Absätze
Inhaltsspezifisch	· Wort-Monogramme (*n=1*)
Social-Media-spezifisch	· Verhältnis Hashtags zu Token · Verhältnis Referenzen zu Token · Verhältnis URLs zu Token · Verhältnis Emoticons zu Token

Tab. 1: Übersicht der gewählten Feature-Kategorien und -Typen

Laut [Sa] sind in der Autorenschaftsattribution Zeichen-N-Gramme das erfolgreichste Feature und werden bei der Analyse von besonders kurzen bzw. Social-Media-Texten u.a. von [AC08], [Sh17], [Sc13] sowie [LWD] verwendet. Bei sogenannten N-Grammen wird der Text als Gruppen von Worten, Zeichen oder Tags dargestellt [Br17]. Die hier verwendeten Zeichen-Tetragramme stellen die Tweets als Sammlung von Zeichenketten mit der Länge 4 dar. Der Satz „*Das ist ein Beispielsatz.*“ würde durch die folgende Menge von Zeichen-Tetragrammen dargestellt: *{*`Das_`; `as_i`; `s_is`; `_is`; …; `satz`; `atz.`*}*. Leerzeichen wurden hier durch _ gekennzeichnet.

Warum Zeichen-N-Gramme so effektiv sind, ist nicht vollständig geklärt. [Sa] fanden allerdings heraus, dass die Erfassung von Präfixen und Suffixen, welche Informationen

über die Morphologie eines Wortes liefern, und Zeichensetzung, besonders zur Effektivität dieses Feature-Typen beiträgt. [St09] sieht einen Vorteil bei Zeichen-N-Grammen im Social-Media-Bereich darin, dass diese von rauschenden Daten z.B. in Form von Grammatik- oder Zeichensetzungsfehlern, nicht übermäßig beeinträchtigt werden. Zudem können Zeichen-N-Gramme Präferenzen bezüglich Groß- und Kleinschreibung wie z.B. CamelCase sowie Zeichensetzung, beispielsweise Smileys in Form von „ *;)* “, erfassen [Ro16].

[Ro16] untersuchten ebenfalls Twitter Texte mittels Zeichen-N-Gramme und kamen aufgrund ihrer guten Klassifikationsergebnisse zu dem Schluss, dass dieser Feature-Typ sehr wichtig für die Autorenschaftsanalyse von Social-Media-Texten ist. Sie konzentrierten sich hierbei auf Tetragramme, da kleinere n redundante Informationen und größere Werte ähnliche Hinweise wie die von Wort-N-Grammen erfassen würden [Ro16]. Deshalb wurden hier ebenfalls Wort-Tetragramme in das Feature-Set aufgenommen.

Aufgrund der Vorteile von Wort- und POS-N-Gramme, welche auch auf Social-Media-Texte übertragbar sind, und der Feststellung von [Ro16], dass Zeichen-Tetragramme, Wort-Unigramme und POS-Uni- und POS-Bigramme 93% der Wichtigkeit ihres Feature-Sets ausmachten, wurden diese in die hiesigen Untersuchungen eingeschlossen. Sie funktionieren nach dem gleichen Prinzip wie Zeichen-N-Gramme. Anstelle von n-langen Zeichenketten, werden einzelne Wort oder POS-Tags, welche die zugehörige Wortart eines Begriffes abbilden, zur Darstellung der Texte verwendet.

Die Erfassung von Funktionswörtern hat sich in der Literatur ebenfalls als erfolgreich herausgestellt. Diese besitzen eine rein grammatikalische Bedeutung und werden lediglich genutzt, um Inhaltswörter zu verbinden [Be18]. [Ro16] sehen Funktionswörter im Bereich von Social-Media-Texten als besonders hilfreich an, da diese auch in kurzen Texten mit hoher Wahrscheinlichkeit auftreten. In der vorliegenden Untersuchung wird der Ansatz und die Wortliste von [We21] übernommen, welche eine Liste von 815 englischen Worten nutzten. Die Liste umfasste zum Zeitpunkt des Downloads 851 Worte und wurde von der Internetseite countwordsfree.com heruntergeladen.

5 Ergebnisse

Mittels Testdatensatz konnten die trainierten SVMs geprüft werden. Hierbei wurden zunächst eine Autorenschaftsattribution mit nur einem Feature-Typ, dann mit einer kompletten Feature-Kategorie und zuletzt mit dem kompletten Feature-Set mit steigender Anzahl an Autor:innen durchgeführt. Ermittelt wurde jeweils der Wert accuracy (Genauigkeit), welcher das Verhältnis zwischen der Anzahl korrekter Vorhersagen und der Anzahl aller Vorhersagen darstellt. Anhand der Ergebnisse erfolgte eine Einschätzung, wie gut sich die Feature-Typen für eine Autorenschaftsanalyse von kurzen Social-Media-Texten eignen.

Anzahl Autor:innen	Social-Media-spezifisch	Inhaltsspezifisch	Strukturell	Syntaktisch	Lexikalisch
5	0,4367	0,5033	0,3667	0,4233	0,6733
10	0,3350	0,4850	0,2350	0,4217	0,6167
20	0,2125	0,3667	0,1408	0,2575	0,4992

Tab. 2: Übersicht der Genauigkeit (accuracy) der Autorenschaftsattribution auf Basis der verschiedenen Feature Kategorien anhand von n zufälligen Autor:innen.

Die Ergebnisse der Autorenschaftsattribution mit allen Features innerhalb der jeweiligen Kategorie sind in Tab. 2 eingetragen. Demnach schneiden die strukturellen Merkmale erkennbar am schlechtesten ab. Dies lässt vermuten, dass strukturelle Eigenheiten aufgrund der Kürze der Texte, keine signifikanten Unterschiede aufweisen und Schreibstile von Autor:innen mit diesen Merkmalen nicht zuverlässig voneinander abgrenzbar sind.

Mit Social-Media-spezifischen Features konnten zwar bessere Ergebnisse erzielt werden, trotzdem wurden bei 20 Autor:innen nur knapp über 20 % der Texte richtig zugeordnet. Somit konnten Informationen zu Eigenheiten im Nutzungsverhalten solcher Elemente erfasst werden, im Vergleich zu anderen Feature-Kategorien schnitt diese Kategorie jedoch deutlich schlechter ab. Fraglich ist, ob eine genauere Erfassung von Emojis eine signifikante Verbesserung erzielt hätte.

Ähnlich verhält es sich mit syntaktischen Merkmalen, deren Ergebnisse hilfreich sein können, sich als alleinige Kategorie jedoch nicht eignen. Wie auch von [Ro16] festgestellt, schnitten die Wort-Monogramme (hier inhaltsspezifischen Merkmale) im Vergleich sehr gut ab. Anhand dieser konnten bei 20 Autor:innen immer noch über 35 % der Tweets richtig zugeordnet werden. Dies lässt darauf schließen, dass Personen bei kurzen Texten eine Präferenz für bestimmte Worte aufweisen. Somit kann empfohlen werden, diesen Feature-Typen bei der Analyse von Social-Media-Texten ergänzend einzusetzen.

Anzahl Autor:innen	Interpunktion	Durchschnittliche Wortlänge	Groß-/Kleinschreibung	Zeichen-Tetragramme
5	0,3033	0,2300	0,3533	0,6700
10	0,2217	0,1700	0,1467	0,6100
20	0,1083	0,0825	0,0825	0,4933

Tab. 3: Übersicht der Genauigkeit (accuracy) der Autorenschaftsattribution mit n Autor:innen und aller lexikalischen Feature-Typen

Auffällig gute Ergebnisse wurden mithilfe der lexikalischen Merkmale erreicht. Hier ist allerdings zu bemerken, dass vor allem die Zeichen-Tetragramme von Bedeutung waren.

In Tab. 3 ist zu sehen, dass die anderen Feature-Typen dieser Kategorie schlechte Ergebnisse erzielten. Unter Verwendung von Zeichen-Tetragramme als alleinstehender Feature-Typ kann bereits eine Vielzahl an Nachrichten richtig zugeordnet werden, weshalb deren Berücksichtigung bei der Analyse von Social-Media-Texten besonders hilfreich ist. Dies stellen auch [Ro16] fest. Bei einem Vergleich mit den in Tab. 4 dargestellten Ergebnissen, welche unter Verwendung des gesamten Feature-Sets erzielt wurden, schneiden Zeichen-Tetragramme ähnlich gut ab.

Abschließend ist festzustellen, dass anhand des komplette Feature-Sets, trotz besonders kurzer Texte, immer noch viele Instanzen richtig zugeordnet werden konnten. Tab. 4 zeigt, dass bei 20 Kandidat:innen fast 50 % und bei 100 Autor:innen noch über 30 % aller Tweets korrekt zugeordneten wurden.

Anzahl Autor:innen	Genauigkeit (accuracy)
10	0,6367
20	0,4967
50	0,3690
100	0,3110

Tab. 4: Übersicht der Ergebnisse der Autorenschaftsattribution mit n Autor:innen und dem gesamten Feature-Set.

6 Zusammenfassung und Ausblick

In diesem Beitrag wurde eine Menge von 14 Feature-Typen (Tab. 1) aufgezeigt, die mit Support-Vector-Machines verwendet werden können, um ein Modell zur Autorenschaftsattribution zu trainieren. Zum Lernen der Modelle wurde jeweils ein Trainingsdatensatz mit insgesamt 300 Twitter-Kurznachrichten von 5-100 unterschiedlichen Autor:innen verwendet. In Abhängigkeit der Anzahl und des Typs der verwendeten Features konnten mit dem Modell eine Prädiktionsgenauigkeiten von bis zu 63% erreicht werden. Somit ist die Zuschreibung eines Tweets zu einer Autorin oder einem Autoren mit der dargestellten Genauigkeit möglich.

Dieses Modell kann damit im Rahmen der Verbrechensbekämpfung und zur Strafverfolgung wertvolle Ansätze für die Ermittlungsarbeit bieten und auch im Rahmen eines Gerichtsverfahrens zur Überführung von Täterinnen und Tätern beitragen. Der präventive Einsatz dieses Modells wäre ebenfalls denkbar. Hier könnte beispielsweise im Rahmen der Schulsozialarbeit bereits bei Vorliegen von Chat-Nachrichten, die als Vorstufe von Mobbings einzuordnen sind, eine gezielte Ansprache der identifizierten Absender:innen erfolgen und so eine Eskalation hin zum Mobbing vermieden werden.

Die vorgestellten Features zeigen, dass die Forschungsfrage beantwortet werden konnte. Eine Autorenschaftsattribution ist unter Berücksichtigung sehr kurzen Länge der Texte mit guter Genauigkeit möglich.

Es wurde dargestellt, dass die Klassifikationsgenauigkeit stark von der Auswahl geeigneter Feature abhängt. Es haben sich Feature die 14 vorgestellten Feature-Typen als sehr gut geeignet erwiesen. Zukünftig sollten weitere Feature konzipiert und getestet werden. Hier sollte gerade im Kontext von Social-Media-Texten und Kurznachrichten das Augenmerk auf die Verwendung von Emoticons gelegt werden.

Kritisch wurde die Annahme bezüglich des Trainingsdatensatzes hinterfragt. Beim gewählten Datensatz der Celebrity-Tweets konnte nicht sicher beantwortet werden, ob die Tweets von einer Person oder einem Social-Media-Team erstellt wurden. So ist fraglich, ob die guten Vorhersageergebnisse erzielt werden konnten, weil sich die Tweets eines Accounts sehr ähnlich sind oder ob die Ergebnisse gut sind, obwohl sich die Tweets stark unterscheiden. Hier müssten zukünftig ebenfalls weitere Untersuchungen angestellt werden. Die Beschaffung eines geeigneten Datensatzes zur Verifikation dieser Hypothese könnte jedoch aufwendig sein, da er vermutlich für diesen Zweck erstellt werden müsste.

Zusammenfassend ist festzustellen, dass mit dem vorgestellten Modell der Autorenschaftsattribution ein Beitrag zur Informationssicherheit und auch zur Verfolgung von Computerkriminalität geleistet werden kann.

Literaturverzeichnis

[AC05] Abbasi, Ahmed; Chen, Hsiu-chin; Applying Authorship Analysis to Extremist-Group Web Forum Messages. IEEE Intelligent Systems 20(5), 67-75, in: Intelligent Systems, IEEE, 20, 2005, S. 67–75.

[AC08] Abbasi, Ahmed; Chen, Hsiu-chin; Writeprints: A Stylometric Approach to Identity-level Identification and Similarity Detection in Cyberspace, in: ACM Transactions on Information Systems, 26, 2008, S. 1–29.

[AMM17] Ahmed, Al-Falahi; Mohamed, Ramdani; Mostafa, Bellafkih; Machine Learning for Authorship Attribution in Arabic Poetry, in: 20103751, 6, 2017, S. 42–46.

[Be18] Beare; Kenneth; Content and Function Words, 02.10.2018, https://www.thoughtco.com/content-and-function-words-1211726. Abgerufen am 23.10.2022.

[BMA13] Bhargava, Mudit; Mehndiratta, Pulkit; Asawa, Krishna; Stylometric Analysis for Authorship Attribution on Twitter, in: Vasudha Bhatnagar, Srinath Srinivasa (Hrsg.), Big Data Analytics: Second International Conference, BDA 2013, Mysore, India, December 16-18, 2013, Proceedings, Springer, Cham, 2013, S. 37–47.

[BNJ03] Blei, David M.; Ng, Andrew Y.; Jordan, Michael I.; Latent Dirichlet allocation, in: 0003-6951, 3, 2003, S. 993–1022.

[Br17] Brownlee, Jason; A Gentle Introduction to the Bag-of-Words Model, 07.08.2017, https://machinelearningmastery.com/gentle-introduction-bag-words-model/. Abgerufen am 17.10.2022.

[CS03] Clement, Ross; Sharp, David; Ngram and Bayesian Classification of Documents for Topic and Authorship, in: 0268-1145, 18, 2003, S. 423–447.

[Di03] Diederich, Joachim; Kindermann, Jörg; Leopold, Edda; Paass, Gerhard; Authorship Attribution with Support Vector Machines, in: 1573-7497, 19, 2003, S. 109–123.

[HS14] Halvani, Oren; Steinebach, Martin; Autorschaftsanalyse — die Illusion der Anonymität, in: Wirtschaftsinformatik & Management, 6, 2014, S. 33–43.

[Ka19] Kalgutkar, Vaibhavi; Kaur, Ratinder; Gonzalez, Hugo; Stakhanova, Natalia; Matyukhina, Alina; Code Authorship Attribution: Methods and Challenges, in: 0360-0300, 52, 2019, 3:1-3:36.

[LWD] Layton, Robert; Watters, Paul; Dazeley, Richard; Authorship Attribution for Twitter in 140 Characters or Less, in: 2010 Second Cybercrime and Trustworthy Computing Workshop, 2010, S. 1–8.

[Ro16] Rocha, Anderson; Scheirer, Walter; Forstall, Christopher; Cavalcante, Thiago; Theophilo, Antonio; Shen, Bingyu; Carvalho, Ariadne; Stamatatos, Efstathios; Authorship Attribution for Social Media Forensics, in: IEEE Transactions on Information Forensics and Security, 12, 2016, S. 5.

[Ro21] Romanov, Aleksandr; Kurtukova, Anna; Shelupanov, Alexander; Fedotova, Anastasia; Goncharov, Valery; Authorship Identification of a Russian-Language Text Using Support Vector Machine and Deep Neural Networks, in: Future Internet, 13, 2021.

[Sa] Sapkota, Upendra; Bethard, Steven; Montes, Manuel; Solorio, Thamar; Not All Character N-grams Are Created Equal: A Study in Authorship Attribution, in: , Proceedings of the 2015 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Denver, Colorado, Association for Computational Linguistics, 2015, S. 93–102.

[Sa20] Savoy, Jacques; Machine Learning Methods for Stylometry: Authorship Attribution and Author Profiling, Cham. Springer International Publishing AG, 2020.

[Sa22] Sakib, Ahmed Shahriar; Top 1000 Twitter Celebrity Tweets And Embeddings: Tweets and Embeddings of most followed celebrity twitter accounts, Juli 2022, https://www.kaggle.com/datasets/ahmedshahriarsakib/top-1000-twitter-celebrity-tweets-embeddings. Abgerufen am 12.10.2022.

[Sc13] Schwartz, R.; Tsur, O.; Rappoport, A.; Koppel, Moshe; Authorship attribution of micro-messages, in: EMNLP 2013 - 2013 Conference on Empirical Methods in Natural Language Processing, Proceedings of the Conference, 2013, S. 1880–1891.

[Sh17] Shrestha, Prasha; Sierra, Sebastian; González, Fabio; Montes, Manuel; Rosso, Paolo; Solorio, Thamar; Convolutional Neural Networks for Authorship Attribution of Short Texts, 2017.

[St09] Stamatatos, Efstathios; A Survey of Modern Authorship Attribution Methods, in:

JASIST, 60, 2009, S. 538–556.

[We21] Weerasinghe, Janith; Singh, Rhia; Greenstadt, Rachel; Feature vector difference based authorship verification for open-world settings, in: CEUR Workshop Proceedings, 2936, 2021, S. 2201–2207.

[Zh06] Zheng, Rong; Li, Jiexun; Chen, Hsiu-chin; Huang, Zan; A framework for authorship identification of Online messages: Writing-style features and classification techniques, in: JASIST, 57, 2006, S. 378–393.

Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 109

Entwicklung einer Prozessmodellierungssprache zur Unterstützung bei datenschutzrechtlicher Dokumentation

Ein studentisches Projekt

Daniel Bierschwale[1], Paul-Ferdinand Steuck[1] und Ralf Knackstedt[1]

Abstract: Aus der Datenschutz-Grundverordnung ergeben sich Anforderungen wie Dokumentationspflichten für Prozesse, welche personenbezogene Daten verarbeiten. Für Fachkräfte resultiert daraus in der Praxis oft ein umfangreicher, ressourcenintensiver Dokumentationsprozess. Als Lösungsstrategie entwickelt diese Arbeit eine neue Sprache zur Prozessmodellierung, die auf der Grundlage von Fachexpertise im Rahmen einer Real-Time Delphi-Studie und einem systematischen Literaturreview entwickelt wurde. Diese Sprache zielt darauf ab, den Prozess der Informationserhebung für die Dokumentationspflicht zu vereinfachen und zu optimieren. Die Arbeit schließt mit einer Evaluation der entwickelten Sprache und einem Ausblick auf weiterführende Forschung.

Keywords: Datenschutz, DS-GVO, Prozessmodellierung, Design Science Research

1 Einleitung

[KNW20] beschreiben die Digitalisierung in der Verwaltung als kontinuierlichen Entwicklungsprozess, durch welchen Prozesse digital abgebildet werden. Besonders durch die digitale Transformation der Verwaltung werden immer mehr personenbezogene Daten verarbeitet. Der Datenschutz tangiert dabei nicht nur technologische Lösungen und Innovationen, sondern ebenfalls die Vorstellungen und Arbeitsabläufe von Verwaltungsmitarbeitenden und Bürgern [ibid.].

Die Datenschutz-Grundverordnung (DS-GVO) stellt Fachkräfte auch aktuell noch vor komplexe und umfangreiche Herausforderungen, wie etwa die unsichere Rechtslage, die den Einsatz neuer Technologien wie KI hemmt [We22]. Die umfangreiche Dokumentationspflicht im Kontext des Datenschutzes stellt insbesondere für Fachkräfte ohne vertiefende Kenntnisse in diesem Bereich eine erhebliche Herausforderung dar.

[1] Universität Hildesheim, Informationssysteme und Unternehmensmodellierung, Universitätsplatz 1, 31141 Hildesheim, {bierschwaled, steuckp, knacks} @uni-hildesheim.de

doi:10.18420/rvi2023-009

Unternehmen wenden im Durchschnitt etwa eine Arbeitsstunde pro Verarbeitung jährlich für die Pflege und Aktualisierung der erforderlichen Informationen auf. In kleineren Unternehmen manifestiert sich der Arbeitsaufwand in einer jährlichen Zeitspanne von etwa 30 bis 40 Stunden. Dieser Aufwand divergiert jedoch abhängig von der Unternehmensgröße und -struktur. Denn im Gegensatz dazu verzeichnen mittlere bis große Unternehmen einen deutlich höheren Zeitaufwand, der zwischen 92 und 297 Stunden pro Jahr liegen kann [Ha23]. Dieses hohe Maß an benötigter Zeit und Ressourcen kann sich hinderlich auf Digitalisierungsprojekte und Innovationspotentiale auswirken [We22].

Im Kontext der Digitalisierung und der E-Government-Gesetzgebung (EGovG) gewinnt das Prozessmanagement und die Prozessmodellierung in der Verwaltung an Bedeutung, da Prozesse unter anderem zu dokumentieren sind [NP18]. Eine hiermit korrelierende Anforderung findet sich auch in der DS-GVO, denn gemäß Art. 30 Abs. 1 DS-GVO ist das Verzeichnis von Verarbeitungstätigkeiten, in welchem sämtliche Verarbeitungsprozesse personenbezogener Daten zu dokumentieren sind, ein wesentlicher Bestandteil. Darüber hinaus reguliert Art. 5 Abs. 2 DS-GVO, dass die Einhaltung der Grundsätze aus Art. 5 Abs. 1 DS-GVO nachweisbar sein muss. Im Sinne der Handhabung der umfassenden Komplexität der DS-GVO, wie in [KEF18] hervorgehoben, wird oftmals versucht die Informationsgewinnung durch den Dialog und/oder den Einsatz von Fragebögen zu erreichen. Eine Möglichkeit zur Nutzung von Synergieeffekten, um die zuvor geschilderten Aufwände für Datenschutzbeauftrage und Fachkräfte bei der Pflege des Verzeichnisses von Verarbeitungstätigkeiten und der Umsetzung der Rechenschaftspflicht zu reduzieren, stellt die Erweiterung bzw. Nutzung von Prozessmodellierungen in der öffentlichen Verwaltung um datenschutzrechtliche Informationen dar.

