

Transitionen in der industriellen Kommunikation

Datensicherheit zwischen bilateralem Austausch und Datenräumen

Hannah-Lena Graw

Beitrag zur Ad-hoc-Gruppe »Transition? Nicht ohne uns! – Studentische Perspektiven auf Transitionen«

Für diesen Beitrag habe ich ein Thema aus meiner Bachelorarbeit wiederaufgegriffen. In der Arbeit untersuche ich, wie Unternehmen externe Erwartungen mit ihrem eigenen Anspruch auf Datensicherheit in Einklang bringen – oder „soziologischer“: die Respezifikation von Ansprüchen am Beispiel von Datensicherheit in plattformbasierten Datenräumen.

Zu dem Thema Datensicherheit bin ich durch meine Mitarbeit an einem Projekt¹ gelangt, welches die Bewältigung externer gesellschaftlicher Anforderungen an Organisationen durch digitale Plattformen untersucht. Im Projekt, wie auch in meiner Arbeit, wird die Initiative Manufacturing-X als empirisches Beispiel für eine besondere Art digitaler Plattformen aufgerufen, die sogenannten „Datenräume“. Dabei handelt es sich um technische Infrastruktur, welche multilateralen Datenaustausch ermöglicht. Die empirischen Daten, auf die ich meine Analyse stütze, stammen sowohl aus Felddokumenten wie Vorhabensbeschreibungen und Informationsmaterialien für zukünftige Partner als auch aus qualitativen Expert*inneninterviews mit Vertreter*innen von Manufacturing-X und Geschäftsführer*innen industrieller Betriebe. Da sich die Initiative noch im Aufbau befindet, sind die Praktiken und Funktionsweisen noch nicht endgültig festgelegt und auch über ihren Erfolg oder ihr Scheitern ist noch nicht entschieden. Wir haben es hier also mit einer *Transition industrieller Kommunikation* zu tun, in der sich bestehende und neue Verhaltensweisen und Deutungen gegenüberstehen und noch nicht ganz klar ist, was sich am Ende durchsetzen wird. In diesem Zusammenhang werden Erwartungen an Datensicherheit bereits jetzt als ausschlaggebendes Kriterium für die Zukunft der Initiative angesehen. So wird die Frage nach der Datensicherheit sowohl in den gesammelten Dokumenten als auch in den Interviews immer wieder aus verschiedenen Perspektiven aufgeworfen.

Manufacturing-X setzt sich aus Akteuren der Wirtschaft, Politik und Wissenschaft zusammen. Die Initiative verfolgt nach eigener Aussage das Ziel „einer digital vernetzten Industrie in der ganzen Breite“ und ist eine Dachinitiative, unter der verschiedene industriespezifische Datenraumprojekte durchgeführt werden (Redaktion Plattform Industrie 4.0 2025).² Hierzu werden aktuell Unternehmen aus den

¹ Das Projekt inteRKombi wird von 2024 bis 2028 durch das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) gefördert. Das an der Johannes Gutenberg-Universität Mainz angesiedelte Projekt ist Teil des Programms „Dynamiken digital vernetzter Wertschöpfungssysteme (DynaVer)“.

² Manufacturing-X. Initiative zur Digitalisierung der Lieferketten in der Industrie, 28.10.25, <https://www.plattform-i40.de/IP/Redaktion/DE/Standardartikel/manufacturing-x.html>

jeweiligen Branchen zur Teilnahme motiviert und erste produktive Anwendungen entwickelt und demonstriert. Wie bei allen digitalen Plattformen setzt man hier auf Netzwerkeffekte und vertrauensbasierte Zusammenarbeit: Die Idee funktioniert erst, wenn genügend Akteure an der Plattform teilnehmen. Andererseits steht man vor dem Problem, dass sich potenzielle Teilnehmer nur überzeugen lassen, wenn der Datenraum auch wirklich funktioniert. Neben anderen Kriterien werden vor allem Unsicherheiten als Hindernisse für die Teilnahme aufgefasst, besonders die Unklarheit darüber, wie sicher geteilte Daten wirklich sind. Daraus wird deutlich, dass Datensicherheit ein ausschlaggebendes Kriterium für die Zukunft der Initiative ist. Die Datensicherheit scheint eine Voraussetzung für das Funktionieren des Datenraumes zu sein. Im Folgenden skizziere ich, wie wir dem soziologisch nachgehen können. Zuvor beschreibe ich den Fall und beantworte die Frage, worum es sich bei Datenräumen für Industrieunternehmen eigentlich handelt.

