Freitag, 31. Oktober 2025, 17:00 Uhr
~10 Minuten Lesezeit

Drittanbieterhölle und Servicewüste

Der Digitalkapitalismus erschwert selbst einfachste Alltagshandlungen und bietet keine Unterstützung.

von Felix Feistel
Foto: Alliance Images/Shutterstock.com

Wer heute im Internet unterwegs ist und dort Dienstleistungen in Anspruch nimmt oder gar

Produkte einkauft, der wird schnell konfrontiert mit einem Geflecht aus Dienstleistungen von Drittanbietern, fortwährenden Weiterleitungen und fehleranfälligen Systemen. Kundenservice wird immer mehr durch nutzlose Chatbots ersetzt, die auf die tatsächlich entstehenden Probleme außer Satzbausteinen keine Antworten haben. Einen echten Menschen zu kontaktieren, wird zunehmend schwierig. Der Einzelne steht einem anonymen Monolithen gegenüber und erhält damit bereits einen ersten Eindruck von der kommenden digitalen Diktatur.

Das Onlineshopping ist in heutiger Zeit ja eigentlich schon gang und gäbe. Immer mehr Dinge, vor allem Elektronikgeräte, Kleidung oder Möbel, werden online eingekauft. Wer dabei auf den Monopolisten Amazon verzichten oder Produkte kaufen will, die nur vom Hersteller direkt vertrieben werden, muss sich dabei auf die Anbieterseite begeben. Oft muss man sich dabei durch eine ganze Angebotspalette klicken und bekommt mehr oder weniger aufdringlich noch den Kauf zusätzlicher Produkte nahegelegt. Schließt man seinen Einkauf dann ab, kommt es schnell zur Auswahl der Zahlungsmethode. Und hier beginnt sie dann, die Drittanbieterhölle.

> ***Denn war es in früheren Zeiten üblich, einfach auf Rechnung zu kaufen, also eine Rechnung per E-Mail oder sogar als leibhaftigen Brief zugeschickt zu bekommen, ist diese Option bei immer weniger Anbietern noch aufzufinden. Stattdessen wird der Kunde auf Onlinedienste verwiesen, etwa Google Pay, Apple Pay oder die Sofortüberweisung von Klarna.***

Statt also eine direkte Geschäftsbeziehung zwischen Anbieter und Kunden zu etablieren, werden Zahlungsdienstleister dazwischengeschaltet, mit denen die eigentliche Geschäftsbeziehung stattfindet. Entscheidet sich der Kunde für eine dieser Methoden — und eine Wahl hat er in der Regel nicht —, wird er auf die Seite dieses Drittanbieters umgeleitet und muss sich dort mit seinen Daten authentifizieren. Hat er ein Google-Pay- oder Apple-Pay Konto, oder auch PayPal, geht dieser Vorgang relativ schnell. Hat er das nicht, bleibt der Anbieter Klarna. Doch auch hier ist umständliche Authentifizierung gefragt. Handynummer für einen Code, dann E-Mail-Adresse und schließlich die Aufforderung, sich einen Account anzulegen.

> ***Viele Menschen werden hier gleichgültig mit den Schultern zucken. „Na und? Dann lege ich mir einfach ein Konto an und kann dann ganz bequem shoppen.“ Allerdings haben wir es hier mit den Tentakeln der großen Datenkraken zu tun. Google, Apple, PayPal, sie alle sammeln Daten über das persönliche Einkaufsverhalten und lassen diese in die Bewertung der Person einfließen.***

All das legt die Grundlage der digitalen Überwachungsinfrastruktur, die letztlich auch mit CO_2-Konto und CBDC gekoppelt werden und dann zur Verhaltenssteuerung genutzt werden kann. Wer das ablehnt, sollte diese Dienste lieber nicht nutzen.