Dieser Beitrag ist das Produkt eines Design Science Research (DSR) Projekts, nach dem Vorgehensmodell von [Pe07], welches im Rahmen einer universitären Lehrveranstaltung von einem studentischen Team durchgeführt wurde. Im Rahmen dieser Lehrveranstaltung haben die Studierenden die Aufgabe, Prozessmodellierungssprachen zu entwickeln oder zu erweitern, um ein reales Problem zu lösen. Hierbei ist von Relevanz, dass in der wissenschaftlichen Literatur keine andere etablierte Prozessmodellierungssprache identifiziert wird, welche das vorliegende Problem in optimaler Weise lösen kann. Der Kurs beginnt mit einer Phase der Themenfindung, in der die Studierenden angehalten sind, ein relevantes und anspruchsvolles Problemfeld zu identifizieren, das sowohl praktische als auch wissenschaftliche Relevanz aufweist. Nach intensiver Diskussion und Überlegung über das Thema, wurde folgende Forschungsfrage formuliert:

Wie sollte eine Prozessmodellierungssprache gestaltet sein, um Fachabteilungen in der Verwaltung bei der Erfassung der Informationen für eine Verarbeitung im Sinne des Datenschutzes zu unterstützen?

Zur Beantwortung der Forschungsfrage und um das Problem aus verschiedenen Perspektiven zu beleuchten, werden die Phasen nach Peffers et al. durchlaufen. Zunächst wird in Kapitel 2 zum Nachweis des Problems auf die methodische Vorgehensweise und die Ergebnisse einer durchgeführten Delphi-Studie mit Personen mit Datenschutzexpertise eingegangen. Anschließend werden in Kapitel 3 mittels eines systematischen Literaturreviews und anhand der DS-GVO selbst Kriterien bzw. Anforderungen für eine Prozessmodellierungssprache, die zur Dokumentation der Informationen gemäß Art. 5 Abs. 2 und insbesondere Art. 30 Abs. 1 DS-GVO notwendig sind, formuliert. Auf Grundlage dieser Erkenntnisse wird in Kapitel 4 im Rahmen unseres DSR-Projekts eine eigene Prozessmodellierungssprache entwickelt. In Kapitel 5 erfolgt die Evaluation der Modellierungssprache unter Berücksichtigung der Vorgehensweise von [GW04] und der Durchführung der Think-Aloud-Methode. Unsere Arbeit endet mit einer Rekapitulation sowie Reflektion der Ergebnisse und einem Ausblick auf mögliche nächste Schritte, die sich sowohl aus unserer Forschungsarbeit als auch aus den in der Lehrveranstaltung erworbenen Kenntnissen ergeben.

2 Datenschutz: Eine kontinuierliche Herausforderung

Dieses Kapitel widmet sich der ersten Phase nach [Pe07], der Problemidentifikation und -motivation, für welche entsprechende Informationen über den Problemstand sowie die Relevanz einer Lösung unverzichtbar sind [ibid.]. Für den Erhalt näherer Informationen darüber, inwiefern Fragebögen und Meetings hinsichtlich datenschutzrechtlicher Dokumentationspflichten zu Mehraufwand für Fachkräfte und Personen mit Datenschutzexpertise führen, wird eine Real-Time Delphi-Studie mit dem Tool eDelphi durchgeführt[2]. Bei dessen Ablauf wurde sich an dem Vorgehensmodell von [SR09] und den Eigenheiten einer Real-Time Delphi-Studie nach [GE19] orientiert. Das Ziel der Real-Time Delphi Studie lag in der Ermittlung und Qualifikation von Ansichten einer Gruppe von Personen mit Expertise zu folgender, übergeordneter Fragestellung:

Kommt es bei der Zusammenarbeit zwischen der Datenschutzabteilung und den Fachabteilungen bei der Erfassung der Informationen für die Verarbeitung personenbezogener Daten für das Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DS-GVO zu einer Überlastung der Datenschutzabteilung und zugleich auch zu Schwierigkeiten bei der Bereitstellung der notwendigen Informationen durch die Fachabteilungen?

Diese Fragestellung wurde im Zuge der Entwicklung des Fragebogens entsprechend der Empfehlung von [SR09] nach dem Konzept der Operationalisierung der Fragestellung nach [Hä09] in zwei Facetten untergliedert, die einzeln beleuchtet werden.

[2] Siehe eDelphi.org: https://www.edelphi.org/

Die Überlastung der Datenschutzabteilung. Diese Facette umfasst Fragen, die sich direkt mit der Belastung für eine Datenschutzabteilung durch den Mehraufwand im Rahmen der Unterstützung der Fachabteilungen bei der Erhebung der Informationen für eine Verarbeitung auseinandersetzen.

Die Bereitstellung der notwendigen Informationen durch die Fachabteilungen. Diese Facette umfasst Fragen, die sich primär auf die Qualität der bereitgestellten Informationen durch die Fachabteilung beziehen und adressieren unter anderem die Kompetenzen der Fachkräfte hinsichtlich des Themas Datenschutz.

Insgesamt haben sich an der Real-Time Delphi-Studie fünf Personen mit Expertise (n=5) beteiligt, die Ihre Qualifikation zum einen durch ihre langjährige Praxiserfahrung von mehr als 8 Jahren in einer Datenschutzabteilung eines internationalen IT-Service Providers und zum anderen durch entsprechende Zertifikate der Gesellschaft für Datenschutz und Datensicherheit zum Thema Datenschutz nachwiesen. Die Ergebnisse der Real-Time Delphi-Studie zeigen auf, dass der bestehende Prozess zur Unterstützung der Fachabteilungen bei der Erfassung der Informationen als ineffizient wahrgenommen wird. Die Personen mit Expertise sind sich nahezu einig und geben an, dass dieser Prozess erheblichen Mehraufwand für die Datenschutzabteilung verursacht. Dieser Mehraufwand führt zu Verzögerungen und Beeinträchtigungen der Arbeit. Zudem zeigen die Ergebnisse, dass Mitarbeitende der Fachabteilungen Schwierigkeiten haben, relevante Kerninformationen wie den Zweck oder die Rechtsgrundlage einer Verarbeitung zu erfassen. Unklare Verantwortlichkeiten und ein mangelndes Verständnis in den Fachabteilungen führen ebenfalls zu Problemen wie Verzögerungen bei der Klärung von Rückfragen. Die Umfrageergebnisse weisen somit auf die Bedeutung einer Lösung hin, um den Mehraufwand für die Datenschutzabteilung zu reduzieren und die Fachabteilungen effektiv bei der eigenständigen Erfassung der Kerninformationen zu unterstützen.

3 Anforderungen an eine Modellierungssprache

Die DS-GVO definiert in Art. 5 verschiedene Grundsätze, dessen Einhaltung für jeden Verantwortlichen obligatorisch sind. Einer dieser Grundsätze, die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO, fordert die Einhaltung der anderen Grundsätze und die Fähigkeit hierfür einen Nachweis erbringen zu können. Dieser Nachweis korreliert unter anderem mit dem Art. 30 DS-GVO, nach welchem von einem Verantwortlichen und gegebenenfalls seinem Vertreter, ein Verzeichnis sämtlicher Verarbeitungen zu führen ist, die in dessen Zuständigkeit fallen. Hierbei handelt es sich jedoch um eine weitreichende Dokumentationspflicht [Br18], die sich auch auf Verarbeitungen als Auftragsverarbeiter gemäß Art. 30 Abs. 2 DS-GVO erstreckt. In Anlehnung an die zweite Phase des Vorgehensmodells nach [Pe07], haben wir den Forschungsstand hinsichtlich der Prozessmodellierung im Bereich der DS-GVO bzw. des Datenschutzes untersucht. Dies erfolgte durch ein systematisches Literaturreview gemäß der Vorgehensweise von [Br09].

Ziel des Literaturreviews war die Synthese der bestehenden Lösungen, um die Grenzen von aktuellen Modellierungssprachen aufzuzeigen und Anforderungen an eine zu entwickelnde Modellierungssprache zu definieren. Die Suche des Literaturreviews wurde anhand der PRISMA-Methode [Mo09] in Google Scholar durchgeführt[3], was zu einer Gesamtzahl von 150 Ergebnissen führte. Hierbei wurden Publikationen in dem Zeitraum von 2018-2023 berücksichtigt. Nach Prüfung der Abstracts und Titel wurden 11 Ergebnisse als relevant identifiziert, wobei als Kriterium für die Relevanz die Einführung einer neuen Modellierungssprache oder die Weiterentwicklung einer existierenden Modellierungssprache im Bereich des Datenschutzes diente. Basierend auf den aus der identifizierten Literatur abgeleiteten Anforderungen und den obligatorischen Inhalten für ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO sowie der Nachweispflicht gem. Art. 5 Abs. 2 DS-GVO wurde ein Kriterienkatalog entworfen. Dieser Katalog dient zum einen als Grundlage für einen Abgleich mit bestehenden Modellierungssprachen der Domäne und zum anderen für eine anforderungsorientierte, systematische Entwicklung der Modellierungssprache. Für den Abgleich mit bestehenden Modellierungssprachen wurden weiterhin fünf Ansätze aus der identifizierten Literatur ausgewählt. Die Kriterien werden in die Kategorien “Daten” und “Prozess” untergliedert. “Daten” umfasst hierbei alle Informationen, die nach der DS-GVO von der Fachabteilung zu dokumentieren sind. “Prozess” beinhaltet unterstützende Komponenten für die Bewertung von Sachverhalten und Entscheidungsfindungen sowie deren Dokumentation.

Kategorie	Kriterium	Kriterium-Beschreibung	[CM19]	[Ag19]	[BR19]	[WSG21]	[MA20]
Daten	Kategorisierung	Kategorien personenbezogener Daten	✓	X	X	X	✓
	Personenbezogen	Hervorhebung von Personenbezogene Daten	✓	X	X	✓	✓
	Rechtsgrundlage	Rechtsgrundlage der Verarbeitung	✓	X	X	X	✓
	Schutzbedarf	Schutzbedarf der Daten	X	X	X	✓	✓
	Speicherdauer	Aufbewahrungszeit der Daten	✓	X	X	X	✓
	Verantwortlichkeit	Verantwortliche Person	X	X	X	X	✓
	Zweckbindung	Zweck zu dem die Daten verarbeitet werden	✓	✓	X	X	✓
Prozess	Einbettung in Geschäftsprozess	Lässt sich im Geschäftsprozess modellieren	✓	✓	X	✓	✓
	Einbindung von Fachexperten	Es ist ersichtlich an welcher Stelle Fachexperten konsultiert werden	X	X	X	X	X
	Dokumentation der Prüfung innerhalb der Modellierungssprache	Durch die Modellierung von Entscheidungen und Einschätzungen sind keine extra Dokumentationen nötig	✓	✓	✓	X	~1
	Leitfragen für Prozess	Unterstützung des Anwenders durch Leitfragen	X	X	✓	X	X
	Meta-Informationen (Dokumentationsziele)	Zusammenfassung der Ergebnisse der Dokumentation	~2	X	X	~3	X
	Modellierung von Prüfschritten	Kerninformationen für einer Verarbeitung werden explizit geprüft	X	~4	✓	X	✓
Legende	✓: Kann durch Modellierungssprache dargestellt werden X: Kann durch Modellierungssprache nicht dargestellt werden ~Zahl: Keine binäre Einteilung möglich, wird im Text näher erläutert						

Abb. 1: Kriterien und Abgleich mit bestehenden Modellierungssprachen

Wie aus Abb. 1 hervorgeht, stellen [CM19] und [WSG21] BPMN-Erweiterungen dar, die die Notation um ausgewählte Aspekte der DS-GVO erweitern. Allerdings bieten sie wenig

[3] Suchstring: “GDPR” AND ((“process” OR “BPMN” OR “ERM” OR “eERM” OR “EPC” OR “eEPC” OR “S-BPM” OR “UML” OR “Flowchart” OR “Model”) AND (“Consent” OR “personal data” OR “lawfulness” OR “legal basis” OR “purpose” OR “storage limitation”))

Unterstützung im eigentlichen Prozess der Dokumentation der datenschutzrechtlichen Kerninformationen ($\sim_2$ und $\sim_3$). [Ag19] modellieren die DS-GVO in BPMN, ohne zusätzliche Notationen einzuführen, wodurch sie leicht in bestehende Geschäftsprozesse integriert werden können. Es fehlt jedoch an ausreichender Dokumentation, und es werden nur wenige Kerninformationen berücksichtigt ($\sim_4$). [BR19] konzentrieren sich ausschließlich darauf, rechtliche Normen in einzelne Workflows zu übertragen. Diese können Fachabteilungen zwar bei der Dokumentation und Bewertung unterstützen, lassen sich jedoch nicht in die konkrete Prozessmodellierungen integrieren. [Ma20] kommen den definierten Kriterien am nächsten. Durch eine umfassende Modellierung der DS-GVO lassen sich alle Kerninformationen überprüfen. Allerdings gestaltet sich die Überführung des bestehenden Geschäftsprozesses in das eigens entworfene IST-Modell als problematisch. Die Unterstützung für die Prüfschritte ist begrenzt und besteht hauptsächlich aus Anleitungen in natürlicher Sprache. Daher wird ein hohes Maß an Modellierungswissen vorausgesetzt, und zusätzliche Dokumentation ist erforderlich ($\sim_1$). Aus dem kriterienbasierten Vergleich wird ersichtlich, dass keine der betrachteten Modellierungssprachen beide Kategorien vollumfänglich abdeckt. Zur Lösung des initial beschriebenen Problems wird demnach eine Modellierungssprache entwickelt. Die zu entwickelnde Modellierungssprache soll die Fachabteilungen dabei unterstützen, die datenschutzrechtlichen Kerninformationen nach einem standardisierten Vorgehen bereits im Zuge der Prozessmodellierung der Geschäftsprozesse zu erheben und zu dokumentieren, um somit die Datenschutzabteilung zu entlasten.

4 Data Protection Process Modelling Language

Im Rahmen der Design- und Entwicklungsphase gemäß [Pe07] wurde die Data Protection Process Modelling Language (DPPML) entwickelt. Diese Sprache ermöglicht es Fachkräfte, die über begrenzte Datenschutzkenntnisse verfügen, ausgewählte Dokumentationsanforderungen eigenständig zu erfüllen, ohne zunächst den Datenschutzbeauftragten einzubeziehen. Die Grundlage der Modellierungssprache bildet BPMN 2.0. Diese Grundlage wurde durch die Einführung weiterer Elemente und Darstellungsmöglichkeiten erweitert, welche aus dem systematischen Literaturreview und der Real-Time Delphi-Studie abgeleitet wurden. DDPML besteht aus drei Bausteinen und kann in andere, bestehende Prozessmodellierungssprachen integriert werden. Ferner besteht die Möglichkeit die Bausteine modular zu verwenden, insofern gewisse Aspekte eigenständig oder anderweitig modelliert werden. Die Abbildung 2 veranschaulicht den ersten Baustein mit integrativem Charakter. Dieser besteht aus drei Symbolen, die in jeder bestehenden Modellierungssprache (hier: BPMN) ergänzt werden können, um den datenschutzrechtlichen Prüfungsbedarf einer Aktivität sowie dessen Status zu kennzeichnen.

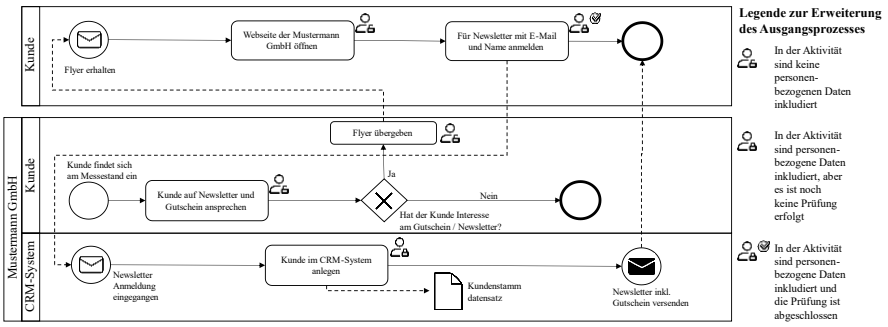

Abb. 2: Der integrative Baustein von DPPML in einem BPMN-Prozess

Der zweite Baustein der DPPML ist ein Informationskasten, in welchem datenschutzrechtliche Aspekte dokumentiert und historisiert werden können. Ferner wird hier der iterative Charakter von DPPML aufgegriffen. So besteht die Option, die relevanten Informationen in Form von eigenständigen Prüfungen für eine Aktivität zu dokumentieren. Der Informationskasten unterstützt dabei die Anforderung der Transparenz gemäß Art. 5 Abs. 1 lit. a DS-GVO und soll die Datenschutzabteilung dabei unterstützen, die Kerninformationen für die Dokumentationspflichten nach Art. 5 Abs. 2 und insbesondere Art. 30 Abs. 1 DS-GVO zu erfassen. Die Abbildung 3 verdeutlicht die aggregierten Informationen, die durch die Fachkräfte ohne Datenschutzexpertise für zwei exemplarische Aktivitäten, aus vorangegangenem Prozessbeispiel, dokumentiert wurden.

Datenschutzrechtliche Kerninformationen	
1. Iteration	**2. Iteration**
Kategorien personenbezogener Daten: Stammdaten, Kontaktdaten, Telekommunikationsdaten	**Kategorien personenbezogener Daten:** Stammdaten, Kontaktdaten, Adressdaten
Rechtmäßigkeit: Art. 6 Abs. 1 S. 1 lit. a DS-GVO	**Rechtmäßigkeit:** Art. 6 Abs. 1 S. 1 lit. a DS-GVO
Zweck: Newsletter-Anmeldung und -versand	**Zweck:** Newsletter-Anmeldung und -versand
Verantwortliche Person: Max Mustermann	**Verantwortliche Person:** Maxine Mustermann
Zeitstempel der Prüfung: 01.02.2023 13:10:34	**Zeitstempel der Prüfung:** 05.02.2023 14:15:36
Prozessschritt: Für Newsletter mit E-Mail und Name anmelden	**Prozessschritt:** Kunde im CRM-System anlegen

Abb. 3: Exemplarische Darstellung des Informationskasten aus Grundlage des Beispielprozesses

Der letzte Baustein von DPPML ist eine eigens entwickelte Modellierungssprache, welche auf grundlegende Elemente von BPMN 2.0 zurückgreift. Dieser Baustein setzt sich aus drei Prüfschritten zur Erfassung der datenschutzrechtlichen Kerninformationen einer Verarbeitung personenbezogener Daten zusammen. In Abbildung 4 werden die Dokumentationsobjekte der Prüfschritte und deren rechtlicher Ursprung dargestellt.

Prüfschritte der DPPML			
Prüfschritte	1. Prüfschritt	2. Prüfschritt	3. Prüfschritt
Dokumentationsobjekt	Personenbezogene Daten	Zweck	Rechtsgrundlage
Rechtliche Grundlage	Art. 5 und 30 DS-GVO	Art. 5 und 30 DS-GVO	Art. 5, 6 und 9 DS-GVO

Abb. 4: Dokumentationsobjekte und rechtliche Ursprung der Prüfschritte

Jeder Prüfschritt der DPPML folgt einem einheitlichen Aufbau. Das Ergebnis eines Prüfschritts stellt die Dokumentation des entsprechenden Dokumentationsobjekts (Personenbezogene Daten, Zweck, Rechtsgrundlage) im Informationskasten dar. Jeder dieser Prüfschritte weist einen iterativen Charakter auf und verfolgt den Grundgedanken der Historisierung von Entscheidungswegen, damit Entscheidungen im Nachgang nachverfolgt und nachvollzogen werden können. Zudem besteht in jedem Prüfschritt die Möglichkeit Begründungen für Entscheidungen zu hinterlegen und an gewissen Stellen bei Bedarf den Datenschutzbeauftragten zu kontaktieren. Entsprechende Elemente der entwickelten Modellierungssprache können der Abbildung 5 entnommen werden.

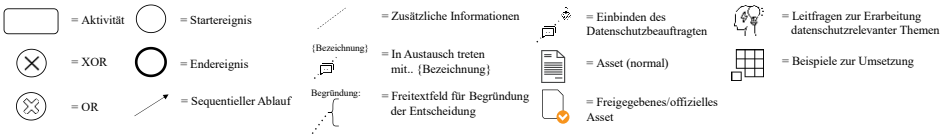

Abb. 5: Legende der DPPML-Prüfschritte

Basierend auf dem in Abbildung 2 vorgestellten Prozessbeispiel für den integrativen Baustein von DPPML in BPMN, wird in Abbildung 6 der dritte Baustein präsentiert. Hierbei wird ein Einblick in eine Teilansicht des ersten Prüfschritts gegeben, in welchem Maxine Mustermann die Aktivität "Kunde im CRM-System anlegen" durchläuft.