Datenräume und das Problem mit der Datensicherheit

Datenräume sollen eine technische Lösung für multilateralen Datenaustausch bieten, beispielsweise für die Nachverfolgung von Produkten und Teilen entlang einer Lieferkette. Sie versprechen teilnehmenden Unternehmen die Möglichkeit, wechselseitig Informationen für eine Zusammenarbeit auszutauschen, ohne durch die Offenlegung wirtschaftlichen Nachteilen ausgesetzt zu sein. Vergleichbar wäre dies mit einem analogen, physischen Raum, beispielsweise bei einem Seminar oder einer Konferenz. Alle Teilnehmenden verfügen über spezifisches Wissen, welches von großem Nutzen für die anderen Anwesenden sein könnte. Eine Kooperation ist durch die bloße Anwesenheit jedoch nicht garantiert. Alle Teilnehmenden entscheiden selbst, wer zu welchen Bedingungen Zugang zu ihrem Wissen erhalten soll. Zum Produktversprechen der Datenräume gehört es, alle Kommunikation zwecks Datenaustauschs sicher an einem Ort zu vereinen, ohne dass Unternehmen dabei die Kontrolle über ihre Daten verlieren. Durch diese versprochene Kontrolle sollen die Datenräume ein höheres Vertrauen zwischen den Akteuren generieren. Zudem besteht die Möglichkeit, anstelle von vielen individuellen Verträgen eine multilaterale Zusammenarbeit mit allen Partnern an einem Ort abzuwickeln.

Wie aber soll eine digitale Dateninfrastruktur dieses Vertrauen aufbauen? Sobald Daten mit einem Kooperationspartner geteilt werden, besteht die Gefahr, dass dieser sie missbraucht, weiterverkauft oder allgemein zugänglich macht. Außerhalb von Datenräumen handeln Unternehmen mit jedem Partner individuelle Verträge aus und bestimmen Bedingungen für vertrauensvolle Zusammenarbeit immer wieder neu. Für die Sanktionierung missbräuchlichen Verhaltens werden gesetzliche Vorschriften durch Vertragsstrafen ergänzt. Bei der Verwendung des Datenraumes stehen den Unternehmen keine anderen Mittel zur Verfügung als bei diesen gängigen bilateralen Verträgen. Daher ist meine These, dass durch die wechselseitige Verfügbarkeit von Informationen lediglich eine Patt-Situation entsteht, in der sich die Unternehmen gegenüberstehen. Sollte ein Unternehmen nachlässig oder böswillig mit den Daten seiner Partner umgehen, würde es damit auch die Veröffentlichung der eigenen Daten riskieren. Basiert die Zusammenarbeit innerhalb von Datenräumen also nicht wie beworben auf Vertrauen, sondern auf der gegenseitigen Möglichkeit, großen Schaden herbeizuführen?

Unternehmen reagieren unterschiedlich auf diese Problematik. Die einfachste Lösung wäre es, den Datenaustausch gar nicht erst über diese Infrastruktur zu organisieren. Da aber einige marktführende Unternehmen, beispielsweise in der Automobilindustrie, die Teilnahme am Datenraum als Bedingung für die weitere Zusammenarbeit aufgestellt haben, befinden sich gerade kleinere, mittelständische Unternehmen in einer Zwangssituation. Entweder sie riskieren die Sicherheit ihrer Daten oder den Fortbestand ihrer Geschäftsbeziehungen. Um ihre interne Datensicherheit zu gewährleisten und gleichzeitig Informationen im Datenraum zur Verfügung stellen zu können (also: das Vertrauensproblem zu lösen), wenden sie Formen der Respezifikation an.