Dann bleibt der schwedische Bezahldienst Klarna. Doch auch hier sollte sich der Kunde im Klaren sein: Der Dienst benötigt persönliche Daten und erfordert zudem das Einloggen in das Bankkonto. Die Zugangsdaten für das Bankkonto werden also an Klarna gegeben, der diese dann nutzt, um die Buchung auf dem Konto vorzunehmen. Der Kunde gewährt damit einem Drittanbieter Zugang zum eigenen Bankkonto. Der Anbieter selbst gibt an, dass dieser Vorgang aufgrund der Verschlüsselung vollkommen sicher sei. Allerdings kam es in der Vergangenheit vor, dass Klarna

Nutzerdaten geleakt hat (https://www.hagel-it.de/it-service/klarna-leakt-bankdaten-von-usern-durch-ein-update.html), und vor dem **omnipräsenten Phishing** (https://www.chip.de/news/Vorsicht-Betrug-Klarna-Kunden-sind-ins-Visier-von-Kriminellen-gelangt_185242560.html) muss man sich auch hier in Acht nehmen.

Zudem kann Klarna auf diese Weise die Daten des Kontos, wie etwa **Zahlungen, auslesen** (https://www.golem.de/news/verbraucherschuetzer-warnt-klarna-analysiert-kontoauszuege-seiner-nutzer-2412-191477.html). Dies geschieht mit Sicherheit in Bezug auf alle Kontovorgänge der letzten 30 Tage vor dem Zahlungszeitpunkt. Wie viele Daten der Anbieter insgesamt ausliest, ist unklar. Im Jahr 2022 erhielt das Unternehmen für die Datenerfassung der Nutzerkonten sogar **einen Big-Brother-Award** (https://www.golem.de/news/big-brother-awards-lieferando-ueberwacht-seine-angestellten-klarna-seine-kunden-2204-164983.html).

Das Unternehmen selbst hingegen gibt an, keine Daten zielgerichtet zu erfassen und auch keine Daten weiterzuverkaufen. Dennoch findet eine Datenübertragung stattfindet, und diese kann auch von Dritten auslesbar sein. Das Unternehmen hat in der Vergangenheit bereits eine hohe Geldbuße aufgrund des Verstoßes gegen die Datenschutzgrundverordnung (DSGVO) in Höhe von **670.000 Euro** (https://www.mimikama.org/klarna-strafe-wegen-verstoss-datenschutz/) zahlen müssen. Auch die vor einigen Jahren veröffentliche Klarna-App weist **erhebliche Sicherheitsmängel** (https://www.golem.de/news/klarna-super-app-mit-super-datenschutzproblemen-2112-161924.html) auf. Zudem entstehen durch Klarna zwar keine direkten Kosten für den Endkunden, allerdings ist der Dienst für die Händler nicht kostenlos — mit der Folge, dass die Kosten auf die **Produktpreise aufgeschlagen werden** (https://www.bezahlen.net/ratgeber/klarna-sofortueberweisung-sicherheit/).

Doch ob Klarna, Google Pay, Apple Pay oder PayPal: Der Kunde sollte sich stets vor Augen führen, dass jede Datenübertragung im Internet potenziell unsicher ist und von Dritten ausgelesen werden kann. Die Konzerne an sich sind schon das Risiko: Sie nutzen die Daten zu undurchsichtigen Zwecken. Oftmals werden diese einfach verkauft; doch auch die umfassende Überwachung der Bürger stützt sich auf diese Daten.

Nun gibt es in der Regel auch noch die Möglichkeit, online mit der Kreditkarte zu zahlen. Hier stellt sich dasselbe Problem: Die Kreditkartendaten können einfach abgefangen und von Dritten genutzt werden, wie es immer wieder passiert. Sie können sogar einfach von spezieller Software erraten werden. Das ist daher relativ einfach, weil hier nur drei Zahlen gebraucht werden: Kartennummer, Ablaufdatum und eine spezielle dreistellige Zahl, die in der Regel auf der Rückseite der Karte zu finden ist. Sind diese erraten, kann der Dritte diese Daten einfach nutzen, um im Internet auf Shoppingtour zu gehen.

> ***Die sicherste Option, nämlich einfach auf Rechnung zu bestellen und dann eine Banküberweisung zu tätigen, wird jedoch immer mehr abgeschafft. Stattdessen werden die Menschen in die Drittanbieterhölle gedrängt, um all ihre Daten an die Konzerne zu geben und sich dem Risiko auszuliefern, dass die Konten geknackt oder die Daten zur flächendeckenden Überwachung und Kontrolle eingesetzt werden.***

Diese Dienste werden den Kunden als bequemere Option dargestellt, sind aber im Endeffekt viel komplizierter und umständlicher als eine einfache Rechnung. Denn zur Zahlung wird man einige Male umgeleitet — vom Onlineshop über den Drittanbieter, wo man sich authentifizieren muss, oft mithilfe von SMS-Codes und per Mail — meistens beides —, und schließlich zurück zum Onlineshop. Dass der Vorgang gelingt, ist dabei noch lange nicht garantiert.