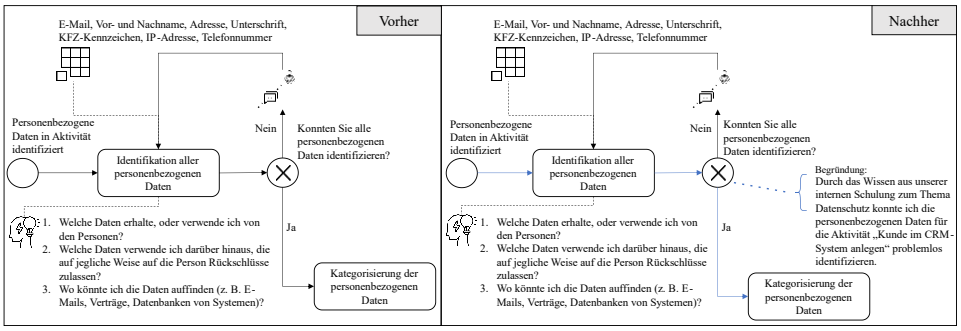

Abb. 6: Teilansicht des ersten Prüfschritts: Kategorisierung personenbezogener Daten

Wie aus Abbildung 6 hervorgeht, wird die modellierende Person, hier Maxine Mustermann, bei der Identifikation der personenbezogenen Daten unterstützt. Diese Unterstützung erfolgt durch Leitfragen und beispielhafte Angaben. Sollte Maxine

Mustermann weiterführende Unterstützung benötigen, besteht die Möglichkeit, den Datenschutzbeauftragten zu kontaktieren. Um eine spätere Nachverfolgung zu ermöglichen, werden die Entscheidungswege von Maxine Mustermann durch eine blaue Hervorhebung gekennzeichnet. Darüber hinaus besteht die Option, die getroffenen Entscheidungen durch entsprechende Begründungen zu unterstützen und zu dokumentieren. Die Ergebnisse dieses Ihrer Prüfung werden im Informationskasten dokumentiert, welcher bereits in Abbildung 3 vorgestellt wurde. Insgesamt wurde in diesem Kapitel eine Modellierungssprache vorgestellt, welche die Option offeriert, bestehende Prozessmodellierungen, um Symbole und Informationen zu ergänzen, die Aufschluss über den datenschutzrechtlichen Prüfungsbedarf einer Aktivität geben (Baustein 1 und 2). Gleichzeitig wurden exemplarisch drei Prüfschritte vorgeschlagen, die von Fachkräften ohne Datenschutzexpertise im Sinne der Unterstützung eingesetzt werden können, um die datenschutzrechtlichen Informationen zu erfassen (Baustein 3). Diese Prüfschritte sind dabei so konzipiert, dass sie von dem jeweiligen Datenschutzbeauftragen adaptiert werden können. Darüber hinaus dienen die Prüfschritte gleichzeitig als Dokumentation und können auch mehrere Iterationen von Entscheidungsprozessen abbilden, deren Ergebnisse im Informationskasten (Baustein 2) festgehalten werden.

5 Evaluation

Zur explorativen Evaluation der Verständlichkeit von DPPML wurde eine Untersuchung unter Anwendung der Think-Aloud-Methode durchgeführt. Die Teilnehmenden bestanden aus Fachkräften aus der Wirtschaft ohne spezialisierte Datenschutzexpertise (n=3), die zuvor nicht an der Delphi-Studie teilgenommen hatten. Diese Teilnehmerauswahl erfolgte in Übereinstimmung mit dem Ziel von DPPML, insb. Fachkräfte ohne tiefgehende Datenschutzkenntnisse in der beruflichen Praxis zu unterstützen. Hierbei wurde sich für die Evaluation an der Vorgehensweise von [GW04] orientiert. Hierdurch werden die Phasen der Demonstration und Evaluation nach [Pe07] umgesetzt. Im Rahmen der Durchführung der Think-Aloud-Methode wurde den Fachkräften die Bausteine von DPPML anhand eines einfachen Szenarios gezeigt. Auf eine inhaltliche Einführung der Probanden wurde verzichtet. Während der Durchführung der Think-Aloud-Methode wurden die Probanden gebeten, die einzelnen Bausteine und Prüfschritte zu betrachten und ihre Gedanken zu diesen Bestandteilen zu artikulieren. Um eine Auswertung der Transkripte in einer einfachen, visuellen Form zu ermöglichen, wird nachstehend die Bewertung der Aussagen der Probanden hinsichtlich der für die Aufgaben definierten Ziele in einer tabellarischen Form in Abbildung 7 dargestellt. Ein „X“ bedeutet dabei, dass die Person das Ziel der Aufgabenstellung nach Ansicht der Autorenschaft verstanden hat. Eine Tilde (~) wird gesetzt, sofern aus den Transkripten hervorgeht, dass die teilnehmende Person zumindest teilweise das Ziel der Aufgabenstellung verstanden hat. Wird kein Symbol gesetzt, geht aus der Antwort der teilnehmenden Person nicht die richtige Intention hervor.

Art der Frage	Ziel der Fragestellung	1. Proband	2. Proband	3. Proband
Allgemeine Fragen	Grundlegende Einordnung des Themenbereichs	~	X	X
	Verständnis der Aufteilung in initiale Modellierung und Prüfschritte		X	X
	Verbindung zwischen Prüfschritten und Prozessmodellierung (iterativ)	X	X	~
1. Prüfschritt – Kategorisierung personenbezogener Daten	Prüfen der Verständlichkeit (Zweck und Ablauf) des ersten Prüfschritts	X	X	~
2. Prüfschritt – Bestimmung des Zwecks	Prüfen der Verständlichkeit (Zweck und Ablauf) des zweiten Prüfschritts	X	X	X
3. Prüfschritt – Bestimmung der Rechtsgrundlage	Prüfen der Verständlichkeit (Zweck und Ablauf) des dritten Prüfschritts	~	X	~

Abb. 7: Ergebnisse der Think-Aloud-Methode hinsichtlich der definierten Ziele

Allgemein geht aus der Sichtung der Transkripte hervor, dass das Modell größtenteils verständlich für die Teilnehmenden war und somit die Modellinterpretation nach [GW04] als effektiv zu bewerten ist. Es wird jedoch auch deutlich, dass bei der initialen Einordnung der Modellierungssprache und den Zusammenhängen zwischen den verschiedenen Bestandteilen Verständnisprobleme auftreten. Diese manifestieren sich vor allem in der Unklarheit der Teilnehmenden bezüglich der Verbindung und Unterschiede zwischen den über- und untergeordneten Prozessebenen, wie aus Äußerungen wie „Ist das da unten der gleiche Prozess?“ oder „oben sieht es eher nach einem Beispielprozess aus und unten scheint es ein bisschen mehr ins Detail zu gehen“ hervorgeht (1. Proband). Wie bereits zuvor beschrieben, wurde im Rahmen der Durchführung der Think-Aloud-Methode auf eine inhaltliche Einführung der Teilnehmenden verzichtet. Dies könnte ein weiterer Faktor sein, welcher sich auf das initiale Verständnis auswirkt. Aus den Antworten der Teilnehmenden zu den Prüfschritten wird ersichtlich, dass die Teilnehmenden die Prüfschritte nicht vollständig durchlaufen, sondern vielmehr die Prüfschritte in Gänze betrachtet haben. Dabei wurden insbesondere die farblichen Hervorhebungen sowie die bisher unbekannten Symbole der Modellierung angesprochen. Die explorative Evaluation zeigt ein grundlegendes Verständnis der Prüfschritte und der weiteren Bausteine von DPPML. Zukünftige Evaluationen in der Verwaltung erfordern eine Einführung in die Modellierung und an den Kontext angepasste Prüfschritte durch Datenschutzbeauftragte, um das Verständnis bei Fachkräften ohne Datenschutzexpertise zu verbessern.

6 Fazit und Ausblick

Im Rahmen dieses Beitrages wurde sich mit der Frage beschäftigt, wie eine Modellierungssprache zu gestalten ist, um Fachkräfte ohne Datenschutzexpertise bei der Erfassung der Kerninformationen einer Verarbeitung im Sinne der DS-GVO zu unterstützen. Diese Frage resultierte aus einer durchgeführten Real-Time Delphi-Studie, welche aufzeigte, dass die beschriebene Aufgabe auch in der aktuellen Zeit noch eine Herausforderung in der Praxis darstellt. Im Sinne einer systematischen Erarbeitung einer Lösung für dieses Problem in Form einer Modellierungssprache, wurde zunächst auf

Grundlage eines Literaturreviews und den Anforderungen der DS-GVO ein Kriterienkatalog definiert. Diese Kriterien dienten als Werkzeug, um zu untersuchen, ob bereits bestehende Modellierungssprachen aus der Literatur eine Lösung darstellen können. Auf Grund der fehlenden Vollständigkeit dieser Lösungen in Hinblick auf den definierten Kriterienkatalog wurde auf dessen Grundlage eine eigene Modellierungssprache entwickelt und im Sinne der Verständlichkeit im Rahmen einer explorativen Evaluation der Modellinterpretation näher untersucht. Auch wenn die Anforderungen der DS-GVO im Hinblick auf das betrachtete Thema für den öffentlichen- und nicht-öffentlichen Sektor ähnlich sind, so bietet es sich zukünftig an, eine weitere Evaluation der Modellierungssprache in einer Verwaltung mit einem größeren Personenkreis durchzuführen. Jedoch ging aus dieser Evaluation hervor, dass DPPML als verständlich zu bewerten ist. Es wird dennoch deutlich, dass auf Grund der Komplexität des Datenschutzes ein Grundverständnis für die Thematik vorliegen muss, damit die Inhalte verstanden werden können. Ferner geht aus der Evaluation hervor, dass in Zukunft semantische Anpassungen vorgenommen werden können, um die Verständlichkeit der Modellierungssprache zu verbessern, indem Textbestandteile reduziert und die Zusammenhänge der einzelnen Bausteine stärker verdeutlicht werden. Weiteres Potential für eine Weiterentwicklung der DPPML ergibt sich aus dem bislang noch nicht erfüllten Kriterium der Dokumentation der Aufbewahrungsfristen personenbezogener Daten. Insgesamt wird deutlich, dass DPPML dazu beitragen kann, Laien im Bereich des Datenschutzes bei der Dokumentation von rechtlichen Anforderungen zu unterstützen. Zukünftig könnte DPPML somit im öffentlichen und nicht-öffentlichen Sektor dazu beitragen, die komplexen Dokumentationspflichten gemäß den Vorgaben der DS-GVO einfacherer zu realisieren und somit Kosten und Zeit einsparen. Die Befähigung von Datenschutz-Laien zur selbstständigen Prüfung der spezifischen Aktivitäten oder Prozesse stellt dabei eine wesentliche Herausforderung dar, bei welcher DPPML versucht, zu unterstützen. Wie aus den Limitationen dieser Ausarbeitung hervorgeht, ist die Modellierungssprache dabei in einem funktionalen Zustand, weist jedoch noch Potential für Verbesserungen durch weitere Entwicklungs- und Evaluationszyklen auf.

Literaturverzeichnis

[Ag19] Agostinelli, S. et.al.: Achieving GDPR Compliance of BPMN Process Models. In (Cappiello, C.; Ruiz, M. Hrsg.): Information Systems Engineering in Responsible Information Systems, Rom 2019. Springer, Cham, S. 10-22, 2019.

[Br09] Vom Brocke, J. et.al.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In (Newell, S.; Whitley, E. A.; Pouloudi, N.; Wareham, J.; Mathiassen, L. Hrsg.): 17th European Conference on Information Systems, Verona 2009. ECIS Proceedings 2009.

[Br18] Brüggemann, S.: Art. 30 Verzeichnis von Verarbeitungstätigkeiten. In (Eßer, M., Kramer, P., von Lewinski, K., Hrsg.): Auernhammer DSGVO BDSG Kommentar, 6. Aufl., Carl Heymanns Verlag, Köln, S. 458-470, 2018.

[BR19] Buchmann, E.; Robak, M.: Deriving Workflow Privacy Patterns from Legal Documents. In: Federated Conference on Computer Science and Information Systems (FedCSIS), Leipzig, 2019. IEEE, S. 555-563, 2019.

[CM19] Capodieci, A.; Mainetti, L.: Business process awareness to support GDPR compliance. Proceedings of the 9th International Conference on Information Systems and Technologies, S. 1-6, 2019.

[Ge19] Gerhold, L.: Real-Time Delphi. In (Niederberger, M.; Renn, O. Hrsg.): Delphi-Verfahren in den Sozial- und Gesundheitswissenschaften. Springer Verlag, Wiesbaden, S. 101-124, 2009.

[GW04] Gemino, A.; Wand, Y.: A framework for empirical evaluation of conceptual modeling techniques. Requirements Engineering 9/4, S. 248-260, 2004.

[Hä09] Häder, M.: Delphi-Befragungen. Ein Arbeitsbuch, 3. Aufl., Springer Verlag, Wiesbaden, 2009.

[Ha23] Harta, L. et.al.: Burdens arising from Art. 30 and 33 of the General Data Protection Regulation. Stiftung Familienunternehmen, München, 2023.

[KEF18] Koc, H.; Eckert, K.; Flaig, D.: Datenschutzgrundverordnung (DSGVO): Bewältigung der Herausforderungen mit Unternehmensarchitekturmanagement (EAM). HMD Praxis der Wirtschaftsinformatik 55/5, S. 942-963, 2018.

[KNW20] Klenk, T.; Nullmeier, F.; Wewer, G.: Handbuch Digitalisierung in Staat und Verwaltung, Springer VS, Wiesbaden, 2020.

[Ma20] Matulevičius, R. et.al.: A Method for Managing GDPR Compliance in Business Processes. In (Herbaut, N.; La Rosa, M. Hrsg.): Advanced Information Systems Engineering, Grenoble, 2020. Springer, Cham, S. 100-112, 2020.

[Mo09] Moher, D. et.al.: Preferred reporting items for systematic reviews and meta-analyses: the PRISMA Statement. Open Medicine 3/3, S. 123-130, 2009.

[NP18] Netzwerk Prozessmanagement, Einführung in das strategische Prozessmanagement der öffentlichen Verwaltung, https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/eGovernment/egov_leitfaden_prozessmanagement.pdf?__blob=publicationFile&v=2, Stand: 12.06.2023.

[Pe07] Peffers, K. et.al.: A Design Science Research Methodology for Information Systems Research. Journal of Management Informations Systems 24/3, S. 45-77, 2007.

[SR09] Schulz, M.; Renn, O.: Das Gruppendelphi. Konzept und Fragebogenkonstruktion, Springer Verlag, Wiesbaden, 2009.

[We22] Weiß, R.: Datenschutz als Herausforderung für die Digitalisierung, https://www.bitkom.org/Bitkom/Publikationen/Datenschutz-als-Herausforderung-fuer-die-Digitalisierung, Stand: 12.06.2023.

[WSG21] Windrich, M.; Speck, A.; Gruschka, N.: Representing Data Protection Aspects in Process Models by Coloring. In (Gruschka, N.; Antunes, L. F. C.; Rannenberg, K.; Drogkaris, P. Hrsg.): 9th Conf. On Privacy Technologies and Policy, Oslo 2021. Springer, Cham, S. 143-155, 2021.

Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
122 Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023

Einschätzungen aus dem griechischen Parlament zum Einsatz von künstlicher Intelligenz in Parlamenten

Jörn von Lucke [1] und Fotios Fitsilis [2]

Abstract: Parlamente analysieren derzeit, ob sich Technologien aus dem Bereich der künstlichen Intelligenz (KI) zur Erledigung bestimmter parlamentarischer Aufgaben eignen. Mit Blick auf Werkzeuge, Anwendungsbereiche, Nutzungsszenarien und Bedürfnisse werden KI-getriebene Veränderungen in Parlamenten erwartet. Der Einsatz von KI im parlamentarischen Raum ist bisher jedoch noch wenig erforscht. Dieser deutschsprachige Beitrag präsentiert empirische Belege für die künftige Nutzung von KI-basierten Werkzeugen und Diensten in einem nationalen Parlament. Die Daten wurden während eines Brainstormings im Jahr 2020 und eines virtuellen Workshops im griechischen Parlament 2021 gesammelt. Die Analyse gibt Aufschluss über die Priorisierung von KI-basierten Technologien im parlamentarischen Umfeld. Im Rahmen der Studie wurden die Relevanz und die Priorität von 210 Anwendungen sowie Themen rund um KI-Technologien mit Blick auf das griechische Parlament untersucht.

Keywords: Künstliche Intelligenz, Parlament, griechisches Parlament, Griechenland

1 Einleitung[3]

Parlamente müssen sich derzeit entscheiden, ob sie künstliche Intelligenz (KI) und KI-gestützte Anwendungen für die Erfüllung parlamentarischer Aufgaben einsetzen wollen. KI-basierte Anwendungen haben das Potenzial, verschiedene Aufgaben des parlamentarischen Alltags zu automatisieren, wie zum Beispiel das Erkennen von Mustern und Ereignissen, das Benachrichtigen relevanter Akteure, das Erstellen von Vorhersagen, das Empfehlen von Maßnahmen, das Erstellen von Prognosen, das Einleiten von Vorsichtsmaßnahmen und sogar das Treffen von Entscheidungen ohne menschliches Zutun. All

[1] The Open Government Institute, Zeppelin Universität, 88045 Friedrichshafen, joern.vonlucke@zu.de, https://orcid.org/0009-0002-0350-7571
[2] Wissenschaftliche Dienste, Hellenisches Parlament, Athen, Griechenland, fitsilisf@parliament.gr, https://orcid.org/0000-0003-1531-4128
[3] In diesem Beitrag werden Forschungsergebnisse des Teams [LF23a] erstmals in deutscher Sprache zusammengefasst. Bei diesem Beitrag handelt es sich um eine überarbeitete und weiterentwickelte Fassung, in der neben einigen Kürzungen noch zusätzliche Ergebnisse aus den laufenden Diskussionen eingeflossen sind.

doi:10.18420/rvi2023-003

dies könnte auch nahezu in Echtzeit geschehen [ELS20]. Dahinter steht jedoch weder eine einzelne Technologie noch eine Sammlung von Nischenanwendungen. Vielmehr werden heute zahlreiche Technologien der KI zugeordnet [CE21:8-12][SU21]. All diese Anwendungen können Parlamentarier in unschätzbarem Maße unterstützen und sie in die Lage versetzen, schnell und effizient fundierte Entscheidungen zu treffen. Trotz der Vorteile liegt die Entscheidung über den Einsatz von KI-Technologie für parlamentarische Aufgaben letztlich bei den Parlamenten selbst, da sie die potenziellen Vorteile gegen die ethischen und rechtlichen Erwägungen eines KI-Einsatzes abwägen müssen.

Mit Blick auf mögliche Werkzeuge, Anwendungsfelder, Nutzungsszenarien und Anforderungen sind KI-induzierte Veränderungen in Parlamenten zu erwarten. Um sich frühzeitig mit diesen Veränderungen auseinanderzusetzen und so einen breiten Überblick zu gewinnen, sollten die entsprechenden Ansätze, Potenziale und Visionen für Parlamente untersucht werden. Brainstorming-Workshops sind ein guter Weg, um einen ersten Überblick über die Bereiche und Anwendungsfelder von KI in Parlamenten zu gewinnen. Ergebnisse solcher Brainstorming-Sitzungen sollten von den nationalen Parlamenten vor Ort auf ihre Relevanz und Priorität hin überprüft werden. Ein effizienter Weg, dies zu tun, sind interaktive Workshops, in denen die Teilnehmer die Vorschläge bewerten und dann über die Ergebnisse diskutieren. Die Analyse einer solchen Bewertung gibt Aufschluss über die Priorisierung von KI-basierten Technologien im parlamentarischen Umfeld und bildet die Grundlage für die Erstellung einer Roadmap für eine nutzerorientierte Entwicklung und Implementierung von KI-basierten Lösungen.

2 Literaturüberblick

Das griechische Parlament ist das nationale Parlament der Griechischen Republik. Als wichtige Institution des griechischen politischen Systems verfügt es über eine Kammer mit 300 für vier Jahre gewählten Abgeordneten, die unter anderem die Rolle des Gesetzgebers wahrnehmen. Es ist in Generaldirektionen organisiert und nutzt Informations- und Kommunikationstechnologien (IKT), die seine parlamentarischen Funktionen, wie in der Verfassung vorgeschrieben, erleichtern und unterstützen.

Um sich schrittweise und ohne Unterbrechungen weiterzuentwickeln, hat das griechische Parlament strategische Ziele festgelegt, die in der Regel in den programmatischen Erklärungen seiner neu gewählten Präsidenten zum Ausdruck kommen. Im digitalen Bereich werden einige der Ziele durch (freiwillige) Aktionspläne im Rahmen der Open Government Partnership konkretisiert. Im Jahr 2018 wurden die Ziele in einem strukturierten Entwicklungsverfahren als vierjähriger Strategieplan 2018-2021 [HP18] (auch „Strategie“ genannt) formalisiert. Ein kombinierter Bottom-up- (für den organisatorischen Teil) und Top-down-Ansatz (für die Vision, Mission und Werte) wurde verwendet, um die notwendigen strategischen Elemente zu erfassen. Der Strategieentwurf wurde einer abschließenden Konsultation unterzogen, in der seine Struktur und die einzelnen strategischen Optionen verfeinert wurden. Die Entwicklung des strategischen Plans wurde von

der zuvor gegründeten Abteilung für strategische Planung und Management-Reengineering, die 2017 zu diesem Zweck eingerichtet wurde, geleitet und unterstützt. Die Strategie enthält wichtige Aussagen, die auf die Digitalisierung aller Aspekte des parlamentarischen Lebens abzielen, und sieht den Einsatz von Informationstechnologie zur Erreichung bestimmter institutioneller Ziele vor.

KI war bisher kein Thema mit strategischem Wert für die parlamentarischen Prozesse. Dies lässt sich jedoch dadurch erklären, dass die Strategie technologieunabhängig sein sollte. Sie enthält also Ziele und Vorgaben, nicht aber die (technologischen) Mittel, um sie zu erreichen. So wurde beispielsweise besonderer Wert auf die Einführung von Interoperabilitätsinstrumenten (Strategisches Ziel 2), die Nutzung offener Daten und die digitale Erstellung von „legislativen Arbeiten“ (Strategisches Ziel 6) gelegt. Letztere können durch den Einsatz künstlicher Intelligenz erheblich verbessert werden.