Respezifikation und Entkopplung

Respezifikation wird dabei nach Niklas Luhmann als Konkretisierung von „gesamtgesellschaftlich einleuchtenden, aber zu allgemein geratenen Kriterien“ (2002, S. 143) verstanden. Sie ermöglicht die praktische Umsetzung von abstrakt gehaltenen Anforderungen. Besonders an wirtschaftliche Unternehmen werden zunehmend solche zu allgemein formulierten Anforderungen gestellt, von gesellschaftlichen Gruppen, von Kooperationspartnern, aber auch durch Erwartungen, die das Unternehmen an sich selbst stellt. In diesem Sinne bezeichnet Luhmann die Respezifikation als Prozesse und soziale Strukturen, durch welche generalisierte Werte, Deutungsschemata und Erwartungen nachvollziehbar werden (Besio und Meyer 2022, S. 441). Der Begriff selbst beschreibt also keine spezifischen Handlungen, welche Akteure wie beispielsweise Unternehmen umsetzen können. Vielmehr werden für diese Konkretisierung verschiedene Strategien angewendet. Cristina Besio und Uli Meyer (2022) nennen in diesem Zusammenhang *Übersetzung*, *Schnittstellen* und *Entkopplung*³. Übersetzung bezeichnet die Umformulierung verschiedener Logiken auf gemeinsame Elemente. Schnittstellen werden von Organisationen aufgebaut, die verschiedene Zwecke erfüllen müssen. Für diesen Beitrag ist speziell die Entkopplung besonders interessant. Entkopplung beschreibt die Trennung „formaler Strukturen von internen Prozessen, so dass externen Erwartungen zwar formal entsprochen wird, aber organisationale Prozesse davon getrennt und ‚geschützt‘ werden“ (Besio und Meyer 2022, S. 442) können. Durch Entkopplung trennen Organisationen also ihre formalen Strukturen von ihren tatsächlichen Arbeitsabläufen (Meyer und Rowan 1977, S. 341). So gelingt es den Unternehmen, mehreren, teils widersprüchlichen Anforderungen gleichzeitig zu entsprechen – in diesem Beispiel der Verpflichtung zur Teilnahme am Datenraum und der Aufrechterhaltung der eigenen Datensicherheit.

Ganz praktisch könnte eine Verarbeitungsstrategie von Unternehmen, die zur Teilnahme am Datenraum gezwungen sind, aber von der Sicherheit nicht überzeugt sind, so aussehen: Die Unternehmen entkoppeln die internen Daten, die für die Zusammenarbeit relevant sind oder von denen die Bereitstellung verlangt wird, von allen übrigen Daten und internen Prozessen. So kann externen Erwartungen entsprochen werden, ohne die Unternehmensstruktur und die eigenen Erwartungen grundlegend verändern zu müssen. Eine solche Entkopplung ermöglicht es, nur die relevanten Daten zu teilen, ohne gleichzeitig zu viel über das eigene Unternehmen preiszugeben. Die technische Architektur des Datenraums unterstützt die Entkopplung in diesem Falle besonders. Durch diese Trennung bleibt ein Großteil der unternehmensinternen Daten vor einem möglichen Scheitern der Zusammenarbeit durch Vertrauensbrüche geschützt.

Überbrückung fehlenden Vertrauens?

Wie bereits beschrieben, verfügen die Datenräume über keine spezifischen Sanktionsmöglichkeiten für den Umgang mit Verstößen. Die vertraglichen Regeln für die Teilnahme am Datenraum unterscheiden sich kaum von bilateralen Verträgen. Manufacturing-X gibt als Entwicklungsinitiative der Datenräume lediglich eigene Standards für die Teilnahme vor. Bei Verstößen kann neben rechtlichen Konsequenzen, die ohnehin zu befürchten wären, lediglich ein Ausschluss aus dem Datenraum folgen. Zum Versprechen der Datenräume an potenzielle Teilnehmer gehört es, dass die technische Architektur Sicherheit und Kontrolle über die eigenen Daten ermöglicht. Ein abweichendes, regelwidriges Verhalten, wie bei-