Jede Datenübermittlung über das Internet ist unsicher, auch wenn die Anbieter noch so gute Verschlüsselung versprechen. Allerdings gehen selbst viele Banken mittlerweile so weit, die Menschen zum Online-Banking zu drängen — indem sie die Preise für am Schalter vorgenommene Kontovorgänge in die Höhe treiben und das Online-Banking als kostenlose oder zumindest günstigere Option anbieten. Es findet also eine allgemeine Verdrängung analoger und direkter Kontaktmöglichkeiten zugunsten der Onlineoptionen und der Drittanbieter — meist große Datenkraken — statt. Immer mehr Datenkraken wollen an den Futtertrögen des digitalen Kapitalismus teilhaben und schalten sich geradezu parasitär in Bezahlvorgänge, Authentifizierungsprozesse oder andere vermeintliche Dienstleistungen ein — oft ohne dass dem Nutzer noch eine Wahl bleibt. Er wird dazu gezwungen, seine Daten an alle möglichen Anbieter zu verschleudern.

Servicewüste

Doch das ist nicht die einzige negative Folge des Digitalkapitalismus.

> ***Denn durch die Verlagerung ins Digitale, verbunden mit der Entwicklung von KI und dem Zwang, Personal einzusparen, verkommt der digitale Kapitalismus zugleich zu einer Servicewüste.***

Das fällt allerdings erst dann auf, wenn die ach so bequemen Vorgänge einmal nicht so reibungslos verlaufen wie versprochen — etwas, das immer häufiger vorkommt. Dann sucht der Kunde meistens vergebens nach einer Kontaktmöglichkeit. E-Mail-Adresse, um sein Leid zu klagen? Fehlanzeige. Stattdessen klickt er sich durch unzählige Seiten FAQs, auf denen die eigenen Probleme natürlich niemals zu finden sind, weil die dort bearbeiteten Fragestellungen nicht über Allgemeinplätze hinausgehen. Findet er

dann nach langem Suchen auf der einhundertsten Unterseite doch eine Mail-Adresse, erhält er auf seine Mails oft eine freundliche Eingangsbestätigung — und hört danach nie wieder etwas.

Bleibt noch das Kontaktformular, das aber oftmals ebenso in die Sackgasse führt. Telefonnummern, um direkt mit einem menschlichen Mitarbeiter zu sprechen, werden auch überall abgebaut. So bleibt der Nutzer am Ende auf einen Live-Chat verwiesen, der — wie könnte es anders sein — von einem KI-Tool geführt wird. Und hier kann er sich dann stundenlang mit der KI unterhalten und wird dabei doch wieder nur auf die FAQs verwiesen, weil die vermeintliche KI in der Regel das Problem überhaupt nicht versteht. So dreht man sich auch hier nur im Kreis, ohne der Lösung des Problems auch nur näher zu kommen. Gibt es einen Live-Chat mit echten Personen, ist dieser oftmals beschränkt auf wenige Stunden in der Woche — und dann wird auch noch auf das hohe Aufgebot an Anfragen verwiesen, weshalb man sich doch bitte später wieder melden solle.

> ***Besonders nervenaufreibend wird dieses Phänomen dann, wenn ein jahrelang problemlos funktionierender Anbieter — etwa ein E-Mail-Service — plötzlich seine Bedingungen ändert, beispielsweise indem beim Einloggen plötzlich eine Authentifizierung mittels Handynummer und ID erforderlich wird.***

Hat der Kunde seine Handynummer und seine richtige Adresse dabei nie angegeben — weil es den Anbieter letztlich nicht zu interessieren hat, wie er heißt und wo er wohnt —, hat er ein Problem. Denn dann scheitert jede Authentifizierung. Für diese — ebenfalls über Drittanbieter durchgeführt — muss er zudem wieder seine Daten in den Rachen der Bestie großer Konzerne werfen — mit den bereits besprochenen Nebeneffekten. Beschwerden stoßen auf taube Ohren, beziehungsweise auf überhaupt keine Ohren, da es keine Stelle gibt, an die diese gerichtet werden könnten. So ist das

eigene Konto in diesem Fall verloren.