Der Einsatz von KI in Parlamenten wird immer wichtiger und kann nicht ignoriert werden. Die aus den wenigen vorliegenden Vorstudien [Ko21][FKS22] und dem Einsatz von KI in repräsentativen Institutionen gewonnenen Erkenntnisse lassen sich übertragen und wirtschaftlich nutzen. Diese haben das Rahmenwerk für den Einsatz solcher Instrumente in Parlamenten gesetzt und auf mögliche Anwendungen und Technologien für deren Implementierung hingewiesen. Andere Forscher haben die Gesetzgebung als Kernkompetenz der Parlamente untersucht [Pa22][PL22]. Interessanterweise entstanden alle diese Studien mit Beteiligung parlamentarischer „Insider“, also Forschern und Experten, die der parlamentarischen Administration angehören. Dies sollte nicht überraschen und als indirekter Beweis für die mangelnde Literaturlage gesehen werden, auf der aufgesetzt werden muss, um die KI-Entwicklung in repräsentativen Institutionen voranzutreiben.

Als Reaktion auf den gesellschaftlichen Druck beginnen die Parlamente, die Chancen und Herausforderungen der KI zu analysieren. Sowohl die Parlamentarische Versammlung des Europarates [PA20] als auch das Globale Parlamentarische Netzwerk der OECD [OE23] haben Gruppen eingerichtet, die sich mit KI beschäftigen. Trotz der breiten Anerkennung der Notwendigkeit, KI einzuführen, gibt es jedoch nur wenige Beispiele für die tatsächliche Umsetzung in den Parlamenten. Das Europäische Parlament ist wahrscheinlich die repräsentative Institution, die sich bisher am gründlichsten mit Fragen der künstlichen Intelligenz befasst hat. So hat es mehrere einschlägige Entschließungen [EP23] verabschiedet und nutzt aktiv KI-Lösungen in seiner Archivabteilung [EPHA23]. Die brasilianische Abgeordnetenkammer hat Ulysses eingeführt, eine API für eine Reihe von KI-Tools zur Verbesserung des Gesetzgebungsprozesses und zur Interaktion mit den Bürgern [Si21;So21;DA21].

Mit der eindrucksvollen Ausnahme des brasilianischen Falles und trotz fehlender empirischer Daten, erscheinen viele dieser Versuche das Ergebnis nicht-linearer Führungsentscheidungen zu sein. Genau diese Forschungslücke, die durch fehlendes institutionelles Wissen und eine inkonsistente Forschungsagenda entsteht, versucht dieser Beitrag zu schließen, indem man eine eigene Forschungsagenda erarbeitet und die für das griechische

Parlament relevanten Top-10 und Top-3 für KI-bezogene Maßnahmen, Ansätze und offene Fragen bestimmt. Diese Methode ist durchaus auf andere Parlamente übertragbar, jedoch nicht die Ergebnisse, die durch deren Anwendung produziert werden.

Ende 2022 führte die Einführung von ChatGPT [OAI23] durch OpenAI zu einem starken Anstieg des Interesses an KI-basierten Lösungen, die direkt oder indirekt Auswirkungen auf die Gesetzgebung haben. Einige Abgeordnete setzen ChatGPT beispielsweise nicht nur zum Entwurf von Grußworten und Reden im Parlament ein, sondern nutzen es auch schon als Grundlage für Gesetzentwürfe, die dann aber von den Gesetzgebern noch substanziell überarbeitet werden mussten [Ma23]. Unabhängig davon, ob es sich um einen Game Changer handelt oder nicht, müssen solche KI-Tools und die damit verbundenen Dienste von den Gesetzgebern ernst genommen werden. Diese eröffnen vielfältige Assistenzdienste, die den Mitarbeitern am Arbeitsplatz eine konkrete und spürbare Entlastung bringen kann, soweit sie richtig und verantwortungsvoll eingesetzt werden. In der Tat können Parlamente zu führenden Institutionen bei der Anwendung von KI-basierten Werkzeugen und Diensten sowohl bei der Anwendung als auch bei der Regulierung von KI werden [Fi19;Fi21]. Die Europäische Kommission hat dies erkannt und das Potenzial von KI und innovativen IKT-Werkzeugen untersucht [Pa22], um überzeugende Vorschläge zur Verbesserung der Rechtsetzung als Kernaufgabe der Parlamente zu kennen.

3 Forschungsansatz

Bei der Konzeption der Studie ging es in erster Linie darum, einen geeigneten Forschungsansatz zu finden, der es erlaubt, ein breites, detailliertes und praxisnahes sowie vielfältiges und nicht einseitig perspektivisches Spektrum möglicher Anwendungsbereiche von KI in Parlamenten zu betrachten. Dabei ist zu beachten, dass sich KI-Tools technisch in mehrere Arbeitsbereiche unterteilen lassen, wie zum Beispiel Zusammenfassung, Klassifizierung, Stimmungsanalyse, semantische Analyse und Empfehlung. Spezifische Technologien und Algorithmen, wie NLP, BERT und GPT-X, können je nach Fall unterschiedlich eingesetzt werden. Da sich Technologien und Algorithmen jedoch rasch weiterentwickeln, wurde eine technologieunabhängige Studie als sinnvoll erachtet. Darüber hinaus sollte es bei der Studie nicht nur um die Sammlung bestehender Lösungen gehen, sondern auch um das Erfassen von Ideen für die Zukunft von Parlamenten, selbst wenn diese noch nicht technisch realisierbar zu sein scheinen. Viele dieser Ideen eignen sich als Leitbilder, die zu langfristigen Visionen und gestaltungsorientierten Ansätzen weiterentwickelt werden können und die Grundlage für Folgenabschätzungen bilden [LF22;LF23].

Für die offene Ideensammlung wurde die Methode des Brainstormings gewählt [Cl89]. Die Methode wurde in zwei Runden auf eine Gruppe von drei Experten aus Wissenschaft und parlamentarischer Praxis angewandt, die folgende Grundvoraussetzungen erfüllten: ausreichende Expertise durch Studium, eigene Forschung zum Thema, praktische Erfahrung und berufliche Fähigkeiten. Als cloudbasierte Brainstorming-Plattform wurde

XLeap eingesetzt [XL23]. In der ersten Runde wurden Ideen für den Einsatz von KI-Technologien in Parlamenten gesammelt und sortiert. In der zweiten Runde wurden die Beiträge überprüft, ergänzt und reflektiert [LF22;LF23].

Die vorläufigen Ergebnisse des Brainstormings können einer parlamentarischen Fachgemeinschaft zur eingehenderen Bewertung vorgelegt werden. Anstelle einer gemischten Beteiligung aus verschiedenen Parlamenten (siehe [Ko21]) wird davon ausgegangen, dass Verwaltungsangestellte und Abgeordnete aus einem einzigen Parlament homogenere Antworten geben. Für diese Zielgruppe scheint eine anschließende Nutzwertanalyse [Rö98] geeignet, um den Nutzen, die Relevanz und die Notwendigkeit der generierten Vorschläge zu ermitteln. Zu diesem Zweck wurde eine Nutzwertanalyse und eine XLeap-basierte Nutzwertbefragung zur Relevanz und Priorität von KI-Vorschlägen mittels zwei unterschiedlicher Fragestellungen durchgeführt. Zunächst wurde für jeden Eintrag die Relevanz des Vorschlags auf einer Likert-Skala von 0 (irrelevant) über 5 (relevant) bis 10 (unbedingt erforderlich) abgefragt. Zweitens wurde die Priorität des Vorschlags mit dem Jahr der Umsetzung als Parameter abgefragt. In diesem Fall reichte die Likert-Skala von 0 (2020) über 5 (2025) bis 10 (2030). Jeder dieser Werte kann in ein konkretes Datum umgerechnet werden (0: 31.12.2020; 5: 31.12.2025; 10: 31.12.2030). Später zu setzenden Zeitziele sowie unrealistische Vorschläge sollten von den Teilnehmern mit dem Maximalwert 10 bewertet werden [LF22;LF23].

4 Ergebnisse des Brainstormings

Auf der Grundlage des ursprünglichen Forschungskonzepts wurde am 14. Juli 2020 eine vierstündige Online-Brainstorming-Sitzung unter Beteiligung von drei ausgewiesenen Experten organisiert. Insgesamt wurden 196 Beiträge gesammelt, die die offene Frage beantworteten: „Wo gibt es Anwendungsfelder für KI in der Arbeit und im Umfeld von digitalen Parlamenten?“ Nach der Eliminierung von Überschneidungen wurde die Zahl der Vorschläge auf 181 reduziert und die Ideen wurden nach Themenbereichen geclustert. Im Zuge einer weiteren Überarbeitung kamen weitere Ideen hinzu und alle Beiträge wurden erneut gesichtet, diskutiert und teilweise überarbeitet. Die endgültige Clusterung umfasste 210 Einträge, die neun Themenbereichen (Cluster) (Tab.) zugeordnet sind. Die Gesamtübersicht aller Vorschläge („210er Liste“) wurde in einem gesonderten Beitrag als Agenda für Forschung und Entwicklung zum Einsatz von KI in Parlamenten vorgestellt und diskutiert [LF23].

Ergebnisse des Brainstormings		Vorschläge		Breite: Likert-Skala	
Nr.	Themenbereiche (Cluster)	n	Anteil	Relevanz	Priorität
#1	Parlamentarier	13	0,06	0..10	0..10
#2	Gesetzgebung	36	0,17	0..10	0..10

#3	Parlamentarische Kontrolle und parlamentarische Diplomatie	14	0,07	0..10	0..10
#4	Politische Bildung und Landeskultur	17	0,08	0..10	0..10
#5	Parlamentsverwaltung, Parlamentsgebäude, Fahrdienst und Parlamentspolizei	37	0,18	0..10	0..10
#6	Parlamentspräsidium, Parlamentsdirektorate und Wahlen	19	0,09	0..10	0..10
#7	Wissenschaftliche Dienste	13	0,06	0..10	0..10
#8	Rahmenwerk	47	0,22	0..10	0..10
#9	Offene Fragestellungen	14	0,07	0..10	0..10

Tab. 1: Statistische Zusammenfassung der Brainstoming-Ergebnisse vom Juli 2020

5 Ergebnisse der Bewertungen von Akteuren rund um das griechische Parlament

Acht Monate nach dem Brainstorming-Workshop fand am 18. März 2021 im griechischen Parlament ein virtueller Workshop statt, um die Vorschläge aus dem Brainstorming zu bewerten. Die 14 Teilnehmer, neun Männer und fünf Frauen, kamen aus sieben verschiedenen parlamentarischen Bereichen. Auch Abgeordnete und ihre Mitarbeiter waren eingeladen, um die Nachfrageseite des griechischen Parlaments zu vertreten. Die Vorbereitungsphase dauerte zwei Wochen, in denen mehrere Gespräche geführt wurden, um verschiedene Aspekte der Studie und spezifische organisatorische Fragen zu klären. Um Zeit für den Workshop zu sparen, wurde den Teilnehmern im Voraus die griechische Übersetzung des Fragebogens zugesandt [LF22].

Zu Beginn des Workshops wurden der Ablauf und das Ziel des Ratings vorgestellt. Alle Teilnehmer wurden auch darüber informiert, dass sie zeitnah die Ergebnisse in Form eines elektronischen PDF-Dokuments zum Abschluss des Workshops erhalten würden. Die Teilnehmer bewerteten dann einzeln und anonym alle 210 KI-bezogenen Vorschläge, die jeweils in Blöcke zu den neun Themenbereichen unterteilt waren. Die Relevanz- und Prioritätswerte für jeden einzelnen Vorschlag wurden mit Hilfe der Moderationssoftware XLeap in dem in Abschnitt 3 erläuterten Setup erfasst und dokumentiert.

Was die Ergebnisse des Workshops im griechischen Parlament betrifft, so erreichten die durchschnittlichen Bewertungen der Vorschläge Werte von 4,31 bis 9,38 auf einer Skala von 0 bis 10. Die fünf am höchsten bewerteten Vorschläge (Top 5) erhielten eine Note von 9,08 oder besser. Elf von 210 Vorschlägen (5,2 %) erreichten eine Bewertung von 9,0 oder besser, während 69 Vorschläge (32,8 %) mit 8,0 oder besser bewertet wurden. Der für die Relevanzskala entscheidende Cut-off-Punkt von 7,5 und besser wurde von 118 der

210 Vorschläge (56,2 %) erreicht. Überraschenderweise wurden 209 von 210 Vorschlägen (99,5 %) mit einem Wert von über 5,0 (relevant) und 210 (100 %) mit einem Wert von über 2,5 beurteilt. Nur die bekannte Typologie von Misuraca und van Noordt [MN20] wurde mit einer Relevanz von 4,31 bewertet. Diese Ergebnisse und die Auswertung der Teilnehmermeinungen unterstreichen ein bemerkenswert hohes Interesse an KI für die zukünftigen Arbeitsabläufe des griechischen Parlaments. Insgesamt gab es wertvolles Feedback für die Vorschläge und für die Forschungs- und Entwicklungsagenda des Forschungsteams. Die Empfehlungen für die Umsetzung dieser Vorschläge sehen einen Umsetzungszeitraum zwischen Dezember 2021 und November 2026 vor. Damit handelt es sich um Zeiträume, die zum damaligen Zeitpunkt alle noch in der Zukunft lagen. [LF23].

6 Diskussion: Ergebnisse und Kommentare

Für die weitere Analyse der Ergebnisse wurden vier verschiedene Arten von Bewertungen aus dem gesamten Datensatz gezogen. Erstens werden die Top 10 der als am relevantesten bewerteten Vorschläge (Kapitel 6.1, Tabelle 1) zusammengestellt, d.h. welche Fragen beantwortet werden müssen und welche Projekte unbedingt umgesetzt werden sollten. Zweitens werden die Top-10-Vorschläge mit der höchsten Priorität (Kapitel 6.2, Tabelle 2) zusammengestellt, d. h. welche am schnellsten umgesetzt werden sollten. Drittens werden für die acht Themencluster die jeweiligen Top-3-Optionen (sortiert nach Relevanz, Kapitel 6.3, Tabelle 3) diskutiert. Dies gibt einen Überblick über alle Themenbereiche, welche Prioritäten in den einzelnen Clustern gesetzt werden. Viertens werden die Top 3 der offenen Fragen (sortiert nach Relevanz, Kapitel 6.4, Tabelle 4) analysiert, um festzustellen, welche Themen bearbeitet werden müssen und welche Diskussionen zuerst angestoßen werden sollten.

6.1 Top 10 zu Relevanz von allen Vorschlägen

Die Ergebnisse des Brainstormings und die Bewertung der Auswahl der Teilnehmer durch das griechische Parlament zeigen ein bemerkenswert hohes Interesse an KI. Die Top 10 aller 210 Vorschläge haben eine Relevanzbewertung von 9,00 oder besser auf einer Skala von 0 bis 10 erhalten.

		Relevanz 0..10		Priorität 31.12.20-31.12.30	
Nr.	Beitrag	↓Ø	SA	Ø	SA
9,01	[131.-] Voraussetzungen: Training und Einstellung von neuen Mitarbeitern in der IT-Abteilung?	9,38	0,08	02.12.2021	0,06
8,01	[211.-] Parlamentarische KI-Systeme mit European Interoperability Framework (EIF, weiterentwickelt mit KI-Portfolio) verbinden	9,38	0,08	19.05.2022	0,12
9,02	[136.-] Ethische Aspekte des Betriebs von KI-basierten Systemen	9,31	0,08	29.01.2022	0,09
9,03	[97.-] Reflexion über die Grenzen des Einsatzes von KI im Parlament	9,15	0,13	29.01.2022	0,10
9,04	[214.-] Wahl-Engineering: Wahlbezirke per KI so umstrukturieren, dass die repräsentative Funktion des Parlaments verbessert werden (klingt nach Gerrymandering, aber es ist genau das Gegenteil)	9,08	0,13	23.04.2022	0,07
8,03	[159.-] Besondere Schutzmaßnahmen beim Einsatz algorithmischer Systeme im Kontext menschlicher Entscheidungen,	9,08	0,11	19.05.2023	0,25
8,02	[114.-] EU/Mercosur-unterstützte Systeminteroperabilität	9,08	0,10	06.11.2023	0,24
5,01	[71.-] Automatische KI-basierte Text- und Spracherfassung	9,00	0,10	15.10.2022	0,23
5,02	[216.-] Grenzen des Parlamentarismus in Zeiten des Einsatzes durch KI: Folgen unüberschaubar - Welche KI-Dienste werden erlaubt und welche müssen verboten werden, um die Funktionalität und Integrität des Parlaments nicht zu gefährden?	9,00	0,11	11.05.2023	0,28
9,05	[139.-] Definition des „Smartes Parlament“-Konzepts, was gehört hinzu?	9,00	0,14	16.07.2022	0,26

Tab. 2: Multikriterien-Tabelle für das Griechische Parlament, sortiert nach Relevanz.

Unter den zehn wichtigsten Vorschlägen für das griechische Parlament, die aufgrund ihrer hohen Relevanz unbedingt umgesetzt werden sollten, befinden sich fünf offene Fragen (9,01-9,05), vier Forderungen (5,02; 8,01; 8,02; 8,03) und nur ein konkreter Vorschlag (5,01). Die Gestaltung von Schulungen und einer Rekrutierungskampagne, ethische As-

pekte und die Grenzen des Einsatzes von KI in Parlamenten, eine KI-basierte Umstrukturierung von Wahlkreisen und die Konkretisierung des Konzepts eines intelligenten Parlaments werden als offene Fragen bewertet, die dringend geklärt werden müssen. Auch die Einbindung in das europäische Interoperabilitätsrahmenwerk und die damit verbundene Systeminteroperabilität sowie spezifische Sicherheitsanforderungen für den Einsatz algorithmischer Systeme im Kontext menschlicher Entscheidungen sind zu klären. Gefordert wird auch ein pragmatischer Umgang mit den unkalkulierbaren Folgen des Einsatzes von KI, etwa durch die Vorlage von Erlaubnis- und Verbotslisten zur Wahrung der Integrität und Arbeitsfähigkeit des Parlaments. Darüber hinaus werden KI-basierte Anwendungen zur automatischen Texterfassung von Manuskripten und Reden gefordert. Letzteres ist der am höchsten bewertete technische Vorschlag hinsichtlich seiner Relevanz und sollte im Hinblick auf eine fortgeschrittene Umsetzung genau geprüft werden. Denn dem griechischen Parlament sind derartige Lösungen nicht fremd. In den späten 2000er Jahren wurde eine Sprache-zu-Text-Anwendung erfolglos getestet. Mehr als ein Jahrzehnt später wurde die Spracherkennung für die halbautomatische Erstellung von Protokollen eingeführt [FP21], obwohl ihre Entwicklung schon früher begann.

6.2 Top 10 zu Priorität von allen Vorschlägen

In Bezug auf die Priorität, die auch im Zusammenhang mit den Umsetzungserwartungen steht, ist festzustellen, dass die Teilnehmer im März 2021 die Zieltermine in die Jahre zwischen Dezember 2021 und November 2026 legten, was einem Zeitraum von fünf Jahren entspricht und somit innerhalb eines überschaubaren Planungshorizonts liegt. Der Termin der nächsten Parlamentswahlen im Frühjahr 2023 könnte dabei eine Rolle gespielt haben. Der Maximalwert von 10 Jahren (2030) wurde selten als Zielvorgabe gewählt. Obwohl alle Standardabweichungen zwischen 0,06 und 0,35 liegen, wobei 19 Werte von 0,30 oder mehr (9,0%) auf eine abweichende Einschätzung hindeuten, hält sich die Abweichung innerhalb der Kohorte in überschaubaren Grenzen. Je niedriger der Wert, desto näher liegen die Einschätzungen der Experten im Zeitverlauf beieinander.

		Relevanz 0..10		Priorität 31.12.20-31.12.30	
Nr.	Beitrag	↓Ø	SA	Ø	SA
9,01	[131.-] Voraussetzungen: Training und Einstellung von neuen Mitarbeitern in der IT-Abteilung?	9,38	0,08	02.12.2021	0,06
9,02	[136.-] Ethische Aspekte des Betriebs von KI-basierten Systemen	9,31	0,08	29.01.2022	0,09
9,03	[97.-] Reflexion über die Grenzen des Einsatzes von KI im Parlament	9,15	0,13	29.01.2022	0,10

7,01	[15.-] KI-basierte intelligente Dokumentensuche in der Parlamentsbibliothek und im ePublikationsraum von Bibliothek/Wissenschaftlicher Dienste	8,69	0,26	03.03.2022	0,13
4,01	[27.-] Intelligente, KI-basierte Suchfunktionen im Frontend der Webseite des Parlaments	8,57	0,19	17.03.2022	0,20
9,04	[215.-] Wahl-Enginering: Wahlbezirke per KI so umstrukturieren, dass die repräsentative Funktion des Parlaments verbessert werden	9,08	0,13	23.04.2022	0,07
8,01	[211.-] Parlamentarische KI-Systeme mit European Interoperability Framework (EIF, weiterentwickelt mit KI-Portfolio) verbinden	9,38	0,08	19.05.2022	0,12
9,09	[127.-] Mögliche Problemfelder: Sicherheitsanalyse und Zusammenarbeit dieser Systeme	8,08	0,22	17.06.2022	0,11
8,14	[161.-] Gesetzlicher Diskriminierungsschutz	8,69	0,19	17.06.2022	0,16
8,19	[103.-] Sicherstellung einer zweckadäquaten Datenqualität	8,46	0,14	16.07.2022	0,13

Tab. 3: Multikriterien-Tabelle für das Griechische Parlament, sortiert nach Prioritäten.