³ Besio und Meyer begründen ihren Ansatz auf dem Begriff der Re-Spezifikation von Luhmann und entwickeln so ihren Begriff der Re-Kombination. Damit erfassen sie, dass „Organisationen in der Regel nicht einzelne Erwartungen re-spezifizieren, sondern dies gleichzeitig mit mehreren Anforderungen aus unterschiedlichen gesellschaftlichen Kontexten [...] tun“ (Besio und Meyer 2022, S. 441). Übersetzung, Schnittstellen und Entkopplung zeichnen sich als Formen des Umgangs mit diesen heterogenen Anforderungen aus.

spielsweise die Weiterverbreitung, kann aber auch durch die technischen Möglichkeiten nicht ausgeschlossen werden. Das Vertrauen in eine regelkonforme Zusammenarbeit generiert sich also eher durch die rechtliche Sicherheit als durch den Datenraum selbst. Ein gewisser Grad an Vertrauen in die anderen Parteien bleibt jedoch eine wichtige Voraussetzung.

Jede wirtschaftliche Zusammenarbeit zwischen Industrieunternehmen erfordert außerdem (unabhängig vom Medium) den Austausch von Daten, selbst wenn es sich nur um Bestelldaten und Lieferadressen handelt. In Zukunft soll die Zusammenarbeit im Datenraum aber auch Echtzeitdaten über Maschinen, Produktzusammensetzung und Produktionsprozesse beinhalten. Je mehr Daten aus diesen sensiblen Bereichen aktiv geteilt werden oder in Zukunft geteilt werden sollen, umso mehr Vertrauen muss zwischen den Parteien aufgebaut werden. Diese Hürde für die Zusammenarbeit besteht zwar unabhängig vom Datenraum, sie könnte aber durch die Teilnahme überwunden werden. Entkopplung kann als Strategie dienen, um fehlendes Vertrauen zwischen den Unternehmen zu überbrücken. Die technischen Möglichkeiten des Datenraums, Daten zu teilen, ohne dabei die Kontrolle über sie zu verlieren, und der über den Betreiber sichergestellte, dauerhafte Zugang zu den Daten unterstützen diese Strategie. Vertrauen in den Datenraum könnte damit mangelndes Vertrauen in potenzielle Geschäftspartner ausgleichen, möglicherweise sogar anfangs ersetzen. Mindestens eine dieser Vertrauensbeziehungen muss jedoch bestehen: entweder die zum Datenraum oder die zum Geschäftspartner.

Als Mittel der Respezifikation durch Entkopplung scheint die technische Infrastruktur des Datenraums es zu ermöglichen, fehlendes Vertrauen in der Zusammenarbeit zu überbrücken. Vertrauen bleibt dabei eine wichtige Voraussetzung für wirtschaftliche Zusammenarbeit, jedoch könnte Vertrauen in den Datenraum mindestens kurzfristig das Vertrauen in den Geschäftspartner substituieren. Entkopplung bietet dabei nicht nur die Möglichkeit, widersprüchlichen Ansprüchen formal zu entsprechen, ohne die internen Strukturen zu beeinträchtigen. Durch die Trennung der geteilten Daten bleiben die übrigen Informationen vor Vertrauensbrüchen geschützt. So trägt Entkopplung zur Datensicherheit im Datenraum bei.

Literatur

- Besio, Cristina, und Uli Meyer. 2022. Organisationale Re-Kombination und sozialer Wandel: Eine Forschungsagenda. *Soziale Systeme* 25:436–456.
- Luhmann, Niklas. 2002. *Das Erziehungssystem der Gesellschaft*. 8. Auflage. Hrsg. Dieter Lenzen. Frankfurt am Main: Suhrkamp.
- Meyer, John W., und Brian Rowan. 1977. Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology* 83:340–363.
- Redaktion Plattform Industrie 4.0. 2025. Manufacturing-X. Initiative zur Digitalisierung der Lieferketten in der Industrie.
<https://www.plattform-i40.de/IP/Redaktion/DE/Standardartikel/manufacturing-x.html> (Zugegriffen: 9. Juli 2026).