Der Digitalkapitalismus in Verbindung mit dem Ausbau zur totalitären Überwachungsmaschinerie zwingt die Menschen also dazu, immer mehr ihrer Daten preiszugeben, die dann von Dritten, Vierten und dem Staat erfasst und verwendet werden. Denn dass die großen Tech-Konzerne allesamt aus der Militärforschung der USA hervorgegangen sind, sollte mittlerweile durchgedrungen sein. Gleichzeitig stellt das System die Menschen vor einen anonymen Monolithen, mit dem eine Kommunikation gar nicht mehr möglich ist. Der entpersonalisierte Datenapparat blockt jede Möglichkeit echter Anfragen und verweist stattdessen auf oberflächliche, vollkommen nutzlose KI-Tools und allgemeine Antwortmöglichkeiten. Gleichzeitig fordert er immer mehr Daten ein und erschwert jede auch noch so banale Handlung — etwa den einfachen Einkauf. Damit erhaschen die Menschen bereits einen Einblick in die geplante digitale Diktatur, bei der sie einer totalitären, digitalen Maschinerie gegenüberstehen, die ihre Regeln ständig ändert und ihnen immer mehr Daten abpressen und Verhaltensweisen aufzwingen kann.

Den meisten Menschen ist das allerdings vollkommen egal, weil sie sich von der scheinbaren Bequemlichkeit — die bei näherem Hinsehen ja überhaupt nicht gegeben ist — verlocken lassen. Wer all das nicht unterstützen will, der wird zunehmend aus der digitalen Sphäre ausgeschlossen — was ja vielleicht an sich nicht schlecht wäre, wenn es Alternativen zu den Diensten, oder zumindest noch eine Möglichkeit auf analoges Leben gäbe. Doch diese werden — siehe Banken — immer mehr abgeschafft, alle Dienste in die digitale Sphäre verlagert.

Auf diese Weise kreiert das System schleichend einen Digitalzwang, der letztlich die Grundlage für die totalitäre Überwachungsmaschinerie darstellt, die sich die Tech-Mogule, Finanz-Oligarchen und ihre Lakaien in der Politik als Idealbild

vorstellen. Gleichzeitig wird das ganze System immer unsicherer, da Daten schnell an Dritte und Vierte gelangen können — sei es durch Kauf oder durch das Hacken — **die ePA lässt grüßen** (https://freedert.online/meinung/233022-einladung-fuer-betrueger-verbaende-fordern/). Und dann können diese Daten missbraucht werden, indem Konten leergeräumt werden oder auf Kosten des Kunden online geshoppt wird.

Der Datenkapitalismus liefert die Menschen also unter anderem der Gefahr der plötzlichen Verarmung oder des Identitätsdiebstahls aus, bietet aber gleichzeitig meist keinerlei Hilfe in solchen Fällen. Damit handelt es sich um ein desinteressiertes, aber zunehmend totalitäres System, das eine große Gefahr für die Menschen und letztlich für die Gesellschaft insgesamt wird.

Die einzigen Gegenmaßnahmen sind die totale Verweigerung der Nutzung dieser Dienste, sowie eine Forderung nach analogen Möglichkeiten für alle Dienste — inklusive des Bezahlens per Bargeld. Nur wenn sich diese Dienste nicht lohnen beziehungsweise boykottiert werden, kann verhindert werden, dass ständig neue parasitäre Unternehmen wie Pilze aus dem Boden schießen, um ihren Anteil vom digitalen Kuchen einzufahren.

Felix Feistel, Jahrgang 1992, studierte Rechtswissenschaften mit dem Schwerpunkt Völker- und Europarecht. Schon während seines Studiums war er als Journalist tätig; seit seinem Staatsexamen arbeitet er hauptberuflich als freier Journalist und Autor. So schreibt er für **manova.news** (https://www.manova.news/), **apolut.net**

(https://apolut.net/), **die Freie Medienakademie** (https://www.freie-medienakademie.de/) sowie auf seinem eigenen **Telegram-Kanal** (https://t.me/Felix_Feistel). Eine Ausbildung zum Traumatherapeuten nach der Identitätsorientierten Psychotraumatheorie und -therapie (IoPT), erweiterte sein Verständnis von den Hintergründen der Geschehnisse auf der Welt.