Unter den 10 wichtigsten Vorschlägen für das griechische Parlament, die mit zeitlicher Priorität (bis Juli 2022) umgesetzt werden sollen, befinden sich fünf offene Fragen (9,01; 9,02; 9,03; 9,04; 9,09), drei Anforderungen (8,01; 8,14; 8,19) und nur zwei konkrete Vorschläge (4,01 & 7,01). Die Ausbildung und Einstellung neuer Mitarbeiter, ethische Aspekte und Grenzen des Einsatzes von KI im Parlament sind dringend zu klären. Eine KI-gestützte Dokumentensuche für die Parlamentsbibliothek, den digitalen Lesesaal der Bibliothek und die Wissenschaftlichen Dienste soll den Nutzern die Suche nach und den Zugriff auf relevante Dokumente deutlich erleichtern. Auch eine KI-gestützte Suchfunktion auf der Startseite der Parlamentswebsite soll für Entlastung sorgen, wenn sie eine qualitativ hochwertige und schnelle Beantwortung von Anfragen ermöglicht. Zudem muss bald geklärt werden, ob KI zur Neueinteilung von Wahlbezirken und zur Durchführung von Sicherheitsanalysen eingesetzt werden kann, oder ob dies neue Probleme schafft. Darüber hinaus wird ein Rahmen für die Einbindung von KI in den europäischen Interoperabilitätsrahmen, für den rechtlichen Schutz vor Diskriminierung und für Mindestanforderungen an die Datenqualität für den Einsatz von KI im Parlament benötigt. Zwei Jahre später, im März 2023, hat das griechische Parlament keines dieser Probleme in Angriff genommen. Bis vor kurzem schien diese Einstufung daher zu optimistisch gewesen zu sein. Seit Einführung von ChatGPT scheint der Zeitplan für die Einführung dieser Vorschläge plötzlich machbar zu werden, trotz einiger Herausforderungen.

6.3 Top 3 zu Relevanz für jedes Cluster

Bei der Betrachtung der beiden Top-10-Rankings fällt auf, dass viele Fragen und Rahmenvorgaben, aber relativ wenige Vorschläge darunter sind. Vielleicht gibt es zu viele unbeantwortete Fragen, die es nahelegen, zunächst über Chancen und Risiken nachzudenken. Aus diesem Grund werden in diesem Abschnitt die Top 3 für jedes der acht Cluster betrachtet (Tabelle 3) und anschließend die Verteilung der Vorschläge visuell dargestellt (Abbildungen 1-8). Anzumerken ist, dass die Top 3 nach Relevanz und, falls zutreffend, nach der geringsten Standardabweichung ausgewählt wurden. Auf diese Weise konnten für jedes Cluster eindeutig drei Vorschläge ausgewählt werden, die sich für eine eingehende Analyse auch aus parlamentarischer Sicht eignen.

Das erste Cluster (Parlamentarier) umfasst 13 Vorschläge. Besonders hohe Bewertungen (Tabelle 3) erhielten ein dank KI-Diensten zuverlässiges Abstimmungssystem für das Plenum und die Ausschüsse (9,00), der Einsatz von KI-basierten Textanalysediensten (8,43) und KI-gestützte Dienste (8,07), die die Arbeit der Abgeordneten im Parlament und in ihren Wahlkreisen erheblich vereinfachen. Die Menschen im Parlament suchen nach substanziellen Erleichterungen für ihre Arbeit, ohne dabei alles grundsätzlich in Frage stellen zu wollen. Zuverlässige Abstimmungssysteme, Textanalytik und andere KI-basierte Dienste können die Abgeordneten und ihre Mitarbeiter potenziell stark entlasten.

Das zweite Cluster enthält Anwendungsbereiche in der Gesetzgebung und umfasst 36 Vorschläge [LF22]. Hohe Bewertungen (Tabelle 3) erhielten die intelligente Prüfung von Gesetzgebungsvorschlägen auf mögliche Auswirkungen auf andere Vorschriften (8,57), die Umwandlung von Rechtsvorschriften (Code) in maschinenverständlichen E-Code (8,57) und eine Sammlung aller kodierten Gesetze (Smart Law) mit der Möglichkeit der KI-Interpretation der Rechtsvorschriften (8,50). Der Grund für die große Begeisterung für diese drei Vorschläge liegt darin, dass solche komplexen Projekte heute, wenn überhaupt, nur noch über komplexe Rechtsinformationssysteme und die Verwendung moderner Dokumentenstandards wie Akoma Ntoso [AN23] und semantischer Webstandards möglich sind. Die Komplexität und der bisherige zeit- und arbeitsintensive Aufwand der entsprechenden Recherchen machen „intelligente Audits“ für Parlamentsjuristen besonders attraktiv.

Das dritte Cluster um parlamentarische Kontrolle und parlamentarische Diplomatie enthält 14 Vorschläge. Zu den Top 3 dieses Clusters (Tabelle 3) gehören KI-gestützte Maßnahmen zur Verringerung von Voreingenommenheit oder Diskriminierung mit KI-gestützten Vorschlägen zur Beseitigung (7,64), algorithmische Überprüfungen von legislativen Bewertungsberichten (7,21) und die Entwicklung von KI-gestützten Technologien zur Bekämpfung von Fake News (7,07). Die Raten für diese Top-3-Gruppe sind niedriger und auch die niedrigsten im Vergleich zu allen anderen Clustern. Der Grund dafür könnte in der Komplexität solcher Lösungen liegen, die eine einfache Umsetzung nicht zulassen.

Das vierte Cluster zu den Themen staatsbürgerliche Bildung und Landeskultur umfasst 17 Vorschläge. Die drei wichtigsten Vorschläge dieses Clusters (Tabelle 3) sind nutzerorientiert und leicht umzusetzen. Der erste Vorschlag fordert intelligente, KI-gestützte Suchfunktionen für das Frontend der Parlamentswebsite (8,57), die die Zugänglichkeit verbessern und die Menschen zu den Daten und Dokumenten bringen könnten, nach denen sie suchen. Ein KI-basierter Coach für Jugendliche und Bürger könnte die Arbeit des Parlaments, seine Prozesse und die Tätigkeit der Abgeordneten auf leicht verständliche Weise erklären (8,00). Wichtig erscheint auch der Aufbau von Kapazitäten für den Einsatz von KI in den parlamentarischen Gremien für die Mitarbeiter des Parlaments und für die Abgeordneten (8,00).

Das fünfte Cluster um Parlamentsverwaltung, Parlamentsgebäude, Fahrdienst und Parlamentspolizei enthält 37 Vorschläge. Zu den drei am höchsten bewerteten Vorschlägen (Tabelle 3) gehören eine KI-basierte Lösung zur automatischen Text- und Spracherfassung (9,00), eine Verordnung über die Zulassung und das Verbot von KI-Diensten im Parlament (9,00) und KI-basierte virtuelle Assistenten für behinderte Menschen auf parlamentarischen Webseiten (8,86). KI kann die Digitalisierung von Dokumenten und Gedanken beschleunigen, indem sie lernt, Sprache, Text und Bilder zu erfassen und zu verarbeiten. KI-basierte Assistenten vereinfachen den Zugang zu komplexen Themen mit Lese- und Navigationshilfen sowie Zusammenfassungen. Durch die Integration entsprechender Dienste in Textverarbeitungssysteme kennen und schätzen die Administratoren diese Funktionen bereits. Gleichzeitig besteht jedoch die Sorge, dass die Nutzung von internetfähiger KI zu unbeabsichtigten Schäden, Spionage oder Sabotage führen kann und damit die Funktionsfähigkeit und Integrität des Parlaments gefährdet wird. Erlaubnis- und Verbotslisten geben den Mitarbeitern zumindest eine gewisse Sicherheit darüber, was erlaubt und was verboten ist, auch wenn dies keinen vollständigen Schutz bieten kann.

Das sechste Cluster rund um das Parlamentspräsidium, Parlamentsdirektorate und Wahlen umfasst 19 Vorschläge. Zu den drei wichtigsten Vorschlägen (Tabelle 3) gehören der Fernzugriff auf das Parlament und die Stimmabgabe für Abgeordnete (8,71), die KI-gestützte Prozessautomatisierung im Parlament (8,29) und ein Index für das Einkommen von Politikern (8,14). Um Identitätsdiebstahl zu verhindern, können KI-basierte Sicherheitsmaßnahmen den Abgeordneten helfen, sich aus der Ferne zu engagieren und sicher abzustimmen. KI-basierte Prozessautomatisierung eröffnet dem Parlament zahlreiche Optimierungen, sobald Prozessmanagement praktiziert wird und elektronische Prozesse vollständig gespeichert werden. Da die Erfassung der Einkünfte und Nebeneinkünfte von Politikern komplex, volatil und langwierig ist, können KI-Anwendungen eine kontinuierliche Überwachung, Vergleiche und ein funktionierendes Berichtswesen gewährleisten.

Das siebte Cluster rund um die Wissenschaftlichen Dienste und die parlamentarische Bibliothek enthält 13 Vorschläge. Die Top 3 dieses Clusters (Tabelle 6) beinhalten eine KI-basierte Dokumentensuche in der Parlamentsbibliothek und dem E-Publikationsraum der wissenschaftlichen Dienste (8,69), die den Zugang zu relevanten Dokumenten vereinfacht, einen KI-basierten Bibliotheksdienst (8,23), der Empfehlungslisten mit Lesetipps

auf Basis von Empfehlungen, Bedarf und Arbeitsprofil generieren kann, sowie Technologieentwicklung und ethisch korrekte Richtlinien für die Gestaltung des KI-Einsatzes in der parlamentarischen Arbeit (8,08).

Im achten Cluster finden sich 47 Vorschläge, die für die Gestaltung eines Rahmenwerks für den Einsatz von KI in Parlamenten relevant sind. Darunter befinden sich Leitbilder, Anwendungsfelder, Einsatzbereiche und relevante Grenzen. Zu den Top 3 des Rahmenwerks (Tabelle 3) gehören die Einbindung in den europäischen Interoperabilitätsrahmen (9,38), eine EU-weite Systeminteroperabilität (9,08) und besondere Sicherheitsvorkehrungen beim Einsatz algorithmischer Entscheidungssysteme (9,08). Die Gründe für diese Bewertung liegen in der chronisch mangelnden Interoperabilität von IKT-Systemen und den intensiven Diskussionen in Europa über das europäische KI-Gesetz.

		Relevanz 0..10		Priorität 31.12.20-31.12.30	
Nr.	Beitrag	↓Ø	SA	Ø	SA
1,01	[137.-] Verlässliche Abstimmungssysteme (durch KI-Technologien) im Plenum und in Ausschüssen	9,00	0,16	17.03.2024	0,29
1,02	[74.-] Einsatz von Text Analytics	8,43	0,15	15.04.2024	0,25
1,03	[138.-] Smarter Abgeordneter - KI-basierte Dienste zur Unterstützung von Abgeordneten im Parlament und in ihrem Wahlkreis	8,07	0,12	31.12.2025	0,23
2,01	[20.-] Intelligente Prüfung von Gesetzgebungsvorhaben auf Wechselwirkungen mit weiteren Regelungen	8,57	0,12	02.07.2023	0,19
2,02	[26.-] Transformation der Gesetzgebung (Code) in maschinenverständlichen E-Code	8,57	0,20	16.10.2023	0,24
2,03	[125.-] Smart Law - Sammlung aller codierter Gesetze mit der Möglichkeit der KI-Interpretation der Gesetzgebung	8,50	0,13	31.12.2023	0,25
3,01	[165.-] KI-basierte Maßnahmen zur Reduktion des Bias/Diskriminierung mit KI-basierten Vorschlägen zur Beseitigung (Bias-Reduction and Counter-Balancing per KI)	7,64	0,20	22.08.2023	0,20
3,02	[143.-] Algorithmische Prüfungen von Berichten zur Evaluation von Gesetzen	7,21	0,26	17.03.2024	0,22
3,03	[188.-] Entwicklung von KI-basierten Counter-Fake-News-Technologien	7,07	0,26	27.07.2023	0,22

4,01	[27.-] Intelligente, KI-basierte Suchfunktionen im Frontend der Webseite des Parlaments	8,57	0,19	17.03.2022	0,20
4,02	[191.-] KI-basierter Coach für Jugendliche und Bürger (KI-Apps; Dystopie: KI-Überwachung von Schülern, KI-basierte Propaganda, Videoanalyse in Klassenzimmern und Bibliotheken, Ki-basierte Überwachung von Social Distancing)	8,00	0,17	26.07.2024	0,29
4,03	[201.-] Wichtiger Punkt: Kapazitätsbildung bezüglich KI bei Parlamentsangestellten sowie Abgeordneten	8,00	0,20	11.05.2023	0,21
5,01	[71.-] Automatische KI-basierte Text- und Spracherfassung	9,00	0,10	15.10.2022	0,23
5,02	[216.-] Grenzen des Parlamentarismus in Zeiten des Einsatzes durch KI: Folgen unüberschaubar - Welche KI-Dienste werden erlaubt und welche müssen verboten werden, um die Funktionalität und Integrität des Parlaments nicht zu gefährden?	9,00	0,11	11.05.2023	0,28
5,03	[226.-] Virtuelle KI-Assistenten für Behinderte (z.B. Lese- und Navigationshilfen) auf den Webseiten des Parlaments	8,86	0,11	10.11.2022	0,24
6,01	[223.-] Sollte man Abgeordnete generell einen Remote Zugang (aus der Ferne) zum Parlament und zu Abstimmungen erlauben? (möglich durch 5G-Netze)	8,71	0,22	16.09.2022	0,19
6,02	[33.-] KI-basierte Prozessautomation im Parlament, auf Basis des vorhandenen Prozessmanagements und elektronischer Prozesse	8,29	0,17	18.03.2023	0,21
6,03	[205.-] Verdienstspiegel der Politiker - Unangemessene überproportionale Bereicherung der Politiker wird transparent, lässt sich durch KI-Applikationen laufend beobachten	8,14	0,24	31.12.2023	0,24
7,01	[15.-] KI-basierte intelligente Dokumentensuche in der Parlamentsbibliothek und im ePublikationsraum von Bibliothek/Wissenschaftlicher Dienste	8,69	0,26	03.03.2022	0,13
7,02	[207.-] KI-Dienste in parlamentarischen Bibliotheken: Leserprofil generiert KI-basiert Neuempfehlungsleseliste, KI-basierte Lesetipps (auf Grund von Empfehlungen: Leser denen dieses Buch gefällt, haben auch ,,,,), KI-basiertes Literatur- und Studienprofil (Metadaten, Zusammenfassung, Grafiken)	8,23	0,25	30.10.2022	0,17

7,03	[98.-] Forschung: Technologieentwicklung und ethisch fundiertes Design zur Parlamentsarbeit	8,08	0,18	31.12.2022	0,17
8,01	[211.-] Parlamentarische KI-Systeme mit European Interoperability Framework (EIF, weiterentwickelt mit KI-Portfolio) verbinden	9,38	0,08	19.05.2022	0,12
8,02	[114.-] EU/Mercosur-unterstützte Systeminteroperabilität	9,08	0,10	06.11.2023	0,24
8,03	[159.-] Besondere Schutzmaßnahmen beim Einsatz algorithmischer Systeme im Kontext menschlicher Entscheidungen,	9,08	0,11	19.05.2023	0,25

Tab. 4: Multikriterien-Tabelle für die Top 3 pro Cluster - Griechisches Parlament - Relevanz.

Die visuelle Clusteranalyse zeigt eine Anhäufung der Vorschläge in allen Clustern, auch wenn jedes Cluster eine unterschiedliche Anzahl von Vorschlägen aufweist. Konkret lässt sich in den Abbildungen 1-8 eine gewisse Korrelation zwischen Relevanz und Priorität erkennen. Nach dem sich wiederholenden Muster sollten Vorschläge mit höherer Priorität schneller umgesetzt werden. Projekte mit geringerer Priorität erhalten mehr Zeit für die Umsetzung. Insgesamt hat sich ein enges Cluster für Werte zwischen 6-9 (Relevanz) und 2-6 (Priorität: 2022-2026) gebildet. Anzumerken ist zudem, dass alle zeitlichen Zielmarken zum Zeitpunkt der Bewertung noch in der Zukunft lagen. Auch in den anschließenden Diskussionen entstand nicht der Eindruck, dass im griechischen Parlament eine Umsetzung von KI-Lösungen vorbereitet oder bereits abgeschlossen wurde. Dennoch sollte bedacht werden, dass dies nur die Eindrücke eines einzigen Workshops sind und dass die Ergebnisse der Priorisierung in anderen nationalen Parlamenten anders ausfallen könnten. Sobald dem Team mehrere Analysen zu anderen Staaten vorliegen, empfiehlt sich die Durchführung einer vergleichenden Analyse.

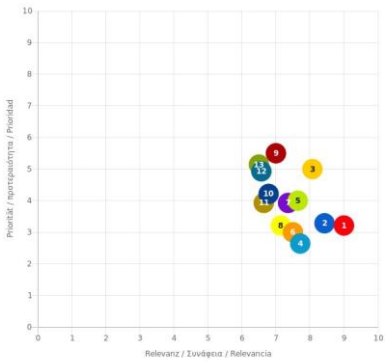

Abb. 1: Cluster #1 – Parlamentarier

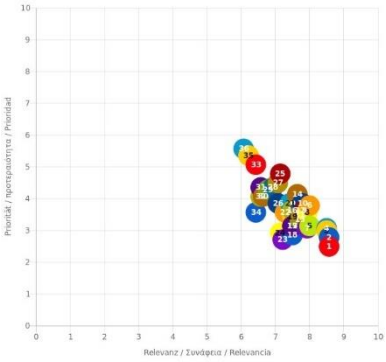

Abb: 2: Cluster #2 – Gesetzgebung

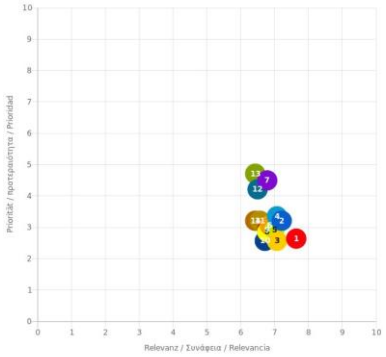

Abb. 3: Parlamentarische Kontrolle & Co

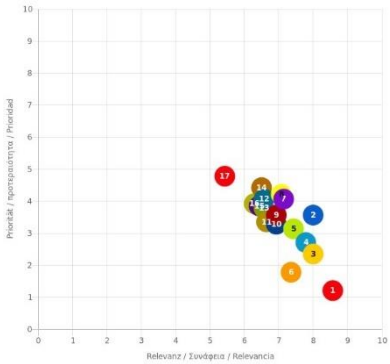

Abb. 4: Politische Bildung und Landeskultur

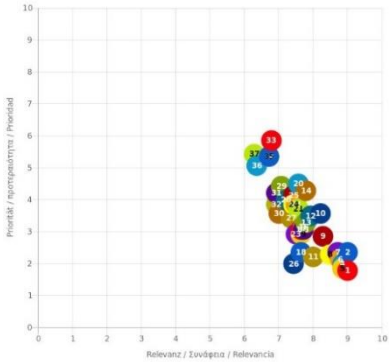

Abb. 5: Parlamentsverwaltung & Co

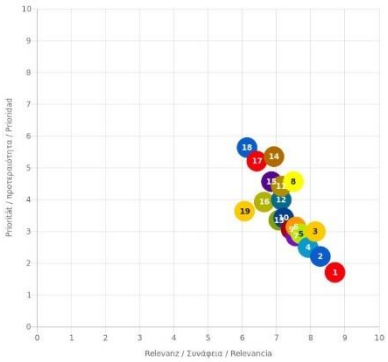

Abb. 6: Parlamentarisches Präsidium & Co

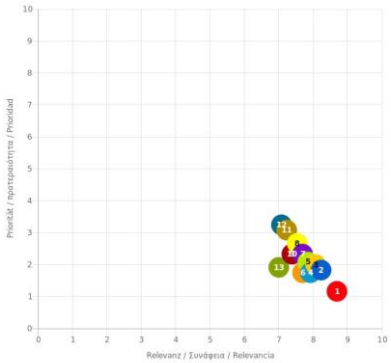

Abb. 7: Wissenschaftliche Dienste

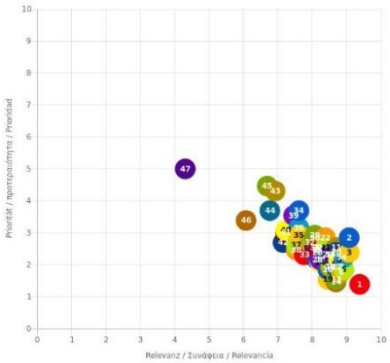

Abb. 8: Rahmenwerk

6.4 Top 3 der offenen Fragestellungen

Abschließend werden die Top-3-Fragen zum Einsatz von KI in Parlamenten (Tabelle 4), die als offen angesehen werden, näher untersucht. Betrachtet man die folgende Reihenfolge, so fällt auf, dass praktische, nutzerbezogene Fragen wichtiger zu sein scheinen als allgemeine Fragen und dass es keine einfachen Antworten gibt: Wie positioniert sich das Parlament in Bezug auf Personal, Ausbildung und Einstellung neu? (9,38) Diese Frage ist relevant, weil der Einsatz von KI im Parlament eine Belegschaft erfordert, die in der Lage ist, mit KI-Technologien zu arbeiten. Das Parlament muss sich neu aufstellen, um Personal mit den erforderlichen Fähigkeiten zu gewinnen und auszubilden. Welche ethischen Aspekte werden relevant? (9,31) Der Einsatz von KI im Parlament wirft ethische Fragen auf, die geklärt werden müssen, insbesondere wie sich der Einsatz von KI auf den Datenschutz, die Sicherheit und andere ethische Fragen auswirken könnte. Wo liegen die Grenzen des Einsatzes von KI im Parlament? (9,15) Der Einsatz von KI im Parlament kann in Bezug auf ihre Wirksamkeit, Genauigkeit und mögliche Verzerrungen Grenzen haben. Es ist wichtig, diese Grenzen bei der Implementierung von KI im Parlament zu berücksichtigen.

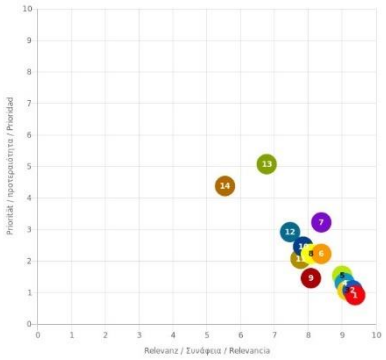

Abb. 9: Offene Fragestellungen

		Relevanz 0..10		Priorität 31.12.20-31.12.30	
Nr.	Beitrag	↓Ø	SA	Ø	SA
9,01	[131.-] Voraussetzungen: Training und Einstellung von neuen Mitarbeitern in der IT-Abteilung?	9,38	0,08	02.12.2021	0,06
9,02	[136.-] Ethische Aspekte des Betriebs von KI-basierten Systemen	9,31	0,08	29.01.2022	0,09
9,03	[97.-] Reflexion über die Grenzen des Einsatzes von KI im Parlament	9,15	0,13	29.01.2022	0,10

Tab. 5: Multikriterien-Tabelle für offene Fragestellungen - Griechisches Parlament - Relevanz

7 Zusammenfassung und Ausblick

Ein kreativer Forschungsansatz, ein Experten-Brainstorming-Team und die Interaktion mit Verwaltungsmitarbeitern wurden eingesetzt, um eine Reihe konstruktiver Vorschläge für den Einsatz von KI in Parlamenten zu sammeln und ihre Relevanz sowie Priorität im griechischen Parlament bewerten zu lassen. Durch dieses innovative Verfahren kann eine bestehende Forschungslücke konkret für Griechenland geschlossen und zugleich darauf hingewiesen werden, wo dringend KI-basierte Innovationen initiiert werden müssen, um effizientere parlamentarische Institutionen zu schaffen.

Dieser Ansatz bietet auch eine gute Grundlage für die Erstellung einer Forschungsagenda zu KI in Parlamenten. Der Workshop hat gezeigt, dass die 210 Vorschläge ein breites Spektrum an relevanten Themen abdecken. Angesichts des gewählten Verfahrens muss kritisch hinterfragt werden, ob drei Experten für ein Brainstorming ausreichend sind oder andere Experten nicht zu anderen Vorschlägen und alternativen Bewertungen zu anderen Zeitpunkten kommen würden. Überraschenderweise gibt es bei der Betrachtung der Ergebnisse keine niedrig bewerteten Vorschläge, obwohl es keine Aussortierung der Beiträge gegeben hat. Die Bewertungen werden sich sicherlich im Laufe der Zeit und von Institution zu Institution ändern, auch unter Berücksichtigung des technologischen Fortschritts von generativen Pretrained Transformer-Modellen (GPT-X & Co) [HZ21].

Dies zeigt sich etwa anhand einer weiteren kleinen Umfrage des Teams, die im Januar und Februar 2023 im Umfeld des griechischen Parlaments zu ChatGPT durchgeführt wurde. Ausgehend von der 210er-Liste des Brainstormings [LF23] wurden die 12 Teilnehmer (n=12) gefragt, ob ChatGPT jeden dieser 210 Vorschläge verändern würde („Does ChatGPT affects the solution?“). Die Antwortmöglichkeiten wurden bewusst binär und damit begrenzt gehalten: Ja/Nein (Yes/No; 1/0)). Nicht die Form und Wirkkraft der neuen Möglichkeiten sind entscheidend, sondern nur die Relevanz von Chat-GPT für den jeweiligen Vorschlag sollten untersucht werden. Analysiert wurde so die durchschnittliche Verteilung der Bewertungen pro Vorschlag. 46 Vorschläge (21,9 %) liegen im obersten Viertel (definitiv Veränderungen zu erwarten: 0.76-1.00). 94 Vorschläge (44,8 %) finden sich im zweiten Viertel (wahrscheinlich Veränderungen zu erwarten: 0.51-0.75). 59 Vorschläge (28,1 %) liegen im dritten Viertel (kaum Veränderungen zu erwarten: 0.26-0.50) und 11 Vorschläge (5,2 %) im untersten Viertel (keine Veränderungen zu erwarten: 0.00-0.25). Kumuliert betrachtet werden 46 Vorschläge (21,9 %, oberstes Viertel) definitiv, 140 Vorschläge (66,7 %, oberste Hälfte) hoch wahrscheinlich sowie 199 Vorschläge (94,8 %, oberstes Drei-Viertel) durchaus von Veränderungen durch ChatGPT betroffen sein. Diese Verteilung zeigt, dass in den kommenden Jahren mit einer hohen Dynamik zu rechnen ist, insbesondere wenn weitere Fortschritte bei den Technologien, Ontologien und dem erlernten Wissen sowie den rechtlichen Fragen (Urheberrechte, Datenschutz) erzielt werden.

Die sich an diese Umfrage anschließende Diskussion drehte sich um konkrete Einsatzmöglichkeiten. Attraktive Anwendungsfelder für textgetriebene GPT-Modelle liegen

sicher in der Generierung von (Entwürfen für) Argumente, Reden, Präsentationen, parlamentarischen Anfragen und Antworten, Briefen, Emails, Agenden und Zusammenfassungen für die Abgeordneten. Solche Systeme können auch neuartige Denk- und Lösungsansätze in Gesetzgebungsverfahren einbringen, auf Unstimmigkeiten verweisen, Texte in einfach verständliche Sprache transformieren, Analysen und Übersetzungen übernehmen. Mit richtig gestellten Prompts, die manchmal auch mehrere Anläufe sowie einige Stunden zur Ideenfindung benötigen, werden sich gezielte Antworten erstellen lassen, die substanzielle Mehrwerte bieten, die aber auch rasch kopiert und verteilt werden können und die für viele Akteure eine erhebliche Erleichterung des Arbeitsalltags bedeuten. Aus diesen Gründen ist davon auszugehen, dass die Nachfrage nach Fortbildungsangeboten im Umgang mit GPT-Modellen in den kommenden Monaten zunehmen wird.

Unabhängig von diesen technischen Fortschritten, mit denen in den kommenden Jahren weiter zu rechnen ist, sind vom Team weitere Workshop-Runden zur Relevanz und Priorität der 210er-Liste mit anderen nationalen Parlamenten geplant. Einige Workshops haben bereits stattgefunden, etwa mit dem Parlament in Argentinien im August 2022 und Kanada im September 2023. Weitere Workshops sind in Vorbereitung. Die bisher gesammelten und noch detailliert zu analysierenden Ergebnisse weichen aber durchaus voneinander ab und belegen damit die Vermutung, dass es in unterschiedlichen Staaten zu divergierenden Bewertungen kommen kann. Dies gilt es in weitere Studien noch zu konkretisieren. Ein breiter intra- und transdisziplinärer Dialog muss auch mit den fortlaufenden Bemühungen zusammengebracht werden, Leitlinien für den Einsatz von KI in parlamentarischen Institutionen zu entwickeln und zu etablieren [FLM23].

Das Interesse am Einsatz von KI in der parlamentarischen Praxis ist groß. Es ist wichtig, dass sich Wissenschaft und parlamentarische Praxis auf den Weg gemacht haben bestehende Forschungslücken zu schließen. Diese Studie hat dazu beigetragen, das allgemeine Verständnis im Hinblick auf die disruptiven und vielleicht überwältigenden Veränderungen, die der jüngste Erfolg von GPT-X & Co. mit sich bringen könnte, zu konkretisieren. Es liegen nun mehrere Vorschläge auf dem Tisch, die teils den Erwartungen entsprechen, teils überraschend sind. Diese Ergebnisse aus dem griechischen Parlament sind möglicherweise nicht allgemein übertragbar. Mit Hilfe ähnlicher Workshops können Parlamente selbst herausfinden, ob, wo und welche KI-basierten Anwendungen relevant sind und Empfehlungen für die Politik und die parlamentarische Praxis ableiten.

Die von den Workshop-Teilnehmern als vorrangig eingestuften Vorschläge stellen die „Spitze des Eisbergs“ der KI-basierten Anwendungen und Dienste dar, die mit einer Vielzahl von Sektoren verbunden sind. Die relativen Unterschiede im Relevanzfaktor zwischen diesen Optionen sind gering. Für das griechische Parlament kann diese Auswahl möglicherweise erhebliche Auswirkungen haben. Bei der Aktualisierung des Strategieplans des Parlaments können etwa KI-basierte Tools und Dienste als Teil der strategischen Ziele und Entscheidungen des Parlaments in Betracht gezogen werden. Darüber hinaus wäre es bei der Planung der nächsten Generation von parlamentarischen IKT-Systemen notwendig neuartige KI-basierte Systeme und Verfahren zu berücksichtigen.

Der Workshop im griechischen Parlament wurde im März 2021 durchgeführt, mitten in der Pandemie, die zur Unterbrechung bestimmter parlamentarischer Prozesse und zur Beschleunigung der digitalen Transformation anderer Prozesse führte [FP21]. Zwangsläufig wurden die Umsetzung der Parlamentsstrategie sowie alle Maßnahmen zur Erstellung eines Folgeplans auf Eis gelegt. Obwohl nur eine der spezifizierten KI-basierten Lösungen direkt in den parlamentarischen Arbeitsbereich eingeführt wurde (siehe Abschnitt 6.1 über die Sprache-zu-Text-Anwendung für die halbautomatische Erstellung von Protokollen), gab es dennoch wesentliche Entwicklungen in Bezug auf die Zusammensetzung des IKT-Sektors und die Untersuchung der entsprechenden Rahmenbedingungen, die in den untersuchten Vorschlägen auf die wichtigsten offenen Fragen verwiesen werden (siehe Abschnitt 6.4). Was die erstere betrifft, so führte eine umfassende administrative Umstrukturierung zu einer neuen Führungsstruktur in der IT-Abteilung und der zuständigen Generaldirektion. Interessanterweise nahmen zwei der neuen Verwaltungsleiter an dem besagten Workshop teil und gewannen so wichtige Erkenntnisse, die in die Entwicklung neuer KI-basierter Lösungen einfließen können. Was den KI-Rahmen betrifft, so beteiligen sich parlamentarische Forscher des griechischen Parlaments derzeit an internationalen Netzwerken und Arbeitsgruppen zur Entwicklung ethischer und operativer Richtlinien.

In den kommenden Jahren wird die Praxis zeigen, welche dieser Ansätze an Bedeutung gewinnen und wie schnell sich das griechische Parlament mit ihnen auseinandersetzen wird. Sobald Lösungen verfügbar sind und sich in der Praxis bewähren, könnten viele andere Parlamente davon profitieren. Es muss jedoch politisch geklärt werden, ob dies im Sinne der nationalen digitalen Souveränität wünschenswert und technisch machbar ist. In Zeiten knapper Kassen könnte ein kollaborativer Ansatz zur Einführung von KI in den Parlamenten überzeugender sein, da die Last auf mehrere Schultern verteilt wird. Allerdings erfordert diese Option vertrauenswürdige Partner, die einen cloudbasierten Ansatz mit KI-Lösungen unterstützen und nicht wegen der Gefahr der Manipulation verteufeln.

Das neue Parlament, das aus den parlamentarischen Wahlen 2023 hervorgehen wird, hat die einmalige Gelegenheit, zum ersten Mal in der griechischen Geschichte die Regeln der Mensch-Maschine-Interaktion festzulegen. Obwohl KI-relevante Themen nicht Bestandteil der politischen Debatte waren, bleibt es abzuwarten, ob das künftige Parlament den Erwartungen der Gesellschaft standhalten und die digitale Transformation zu einem „Parlament der Zukunft“ konstruktiv fortsetzen wird.

Literaturverzeichnis

[AN23] Akoma Ntoso: http://www.akomantoso.org, Stand: 17.08.2023.

[CE21] Council of Europe: Artificial Intelligence, Human Rights, Democracy, And The Rule Of Law – A Primer, Council of Europe and The Alan Turing Institute, Strasbourg, 2021.

[Cl89] Clark, C.: Brainstorming - How to Create Successful Ideas, Wilshire Book Company,

Chatsworth, 1989.

[DA21] De Almeida, P.G.R: El camino hacia un parlamento inteligente – Cámara de Diputados de Brasil. In: Red Información, No 24, S. 4-12, Instituto Nacional Demócrata para Asuntos Internacionales, Bogotá, 2021. https://www.redinnovacion.org/revista/red-informaci%C3%B3n-edici%C3%B3n-n%C2%B0-24-marzo-2021, Stand 17.08.2023.

[ELS20] Etscheid, J, von Lucke, J., Stroh, F.: Künstliche Intelligenz in der öffentlichen Verwaltung, Digitalakademie@BW & Fraunhofer IAO, Stuttgart, S. 11-12, 2020.

[EP23] European Parliament: Proposal for a Regulation on a European Approach for Artificial Intelligence - Q2 2021, legislative train 06.2023, Stand: 17.08.2023. https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/a-europe-fit-for-the-digital-age/file/regulation-on-artificial-intelligence

[EPHA23] European Parliament: Historical Archives (2023). https://historicalarchives.europarl.europa.eu/home.html, Stand: 17.08.2023.

[Fi19] Fitsilis, F.: Imposing regulation on advanced algorithms. Springer, Cham, 2019.

[Fi21] Fitsilis, F.: Artificial Intelligence (AI) in Parliaments - Preliminary Analysis of the Eduskunta Experiment. The Journal of Legislative Studies, 27(4), S. 621-633, 2021.

[FKS22] Fitsilis, F., Koryzis, D., & Schefbeck, G.:. Legal informatics tools for evidence-based policy creation in parliaments. International Journal of Parliamentary Studies, 2(1), S. 5-29, 2022.

[FLM23] Fitsilis, F.; von Lucke, J.; Mikros, G. et al. Leitlinien zur Einführung und Nutzung von Künstlicher Intelligenz in der parlamentarischen Arbeit. Athen 2023. https://doi.org/10.6084/m9.figshare.22691665.v2, Stand: 17.08.2023.

[FP21] Fitsilis, F., & Pliakogianni, A.: The Hellenic Parliament's Response to the COVID-19 Pandemic: A Balancing Act between Necessity and Realism. In: IALS Student Law Review 8, S. 19-27, 2021.

[HP18] Hellenisches Parlament: Stratigikó Schédio 2018-2021, Athen, 2018.

[HZ21] Han, X., Zhang, Z. et al. (2021). Pre-trained models: Past, present and future. AI Open 2, S. 225-250. https://doi.org/10.1016/j.aiopen.2021.08.002, Stand: 17.08.2023.

[Ko21] Koryzis, D. et al: ParlTech: Transformation Framework for the Digital Parliament. Big Data and Cognitive Computing, 5(1), 15, S. 1-16, 2021.

[LF22] von Lucke, J., Fitsilis, F.: Using Artificial Intelligence for Legislation - Thinking About and Selecting Realistic Topics. In: Marijn Janssen et al (Hrsg.) EGOV-CeDEM-ePart 2022 - Proceedings of Ongoing Research, Practitioners, Workshops, Posters, and Projects of the International Conference EGOV-CeDEM-ePart 2022, S. 32-42, 2022.

[LF23] von Lucke, J., Fitsilis, F.: Research and Development Agenda for the Use of AI in Parliaments. In: David Duenas Cid et al. (Hrsg.): DGO '23: Proceedings of the 24th Annual International Conference on Digital Government Research, Association for Computing Machinery (ACM), New York, S. 423-433, 2023.

[LF23a] von Lucke, J., Fitsilis, F.: Using Artificial Intelligence in Parliament - The Hellenic Case. In: Ida Lindgren et al. (Hrsg.): EGOV 2023 Proceedings, Springer, LNCS 14130,

S. 174–191, 2023.

[Ma23] Maruri, K.: Lawmakers Experiment With ChatGPT to Write Bills, Governing, Folsum (2023), https://www.governing.com/next/lawmakers-experiment-with-chatgpt-to-write-bills, Stand: 17.08.2023.

[MN20] Misuraca, G., van Noordt, C.: Overview of the use and impact of AI in public services in the EU. Publications Office of the European Union, 2020.

[OAI23] Chat-GPT: https://chat.openai.com, Stand: 17.08.2023.

[OE23] Organisation for Economic Co-operation and Development: The OECD Global Parliamentary group on AI, https://oecd.ai/en/parliamentary-group-on-ai, Stand: 17.08.2023.

[PA20] Parliamentary Assembly of the Council of Europe (PACE): Artificial Intelligence: Ensuring respect for democracy, human rights and the rule of law, Strasbourg, 2020.

[Pa22] Palmirani, M. et al. Legal Drafting in the Era of Artificial Intelligence and Digitisation. European Commission, Brüssel 2022.

[PL22] Palmirani, M., & Liga, D.: Derogations Analysis of European Legislation Through Hybrid AI Approach. In: International Conference on Electronic Government and the Information Systems Perspective, S. 123-137, Springer, Cham, 2022.

[Rö98] Röthig, P.: Handbuch für Organisationsuntersuchungen in der Bundesverwaltung, 5. Auflage, Bundesministerium des Innern, Bonn, S. 31, 1998.

[Si21] Silva N.F.F. et al.: Evaluating Topic Models in Portuguese Political Comments About Bills from Brazil's Chamber of Deputies. In: Proceedings on Intelligent Systems BRACIS 2021, S. 104-120, Springer, Cham, 2021.

[So21] Souza, E. et al: An Information Retrieval Pipeline for Legislative Documents from the Brazilian Chamber of Deputies. In: Legal Knowledge and Information Systems, 346, S. 119-126, IOS Press, Clifton, 2021.

[SU21] Stanford University: Artificial Intelligence Index Report 2021, Stanford, 2021.

[XL23] Xleap: https://www.xleap.net. Stand: 17.08.2023.

Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
144 Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023

Der Einsatz von Neural Language Models für eine barrierefreie Verwaltungskommunikation

Anforderungen an die automatisierte Vereinfachung rechtlicher Informationstexte

Michael Gille [1], Thorben Schomacker[2], Jörg von der Hülls[3], Marina Tropmann-Frick[4 5 6]

Abstract: Machine-learning-based text simplification can be used to meet legal obligations to provide comprehensibility-enhanced public service texts. The article examines the use of artificial intelligence for public administration communication in rule-based easy language. The authors outline essential technical, legal and normative requirements for the development and use of automated text simplification through neural language generation. As part of the Open-LS research project, a contribution is made to clarifying the possibilities and limits of the use of artificial intelligence systems for text simplification in public services.

Keywords: Text simplification, Transformer, AI Regulation, Leichte Sprache, DIN SPEC 33429

1 Einleitung

Das Textverständnis kognitiv und lernbeeinträchtigter Menschen [7] wird durch Übertragungen in verständlichkeitsoptimierte Sprache unterstützt, gerade auch um Inklusion und soziale Teilhabe zu fördern [Bund08]. Bislang überführen menschliche Übersetzer Texte in vereinfachte Versionen. Die Umwandlung von Informations- und

[1] michael.gille@haw-hamburg.de, https://orcid.org/0000-0001-9978-0817
[2] thorben.schomacker@haw-hamburg.de, https://orcid.org/0009-0002-3577-341X
[3] joerg.vonderhuells@haw-hamburg.de
[4]marina.tropmann-frick@haw-hamburg.de, https://orcid.org/0000-0003-1623-5309
[5] Alle Autoren sind tätig an der Hochschule für Angewandte Wissenschaften Hamburg (HAW Hamburg), Berliner Tor 5, 20099 Hamburg, Deutschland.
[6] Diese Arbeit wird gefördert durch UpdateHamburg (Schomacker) und durch Hamburg Call for Transfer (von der Hülls). Das Projektteam dankt der Hamburgischen Investitions- und Förderbank für die Projektförderung des Projekts Open-LS im Rahmen des Programms PROFI Impuls. Wir danken zudem den anonymen Gutachtern für ihr wertvolles Feedback.
[7] Während in der Gesetzgebung von „*Menschen mit geistigen Behinderungen und Menschen mit seelischen Behinderungen*“ (§ 11 (1) Satz 1 BGG) die Rede ist, wird im Rahmen dieses Beitrags von kognitiv und lernbeeinträchtigten Menschen oder, in Übereinstimmung mit DIN SPEC 33429-E [Dinn23] , die Bezeichnung „*Menschen mit Lernschwierigkeiten*“ verwendet. Der gesetzliche Begriff wird teilweise als (zu) defizitorientiert und diskriminierend empfunden.

doi:10.18420/rvi2023-013

Kommunikationstexten in eine barrierefreie Sprachfassung insbesondere nach § 11 Behindertengleichstellungsgesetz (BGG) [KoVM23] sind mit Kosten für den öffentlichen Haushalt verbunden. Zwar sind seit der Einführung gesetzlicher Vorschriften zur Barrierefreiheit vor über zwanzig Jahren erhebliche Fortschritte zu verzeichnen, jedoch bleibt die Umsetzung lückenhaft [Thap21, AsHZ23, Bund21. Ahle23], obwohl bis zu 12 % der Bevölkerung Deutschlands Schwierigkeiten haben, Standardsprache zu verstehen und zu verwenden [GrBu20]. Automatisierte Ansätze, die auf Techniken des maschinellen Lernens basieren, können helfen, die Kosten der Textvereinfachung zu senken [GrBu20, Gugg19]. Anders als Chatbots und ähnliche Dialogsysteme, die Unterhaltungen simulieren, geht es bei der Textvereinfachung um Übersetzungen in barrierefreie Sprache, nicht unähnlich einer Übersetzungsleistung in eine andere Sprache. Der Einsatz von Künstlicher Intelligenz (KI)[8] kann die Effizienz der Verwaltung steigern und sogar individuelle Kommunikationslösungen ermöglichen [Gugg19, Deut22]. Das vergleichsweise neue Forschungsfeld der automatisierten Textvereinfachung (Text Simplification, TS) greift auf KI in Gestalt neuronaler Sprachmodelle (Neural Language Models, NLM) zurück, um Texte in komplexitätsreduzierte Fassungen zu übertragen. Vortrainierte Sprachmodelle erlernen die Vereinfachungsaufgaben maschinell anhand großer Mengen spezieller Trainingsdaten insbesondere in Gestalt paralleler Korpora, wobei es bislang kaum geeignete deutschsprachige Datensätze gibt [Stod22].

Der Beitrag untersucht technische, regulatorische und normative Rahmenanforderungen des Einsatzes machine-learning-basierter Anwendungen zur Textvereinfachung für den verständlichkeitsoptimierten behördlichen Kontakt mit Personen, die auf barrierefreie Text- und Kommunikationsformen angewiesen sind. Hintergrund ist das interdisziplinäre Forschungsprojekt Open LS. Mit Methoden der Computerlinguistik wird ein textvereinfachendes NLM für Textformate entwickelt, das auf Personen mit Lernschwierigkeiten zugeschnitten und gezielt für die Übertragung von Rechtstexten trainiert wird, um deren Verständlichkeit für diesen Adressatenkreis zu verbessern. Nachfolgend werden spezifische Anforderungen an textvereinfachende KI-Systeme für die Erstellung barrierefreier rechtlicher Informationstexte der öffentlichen Verwaltung betrachtet und erste Ergebnisse aus dem Projekt (Open-LS) vorgestellt. Zunächst werden der Soll-Output sowie die technischen Modellmerkmale der Neural Language Generation (NLG) beim Einsatz für die Textvereinfachungsaufgabe umrissen und wesentliche Schritte des Trainings beschrieben (Abschnitt 2). Anschließend wird der rechtlich-normative Rahmen auf Anforderungen für Modell und Betrieb hin untersucht (Abschnitt 3) und Modellanforderungen abgeleitet (Abschnitt 4). Der Beitrag schließt mit einem Ausblick einschließlich Angaben zu Limitationen und Forschungslücken (Abschnitt 5).

[8] „KI“ meint eine Maschine, welche dazu gebracht wird, sich so zu verhalten, wie man es bei einem Menschen als intelligent bezeichnen würde (gemäß der Definition in [MMRS55]). Dem Begriff „KI-System“ liegt im Folgenden die Definition aus Art. 3 Nr. 1 KI-VO (Entwurf der EU-Kommission v. 21.4.2021) zugrunde.

2 Automatische Vereinfachung rechtlicher Informationstexte durch Neural Language Generation

2.1 Leichte-Sprache-Text als Output der Vereinfachung

Ein Text gilt gemäß § 4 BITV 2.0 als barrierefrei, wenn er in "Leichter Sprache" formuliert ist. Unter Leichter Sprache (LS) wird eine verständlichkeitsoptimierte und regelbasierte Kunstform des Deutschen verstanden, nicht zu verwechseln mit "Einfacher Sprache", womit vereinfachte Varianten im Graubereich zwischen Standardsprache und LS bezeichnet werden [Maaß20]. Existierende Sprachmodelle wie ChatGPT wurden überwiegend auf Alltags- und Standardsprache trainiert. LS unterscheidet sich von Alltagssprache, die mit geringen regionalen Abweichungen von der Mehrheit der Bevölkerung deutschsprachiger Länder verwendet wird. Derzeit übersetzen spezialisierte menschliche Übersetzer standardsprachliche Texte in Leichte Sprache, wobei juristische Texte aufgrund ihres fachsprachlichen Charakters und ihres normativen Inhalts eine besondere Herausforderung darstellen [GaGe22].

Rechtliche Texte weisen in den verschiedenen Rechtsgebieten ähnliche sprachliche Merkmale auf, wie z.B. die Verwendung juristischer Fachsprache, Formalisierung, lange und komplexe Sätze, ein hohes Maß an Intertextualität, häufig gemischte Autorenschaft, ein breites Spektrum von Adressaten und ein fachspezifisches Spannungsverhältnis zwischen Genauigkeit der Formulierungen und begrifflicher Vagheit [Baum20]. Darüber hinaus sind viele Rechtstexte funktional auf Rechtsverbindlichkeit angelegt und begründen Rechte und Pflichten. In der Begründung, Organisation und Kommunikation rechtlicher Beziehungen unterscheiden sich diese Texte grundlegend von Texten, die Gegenstand der meisten zum NLM-Training genutzten intra- und monolingualen Korpora sind.

Die Vereinheitlichung von Leichte-Sprache-Regeln ist auch im Hinblick auf die barrierefreie Kommunikation durch die öffentliche Hand relevant. Die Empfehlungen des Standards des Deutschen Instituts für Normung, DIN SPEC 33429 (Entwurf), richten sich an den gesamten Personenkreis der an der Erstellung von Texten in LS Beteiligten einschließlich Auftraggebern, wobei diese Regeln auch bei Ausschreibungen sowie bei der Qualitätssicherung herangezogen werden können [Dinn23]. Dieses Regelwerk wird hier aufgrund der absehbaren Maßgeblichkeit für Übersetzungen in LS bei der Formulierung von Anforderungen an Output-Texte zugrunde gelegt.

2.2 Neural Language Models

Spezialisierte Modelle wie Neuronale Netze für die Sprachverarbeitung und -modellierung (= NLM) werden ständig weiterentwickelt. Die Grundlage für das Gelingen jedes Vorhabens mit neuronalen Netzen sind Daten. Die Verarbeitung von Sprachdaten

durch NLM beginnt zunächst mit Tokenisierung. Hier wird anfänglich der Text in linguistische Bausteine (wie beispielsweise Wörter) unterteilt. Diese Bausteine bilden dann semantische Einheiten, die sog. Token. Z.B. ist der Token „Ludwig XIV." aus zwei Wörtern zu einer semantischen Einheit zusammengefasst worden. Im nächsten Schritt, dem Embedding, werden die Token in eine verteilte mathematische Repräsentation (Vektor) transformiert. Dadurch können semantische Beziehungen durch die Verteilung im Vektorraum dargestellt werden [TuWW22].

Im Bereich des NLP gibt es zwar textuelle Daten in großer Zahl, gleichwohl mangelt es für viele Anwendungen an task-spezifischen, aufbereiteten Daten [ScTr21], um NLMs ausreichend zu trainieren. Diese Schwierigkeit kann durch Transferlernen bewältigt werden. Transferlernen ermöglicht es, aus Daten, die nicht speziell für den Task aufbereitet wurden, Wissen abzuleiten und dieses später für spezifische Tasks abzurufen. Die wohl weitverbreitetste Architektur für Transferlernen ist die Transformer Architektur [VSPU17]. Diese Architektur ermöglicht, das Anlernen des NLM in zwei Schritte aufzuteilen: 1) Vortrainieren auf nicht aufbereiteten Rohtexten, wodurch dem Modell ein generelles Welt- und Sprachverständnis beigebracht wird. 2) task-spezifisches Fine-Tuning, beispielsweise Textklassifikation oder Übersetzen. Auch wenige task-spezifische Datenpunkte können reichen, da das Modell bereits Sprachverständnis durch Vortrainieren aufweist. [TuWW22] Dadurch können task-spezifische Daten präziser für das Lernen von task-spezifischem Verständnis verwendet werden und müssen kein grundlegendes Sprachverständnis mehr schaffen [RSRL20].

Ein klassischer Transformer besteht aus zwei Komponenten: 1) Der Encoder extrahiert Eigenschaften aus dem Input und speichert in einer verteilten Repräsentation (wie bspw. Vektoren) den Kontext. 2) Der Encoder verarbeitet sequenziell den Kontext zu einem task-spezifischen Ergebnis. Seit ihrer Einführung haben sich drei Stränge der Transformer Architektur herausgebildet [TuWW22, S.78–84]: 1) **Encoder-Only** Modelle eignen sich vor allem für NLU-tasks (Natural Language Understanding) wie zum Beispiel Klassifikation, Eigennamenerkennung oder das Beantworten von Fragen. 2) **Decoder-Only** sind vergleichsweise gut darin, das nächste Wort vorherzusagen. Daher werden sie häufig für Textgenerierung (= Natural Language Generation (NLG)) eingesetzt. Die bekanntesten Vertreter sind die Modelle aus der GPT-Familie. 3) **Encoder-Decoder Modelle** kombinieren die Eigenschaften dieser beiden Stränge. Sie funktionieren sowohl für NLU als auch für NLG-tasks. Für Textvereinfachung können also Encoder-Decoder und Encoder-Only Transformer eingesetzt werden, da es sich um einen NLG-task handelt.

2.3 Automatische Textvereinfachung

Bisherige Ansätze für deutschsprachige Textvereinfachung basieren auf parallelen Datensätzen (Standardsprache → Vereinfachung). Anfänglich wurde mit statistischen Regeln gearbeitet [SuEV16]. Ab 2020 wurden zunehmend NLMs zur Textvereinfachung eingesetzt [SäEV20, RSKK21, SpRE21, EBKP22, StMK23]. Diese Ansätze greifen auf

Encoder-Decoder Transformer Modelle zurück. Mittlerweile wurden Decoder-Only Transformer Ansätze vorgestellt [AOWJ23, DGLM23], welche auch nur mit monolingualen Daten (Einfache Sprache/LS) trainiert werden können. Einen ersten vollständigen Überblick über wissenschaftlich veröffentlichten deutschen Textvereinfachungsdatensätze sowie über KI-gestützte Ansätze zur automatischen Textvereinfachung liefern Stodden et. al. [StMK23] sowie Schomacker et. al. [SGMH23]. Da nach wie vor Encoder-Decoder Transformer Ansätze vielversprechendere Ergebnisse liefern [AlIn23, AOWJ23, DGLM23] wird hier ein Encoder-Decoder Ansatz zugrunde gelegt.

Für die Evaluation automatisch-generierter Textvereinfachung werden in der Regel automatische Verfahren eingesetzt. Evaluation durch Menschen oder Expert*innen sind selten [GrSa22]. Häufig werden statistische Metriken, welche für die Auswertung interlingualer Übersetzungen entwickelt wurden, verwendet [GrSa22]. Prominente Vertreter sind BLEU [PRWZ02] und ROUGE [Lin04]. Beide basieren auf dem Vergleichen von einzelnen Worten oder Wortketten (N-Grams) der generierten Übersetzung und einer vorher ausgewählten richtigen Lösung. Es existieren auch Metriken, wie SARI [XNPC16], die speziell für Textvereinfachungen entwickelt wurden und neben der Ähnlichkeit mit einer richtigen Lösung u.a. auch die Komplexität des Textes messen.

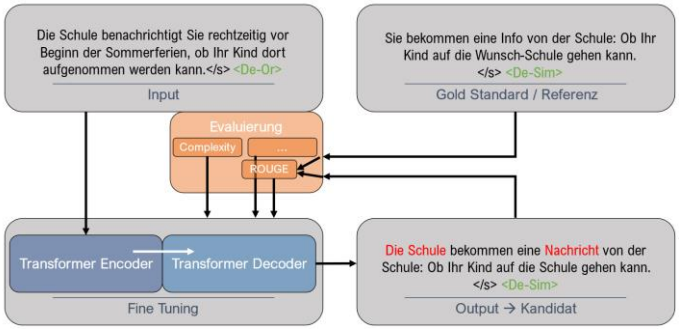

Abb. 1: Schematische Abbildung des Fine-Tuning eines vortrainierten Encoder-Decoder Transformers (z. B. mBART [LGGL20]) für Textvereinfachung. In Rot sind die fehlerhaften Stellen markiert. Die (html-artigen) grünen Anmerkungen markieren die Sprachvariante <De-Or> für Standarddeutsch und <De-Sim> für LS.

3 Rechtlicher und normativer Rahmen für automatisierte Textvereinfachung

Die Betrachtung des Rechtsrahmens für den verwaltungsseitigen Einsatz NLP-basierter Anwendungen zur automatisierten Sprachvereinfachung zielt auf die Identifikation von Modell- und Prozessanforderungen ab. Ihr liegt die Unterscheidung zwischen Anforderungen an das verwaltungsseitig bereitzustellende Textangebot in LS und betreiber- bzw. anbieterbezogenen Anforderungen.

3.1 Automatisierte behördliches Kommunikationsangebot in Leichter Sprache

Anforderungen an Texte juristischen Inhalts in LS zur behördlichen Kommunikation und Interaktion ergeben sich aus der UN Behindertenrechtskonvention, [Bund08] dem BGG, der BITV 2.0 sowie dem Onlinezugangsgesetz (OZG) [KoVM23] auf Grundlage der EU-Richtlinie zur Regelung des barrierefreien Zugangs zu Websites und mobilen Anwendungen öffentlicher Stellen [Dase16]. Bei den durch DIN SPEC 33429-E [Dinn23] noch einmal stärker kanonisierten Leichte-Sprache-Standards handelt es sich um *Soft Law*, das auf freiwillige Anwendung ausgerichtet ist. Durch Bezugnahme in Ausschreibungen und Verträgen wird dieser neue Standard bei Auftragsverhältnissen leistungs- und qualitätskonkretisierend für Dienstleistende verbindlich. Der Standard wurde vom Bundesministerium für Arbeit und Soziales initiiert und zielt als Standardisierungsvorhaben gerade auf die BITV 2.0 ab [Dind22]. Der neue Standard wird, ähnlich DIN EN 301 549, nach § 3 BITV 2.0 bei der öffentlichen Beschaffung zugrunde gelegt werden.

Die Anwendbarkeit automatisierter Textvereinfachung kann grundsätzlich nicht zu Verwaltungshandeln mit Regelungsgehalt führen, was die Bandbreite möglicher Textfunktionen des Ziel-Outputs einschränkt. Zwar können nach § 35a VwVfG (§ 155 (4) AO, § 31a SGB X) Verwaltungsakte vollautomatisiert erlassen werden, wenn kein Beurteilungsspielraum vorliegt und auch keine Ermessensentscheidung zu treffen ist. Nach § 24 (1) S 3 VwVfG muss die Behörde bei Einsatz „*automatische[r] Einrichtungen zum Erlass von Verwaltungsakten*“ gleichwohl eine individuelle Sachverhaltsaufklärung betreiben. In jedem Fall unterliegt der Einsatz selbstlernender Algorithmen bei verwaltungsrechtlichen Entscheidungen einem gesetzlichen Erlaubnisvorbehalt [Gugg19]. In Anbetracht der Risiken für die häufig besonders vulnerablen Adressaten von LS gilt dies erst recht. Mangels Rechtsgrundlage muss sich die automatisierte Textvereinfachung auf Grundlage des DIN Standards hinsichtlich ihrer Funktion auf Informations- und Kommunikationstexte beschränken, bei denen es sich um “v*ollständig automatisiertes Realhandeln*" handelt [ScSH22]. Für diese Textfunktionen greifen der risikoorientierte Haftungsrahmen (Abschn. 3.2) sowie die daraus ableitbaren Anforderungen (Abschn. 4).

3.2 Risiko- und Haftungsregeln für Betreiber NLG-basierter Anwendungen

Eine vertragliche oder außervertragliche Haftung des Betreibers oder Anbieters setzt eine Verletzung von Sorgfaltspflichten oder bei entsprechender gesetzlicher Haftungserweiterung die Erfüllung eines Gefährdungstatbestandes voraus. Die Grundzüge des risikobasierten Ansatzes der EU sind ausbuchstabiert und von den Mitgliedstaaten konsentiert [Cham23, Fino23, Hack23]. Erster Anknüpfungspunkt ist das „klassische" deliktische Haftungsrecht, für das vor allem die Frage des Sorgfaltsmaßstabs sowie die Beweislastverteilung diskutiert werden. Hier ist die EU zudem mit dem Entwurf zweier KI-(Produkt)Haftungsrichtlinien [Bund22, BoSi22, Mayr23, Hack23] aktiv geworden. Der Ansatz beschränkt sich im Wesentlichen auf die EU-weite Harmonisierung von Beweiserleichterungen (Auskunftsansprüche sowie widerlegbare Vermutungen bzgl. Sorgfaltspflichtverletzungen und Ursächlichkeit für einen Schadenseintritt, Art. 3f. KI-Haftungsrichtlinie) im Rahmen des in den Mitgliedstaaten geltenden Haftungsrechts, allerdings bezogen auf sämtliche zivilrechtlichen Schadensersatzansprüche einschließlich deutscher Amtshaftungsansprüche [Stau23].

Sorgfaltspflichten des Betreibers bzw. Anbieters können verletzt sein, wenn das KI-System den technischen Standards nicht entspricht, wenn Programmier-, Trainings- oder Überwachungsfehler vorliegen. Die u.a. im Kontext des Produktsicherheitsrechts entwickelten Haftungsgrundsätze gelten gleichermaßen für digitale Produkte. [MüWa20] Obgleich DIN-Normen als *Soft Law* mangels Allgemeinverbindlichkeit keine umsetzungspflichtigen Rechtsvorschriften sind, besteht eine Pflicht zur Beachtung des Norminhalts bei der Beurteilung von Konformität und Risiken [Wilr23]. Haftungsrechtlich führt die Nichteinhaltung von DIN-Normen regelmäßig zu einer Sorgfaltspflichtverletzung, auch wenn eine Haftung vom Vorliegen weiterer Voraussetzungen abhängt [MüWa20]. Umgekehrt kommt der Hersteller bzw. Betreiber einer KI bei Einhaltung der Norm in den Genuss einer „*administrativen Konformitätsvermutung*" [Wilr23], ohne automatisch von einer Haftung befreit zu sein. [MüWa20].

Das Risiko von schadensbegründenden fehlerhaften Outputs eines autonomen KI-Systems wird rechtlich vor allem als Autonomie- und Opazitätsrisiko im Rahmen der Betreiberhaftung diskutiert [Burc22]. Mögliche Szenarien in Bezug auf textvereinfachende Algorithmen wären bspw. unzutreffende, lückenhafte, missverständliche oder unverständliche Textübertragungen, die zu einer Nichtgeltendmachung von Ansprüchen führen könnten. Schwierigkeiten bereitet bei autonomen Systemen zudem die Abgrenzung zwischen der Verwirklichung von Opazitätsrisiken und Sorgfaltspflichtverletzungen des Geschädigten oder eines Dritten. Autonomierisiken sind jedenfalls dann nicht verwirklicht, wenn eine menschliche Sorgfaltspflichtverletzung schadensursächlich geworden ist, etwa bei falscher Nutzung, fehlerhafter Programmierung, unzureichendem Training oder fehlender Überwachung [Burc22]. Bei reinen Textübersetzungen wird dies i.d.R. klar zuordenbar sein. Bei

Verständnis- und Interpretationsfehlern kann die Risikoallokation oft nicht eindeutig erfolgen, v.a. dann nicht, wenn die Vulnerabilität der Adressaten von LS berücksichtigt werden muss [Fior21].

Weiterer rechtlicher Anknüpfungspunkt ist die Anwendung von Gefährdungshaftungstatbeständen, wie sie die EU Kommission für die Produkthaftung sowie in der (Entwurfsfassung der) sog. KI Verordnung vorgestellt hat [KGAK23, Wend22]. Bei der Gefährdungshaftung entfällt das Erfordernis einer Sorgfaltspflichtverletzung. Bereits der bloße Betrieb einer Gefahrenquelle (= KI-System) führt – unabhängig von Vorsatz oder Fahrlässigkeit – bei einem verursachten Schaden zu einer Haftung. Durch die Neuregelungen wird auch mit einflussreichen Vorgaben für den Einsatz von KI-Systemen durch die öffentliche Hand gerechnet. [ScSH22] Der risikobezogene Ansatz der KI-VO-E drückt sich in der Unterscheidung von verbotenen Praktiken, Hochrisiko-KI-Systemen, Systemen mit begrenztem Risiko sowie KI-Systeme mit geringem Risiko aus.

Für den Einsatz von Textvereinfachungssystemen zu Kommunikations- und Informationszwecken (Textfunktion) ist im Regelfall nicht davon auszugehen, dass es sich um ein Hochrisiko-KI-System handelt, obwohl sich der Adressatenkreis aus vulnerablen Personen zusammensetzt. Es fehlt, jedenfalls bei einer reinen Übersetzung zu Informationszwecken, in aller Regel an einem einschlägigen Hochrisiko-Einsatzbereich nach Anhang III zu Art. 6 (2) KI-VO-E. Somit wäre eine Textübersetzungs-KI als System mit begrenztem oder geringem Risiko einzustufen. Für Systeme mit begrenztem Risiko sollen künftig die Transparenzpflichten sowie weitere Anforderungen gelten (s. Abschn. 4). Diese Regeln greifen auf Überlegungen zur sogenannten *Responsible AI* [GöTB23] in Übereinstimmung mit den Ethikleitlinien der Hochrangigen Expertengruppe für KI zurück [Euro22]. Der umfassende risikozentrierte und differenzierende Ansatz der EU für KI-Systembetreiber und -anbieter resultiert in konkreten Anforderungen, die zudem dynamisch mit dem jeweiligen Stand der Technik anzupassen sind [Cham23]. Der geplante EU-Haftungsrahmen für KI-Systeme basiert dabei auf planvoller Risikobewertung und damit auf einem im Kern nicht-rechtlichen Konzept. Aus der Sicht der Institutionentheorie sind die Risiken transformierte Unsicherheiten, die ein aktuarisches Management in Gestalt von Versicherungen ermöglichen [Nort90]. Das Haftungsrecht schafft folglich negative Anreize durch die Definition von Haftungsrisiken, die Betreiber und Anbieter von KI-Systemen anstreben zu minimieren und zu versichern [LiFH22, Schu23]. Im folgenden Abschnitt werden die daraus ableitbaren Anforderungen weiter konkretisiert.

4 Ableitung von Anforderungen an eine rechts- und standardkonforme Textvereinfachung

Automatische Textvereinfachung, vor allem mittels eines Encoder-Decoder Ansatzes, bedarf paralleler hochqualitativer Daten. [HGNM20, DGLM23] bemängeln, dass die bisherige (Trainings-)Datengrundlage in zu geringem Maße die Regeln der LS umsetzt. Auf Basis von DIN SPEC 33429 kann ein LS-Framework sowohl für die Datenannotation als auch die Evaluation von KI-Modellen entwickelt werden. Die Analyse von DIN SPEC 33429-E hat einen vorläufigen Katalog mit 54 Anforderungen an eine standardkonforme Textvereinfachung ergeben. DIN SPEC 33429-E liefert Empfehlungen für die Umsetzung von LS. Da ein rein textbasierter Datensatz das Ziel ist, sind nur die sprachlichen Empfehlungen (Kap. 5) relevant. Es wurden alle Unterkapitel betrachtet und Anforderungen abgeleitet. Zu einigen Unterkapiteln wurde mehr als eine Anforderung definiert. Durch diesen Detailgrad wird die Zuweisung einer Überprüfungsmöglichkeit vereinfacht und transparent. Die Zuweisungen (pro Anforderungen eine Überprüfungsmöglichkeit) wurde zunächst durch einen in Computerlinguistik-erfahrenen Informatiker geprüft, für welche der Anforderungen eine automatisierte Form der Auswertung, durch beispielsweise LanguageTool-Regeln für LS, umsetzbar sind. Für die nicht-automatisierbaren Anforderungen, wurden zwei, in LS-geschulte Experten konsultiert, ob diese Anforderungen selbständig oder partizipativ [9] überprüft werden können. Dadurch ergeben sich drei Kategorien für die Auswertungsform: 1) AUTOMATISCH, 2) EXPERTE, und 3) PARTIZIPATION. Wir geben eine konkrete Umsetzungsmethode an, wie beispielsweise eine Skala; zudem werden qualitative und partizipationsbezogene Evaluationskriterien abgeleitet. Eine aktuelle Fassung des Katalogs ist auf der Open-LS Projektseite zu finden.[10]

Eine Untersuchung des geplanten Rechtsrahmens ergibt weitere Modellanforderungen. Das KI-System muss gem. Art. 52 KI-VO-E so konzipiert sein, dass die Nutzer über die automatisierte Texterstellung informiert sind, soweit dies nicht aufgrund der Umstände erkennbar ist. Da der maschinell vereinfachte Text nicht durch eine Prüfgruppe i.S.v. DIN SPEC 33429 geprüft wurde, wäre wohl auch hierauf hinzuweisen. Des Weiteren sind gem. Art. 69 KI-VO-E i.V.m. Art. 8-15 KI-VO-E weitere Gesichtspunkte im Rahmen der Selbstregulierung zu beachten: Daten (Training, Validierung, Testung von Datensets) und Daten-Governance sind an detaillierten Designanforderungen das Training und die Evaluation betreffend zu orientieren (Art. 10 (2)-(4)). Besonders Augenmerk legt der Verordnungsentwurf auf Verzerrungen (*Bias*). Da in dem hier verfolgten Ansatz ungeachtet der Heterogenität der Zielgruppe ein grds. einheitlicher Regelkatalog betrachtet wird, kommt der Abmilderung dieses Homogenitätsbias im Rahmen der Data Governance eine Schlüsselrolle zu.

[9] Partizipativ meint, gemäß DIN SPEC 33429-E, durch eine Prüfgruppe aus der Zielgruppe für LS
[10] https://open-ls.entavis.com/dinspec33429anforderungen/

Vor Inbetriebnahme müssen die technische Dokumentation (Art. 11 i.V.m. Annex IV) geplant sowie Aufzeichnungen (Art. 12) ermöglicht sein. Diese Vorgaben sind auch im Hinblick, auf die in Abschnitt 3.2 genannten (widerleglichen) gesetzlichen Vermutungsregeln (Sorgfaltspflichten, Ursächlichkeit) und Beweislastverteilungen sowie zur Verringerung von Opazitätsrisiken auch im Zusammenhang mit Auskunftsansprüchen sinnvoll. Weiteren Anforderungen folgen aus Art. 13-15. Ein Risikomanagementsystem (Art. 9), wohl gerade auch mit Fokus auf die Vulnerabilität der Übersetzungsadressaten und der Möglichkeit eines *Unfair Bias*, ist einzurichten. Es liegt grds. in der Verantwortung des KI-Anbieters, auf welchem technischen Weg die jeweilige Anforderung umgesetzt wird. Der Stand der Technik wird dabei in jedem Fall zu berücksichtigen sein, wozu auch DIN EN 15038 (Übersetzungen), DIN EN 15838 (Kundenkontaktzentren), EN 301 549 (EU-Konformität digitaler Objekte zur Barrierefreiheit von IKT) gehören.

5 Zusammenfassung, Limitationen und Ausblick

LS Texte als Output automatisierter Textvereinfachung durch NLM müssen vielfältigen Anforderungen genügen. Neben den skizzierten Anforderungen für Encoder-Decoder-Modelle ist die Qualität der Trainingsdaten zentral, auch aufgrund gesetzlicher Vorgaben. Für die Vereinfachung rechtlicher Texte bedarf es paralleler, regelkonform annotierter Korpora. Regeln für den Vereinfachungsoutput müssen bei behördlichen Informations- und Kommunikationstexten zwischen output-bezogenen und betreiberbezogenen Anforderungen unterscheiden. Erstere legen nahe, der Annotation und Evaluation die einschlägige DIN-Vorschrift zugrunde zu legen, was an einer entsprechenden Auswertung des Entwurfs von DIN SPEC 33429 illustriert wurde. Betreiber müssen sich an dem risikobasierten Haftungsrahmen orientieren, mit je nach Einsatzgebiet unterschiedlichen Risikokategorien und Vorgaben der KI Verordnung.

Dem Beitrag liegt der aktuelle Stand der Technik mit Bezug zur deutschsprachigen Textvereinfachung zugrunde. Es wurden NLM zur Vereinfachung deutscher Texte und ihre Eignung zur Übertragung juristischer Texte sowie die einschlägigen Anforderungen der Barrierefreiheit untersucht. Die allgemeine Methodik dieser Arbeit ist im Grundsatz für Textvereinfachungen für jede Domäne und jede Sprache anwendbar. Für andere Sprachen als Deutsch können keine allgemeingültigen Schlussfolgerungen getroffen werden. Diese Arbeit stützt sich auf die aktuelle Entwurfsfassung einer DIN-Norm, die endgültige Fassung und ihre Implikationen können davon abweichen. Gleiches gilt für den Rechtsrahmen der EU. Außerdem basiert die DIN-Norm auf Annahmen über ihre Adressaten, die eine Homogenitätsverzerrung hinsichtlich der demgegenüber heterogenen Zielgruppe mit Lernschwierigkeiten beinhaltet. Eine weitere Einschränkung bilden funktionale Verwendungsbeschränkungen auf reine Informationstexte sowie die Übertragung von Texten mit anderen Textfunktionen in reine Informationstexte, d.h., dass die Ziel-Textfunktion auf Informationsfunktionen beschränkt ist.

Im Rahmen des Open-LS Projekts werden weitere Forschungslücken adressiert:

1. Aufbau eines anforderungskonformen Trainingsdatensets für rechtliche Texte;
2. Anforderungskonforme Entwicklung, Training und Evaluation eines NLM;
3. Erforschung kosteneffizienter Möglichkeiten, um die Daten mit zielgruppenspezifischen KI-generierten Illustrationen zu ergänzen;
4. Untersuchung der Übertragbarkeit des Modells auf Domänen und Unterdomänen (z.B. juristische Unterdomänen), für die es nicht trainiert wurde;
5. Methodische Weiterentwicklung geeigneter normkonformer Evaluationsansätze.

Literaturverzeichnis

[Ahle23] Ahlers, Rechtsanwalt Moritz: Der Referentenentwurf zum „Onlinezugangsgesetz 2.0“ aus vergaberechtlicher Sicht. In: Neue Zeitschrift für Baurecht und Vergaberecht. (2023), S. 147

[AlIn23] Alkaldi, Wejdan ; Inkpen, Diana: Text Simplification to Specific Readability Levels. In: Mathematics Bd. 11, Multidisciplinary Digital Publishing Institute (2023), Nr. 9, S. 2063

[AOWJ23] Anschütz, Miriam ; Oehms, Joshua ; Wimmer, Thomas ; Jezierski, Bartłomiej ; Groh, Georg: Language Models for German Text Simplification: Overcoming Parallel Data Scarcity through Style-specific Pre-training, arXiv (2023). — arXiv:2305.12908 [cs]

[AsHZ23] Asghari, Hadi ; Hewett, Freya ; Züger, Theresa: On the Prevalence of Leichte Sprache on the German Web. In: Proceedings of the 15th ACM Web Science Conference 2023, WebSci ’23. New York, NY, USA : Assoc for Computing Machinery, 2023, S. 147–152

[Baum20] Baumann, Antje: Rechtstexte als Barrieren – Einige Merkmale der Textsorte „Gesetz“ und die Verständlichkeit. In: Maaß, C. ; Rink, I. (Hrsg.): Hdb Barrierefreie Kommunikation, Bd. 3, Berlin : Frank & Timme, 2020

[BoSi22] Bomhard, David ; Siglmüller, Jonas: Europ. KI-Haftungsrichtlinie Der aktuelle Kommissionsentwurf und seine praktischen Auswirkungen (2022), S. 506ff.

[Bund08] Bundesgesetzblatt Jahrgang 2008 Teil II Nr. 35: Rechte von Menschen mit Behinderungen — Gesetz zu dem Übereinkommen der Vereinten Nationen vom 13. Dezember 2006 über die Rechte von Menschen mit Behinderungen sowie zu dem Fakultativprotokoll vom 13. Dezember 2006 zum Übereinkommen der Vereinten Nationen über die Rechte von Menschen mit Behinderungen, 2008

[Bund21] Bundesministerium für Arbeit und Soziales: Bericht der Bundesrepublik Deutschland an die Europäische Kommission über die periodische Überwachung der Einhaltung der Barrierefreiheitsanforderungen von Websites und mobilen Anwendungen öffentl. Stellen gemäß Artikel 8 der Richtlinie (EU) 2016/2102, 2021

[Bund22] Bundesrat: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte COM(2022) 495 final (Nr. BR Drucksache 515/22), 2022

[Burc22] Burchardi, Dr Sophie: Risikotragung für KI-Systeme. In: , EuZW 2022., S. 685ff.

[Cham23] Chamberlain, Johanna: The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation. In: European Journal of Risk Regulation Bd. 14, Cambridge University Press (2023), Nr. 1, S. 1–13

[Dase16] Das Europäische Parlament und der Rat der Europäischen Union: Richtlinie (EU) 2016/2102 des Europäischen Parlaments und des Rates über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen.

[Deut22] Deutscher Bundestag: Technikfolgenabschätzung (TA): Künstliche Intelligenz und Distributed-Ledger-Technologie in der öffentlichen Verwaltung (Nr. BT Drucksache 20/3651), 2022

[DGLM23] Deilen, Silvana ; Garrido, Sergio Hernández ; Lapshinova-Koltunski, Ekaterina ; Maaß, Christiane: Using ChatGPT as a CAT tool in Easy Language translation (2023). — arXiv:2308.11563 [cs]

[Dind22] DIN e.V.: Geschäftsplan für ein DIN SPEC-Projekt nach dem PAS-Verfahren zum Thema „Empfehlungen für Deutsche Leichte Sprache", 2022

[Dinn23] DIN-Normenausschuss: Empfehlungen für Deutsche LS (DIN SPEC 33429).

[EBKP22] Ebling, Sarah ; Battisti, Alessia ; Kostrzewa, Marek ; Pfütze, Dominik ; Rios, Annette ; Säuberli, Andreas ; Spring, Nicolas: Automatic Text Simplification for German. In: Frontiers in Communication Bd. 7, Frontiers Research Foundation (2022), S. 706718

[Euro22] Europäische Kommission: Hochrangige Expertengruppe für künstliche Intelligenz | Gestaltung der digitalen Zukunft Europas. URL https://digital-strategy.ec.europa.eu/de/policies/expert-group-ai. - abgerufen am 2023-06-19

[Fino23] Finocchiaro, Giusella: The regulation of AI. In: AI & SOCIETY (2023)

[Fior21] Fioravanti, Chiara: Communicating the Law and Public Information to Vulnerable Audiences: Contexts and Strategies. In: Journal of Open Access to Law Bd. 9 (2021), Nr. 1, S. 8–8

[GaGe22] Gallegos, Isabel ; George, Kaylee: The Right to Remain Plain: Summarization and Simplification of Legal Documents.

[GöTB23] Göllner, Sabrina ; Tropmann-Frick, Marina ; Brumen, Boštjan: Aspects and Views on Responsible Artificial Intelligence. In: Machine Learning, Optimization, and Data Science, Lecture Notes in Computer Science. Cham, 2023

[GrBu20] Grotlüschen, A. ; Buddeberg, K. (Hrsg.): LEO 2018: Leben mit geringer Literalität. Bielefeld : wbv, 2020 — ISBN 978-3-7639-6072-9

[GrSa22] Grabar, Natalia ; Saggion, Horacio: Evaluation of Automatic Text Simplification: Where are we now, where should we go from here. In: Actes de la 29e Conférence sur le Traitement Automatique des Langues Naturelles. Volume 1 : conférence principale. Avignon, France : ATALA, 2022, S. 453–463

[Gugg19] Guggenberger, L.: Einsatz künstlicher Intelligenz in der Verwaltung. In: , NVwZ. Bd. 12 (2019), S. 844

[Hack23] Hacker, Philipp: The European AI Liability Directives -Critique of a Half-Hearted Approach and Lessons for the Future, arXiv (2023). — arXiv:2211.13960 [cs]

[HGNM20] Hansen-Schirra, Silvia ; Gutermuth, Silke ; Nitzke, Jean ; Maaß, Christiane ; Rink, Isabel: Technologies for the Translation of Specialised Texts into Easy Language. In: , 2020 — ISBN 978-3-7329-0688-8, S. 99–127

[KGAK23] Kazim, Emre ; Güçlütürk, Osman ; Almeida, Denise ; Kerrigan, Charles ; Lomas, Elizabeth ; Koshiyama, Adriano ; Hilliard, Airlie ; Trengove, Markus: Proposed EU AI Act. In: AI and Ethics Bd. 3 (2023), Nr. 2, S. 381–387

[KoVM23] Kossens ; V. d. Heide ; Maaß: BGG § 11 Verständlichkeit und leichte Sprache.

[LGGL20] Liu, Yinhan ; Gu, Jiatao ; Goyal, Naman ; Li, Xian ; Edunov, Sergey ; Ghazvininejad, Marjan ; Lewis, Mike ; Zettlemoyer, Luke: Multilingual Denoising Pre-training for Neural Machine Translation. In: Transactions of the Association for Computational Linguistics Cambridge, MA, MIT Press (2020)

[LiFH22] Li, Shu ; Faure, Michael ; Havu, Katri: Liability Rules for AI-Related Harm: Law and Economics Lessons for a European Approach. In: European Journal of Risk Regulation Bd. 13, Cambridge University Press (2022), Nr. 4, S. 618–634

[Lin04] Lin, Chin-Yew: ROUGE: A Package for Automatic Evaluation of Summaries. In: Text Summarization Branches Out. Barcelona, Spain : Association for Computational Linguistics, 2004, S. 74–81

[Maaß20] Maaß, Christiane ; Hansen-Schirra, S. ; Maaß, C. (Hrsg.): Easy Language – Plain Language – Easy Language Plus: Balancing Comprehensibility and Acceptability, Easy–Plain–Accessible. Bd. 3., Berlin : Frank & Timme, 2020.

[Mayr23] Mayrhofer, Ann-Kristin: Produkthaftungsrechtliche Verantwortlichkeit des „Trainer-Nutzers“ von KI-Systemen. In: , RDi 2023. (2023), S. 20ff.

[MMRS55] McCarthy, J. ; Minsky, M. L. ; Rochester, N. ; Shannon, C.E.: A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence (1955)

[MüWa20] Münchener Kommentar zum BGB ; Wagner: BGB § 823, 2023.

[Nort90] North, Douglass C.: Institutions, Institutional Change and Economic Performance, Political Economy of Institutions and Decisions. Cambridge : Cambridge University Press, 1990 — ISBN 978-0-521-39416-1

[PRWZ02] Papineni, Kishore ; Roukos, Salim ; Ward, Todd ; Zhu, Wei-Jing: Bleu: a Method for Automatic Evaluation of Machine Translation. In: Proceedings of the 40th Annual Meeting of the Association for Computational Linguistics. Philadelphia, Pennsylvania, USA : Ass. for Computational Linguistics, 2002, S. 311–318

[RSKK21] Rios, Annette ; Spring, Nicolas ; Kew, Tannon ; Kostrzewa, Marek ; Säuberli, Andreas ; Müller, Mathias ; Ebling, Sarah: A New Dataset and Efficient Baselines for Document-level Text Simplification in German. In: Proceedings of the Third Workshop on New Frontiers in Summarization. Online and in Dominican Republic : Association for Computational Linguistics, 2021. — tex.ids= riosNewDatasetEfficient2021a, S. 152–161

[RSRL20] Raffel, Colin ; Shazeer, Noam ; Roberts, Adam ; Lee, Katherine ; Narang, Sharan ;

Matena, Michael ; Zhou, Yanqi ; Li, Wei ; u. a.: Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer. In: arXiv:1910.10683 [cs, stat] (2020). — arXiv: 1910.10683

[SäEV20] Säuberli, Andreas ; Ebling, Sarah ; Volk, Martin: Benchmarking Data-driven Automatic Text Simplification for German. In: Proceedings of the 1st Workshop on Tools and Resources to Empower People with REAding DIfficulties (READI). Marseille, France : European Language Resources Association, 2020

[Schu23] Schuett, Jonas: Risk Management in the Artificial Intelligence Act. In: European Journal of Risk Regulation, Cambridge University Press (2023), S. 1–19

[ScSH22] Schoch ; Schneider ; Hornung: VwVfG § 35a Rn. 3-7.

[ScTr21] Schomacker, Thorben ; Tropmann-Frick, Marina: Language Representation Models: An Overview. In: Entropy Bd. 23, Multidisciplinary Digital Publishing Institute (2021), Nr. 11, S. 1422

[SGMH23] Schomacker, Thorben ; Gille, Michael ; Marina Tropmann-Frick ; von der Hülls, Jörg: Data and Approaches for German Text Simplification - Next Steps toward an Accessibility-enhanced Communication. In: , 2023

[SpRE21] Spring, Nicolas ; Rios, Annette ; Ebling, Sarah: Exploring German Multi-Level Text Simplification. In: Proceedings of the International Conference on Recent Advances in Natural Language Processing (RANLP 2021). Held Online : INCOMA Ltd., 2021, S. 1339–1349

[Stau23] Staudenmayer, Dr Dirk: Haftung für Künstliche Intelligenz. In: , NJW 2023. (2023), S. 894ff.

[StMK23] Stodden, Regina ; Momen, Omar ; Kallmeyer, Laura: DEPLAIN: A German Parallel Corpus with Intralingual Translations into Plain Language for Sentence and Document Simplification, arXiv (2023). — arXiv:2305.18939 [cs]

[Stod22] Stodden, Regina: Erstellung eines parallelen Vereinfachungskorpus für die deutsche Sprache – Unter Verwendung des HHU Annotationstools TS-anno (2022)

[SuEV16] Suter, Julia ; Ebling, Sarah ; Volk, Martin: Rule-based Automatic Text Simplification for German. In: Proceedings of the 13th Conference on Natural Language Processing, 2016, S. 279–287

[Thap21] Thapa, Basanta Für mehr Barrierefreiheit in der digitalen Verwaltung, 2021

[TuWW22] Tunstall, Lewis ; von Werra, Leandro ; Wolf, Thomas: Natural Language Processing with Transformers. Revised Edtion. Erscheinungsort nicht ermittelbar : O'Reilly Media, Inc., 2022

[VSPU17] Vaswani, Ashish ; Shazeer, Noam ; Parmar, Niki ; Uszkoreit, Jakob ; Jones, Llion ; Gomez, Aidan N ; Kaiser, Lukasz ; Polosukhin, Illia: Attention is All you Need. In: Guyon, I. ; Luxburg, U. V. ; Bengio, S. ; Wallach, H. ; Fergus, R. ; Vishwanathan, S. ; Garnett, R. (Hrsg.): Advances in Neural Information Processing Systems 30, 2017, S. 5998–6008

[Wend22] Wendehorst, Christiane: Liability for Artificial Intelligence:. The Cambridge Handbook of Responsible Artificial Intelligence: Interdisciplinary Perspectives, Cambridge University Press, 2022

[Wilr23] Wilrich, Thomas: Rechtliche Bedeutung von DIN-Normen und technischen Regelwerken - beck-online.pdf. In: , NJW 2023. (2023), S. 1400ff.

[XNPC16] Xu, Wei ; Napoles, Courtney ; Pavlick, Ellie ; Chen, Quanze: Optimizing Statistical Machine Translation for TS. In: Transactions of the Association for Computational Linguistics Bd. 4. Cambridge, MA, MIT Press (2016), S. 401–415

ERSTE DER ZWEITEN LETZTEN SEITEN

ZWEITE DER ZWEITEN LETZTEN SEITEN