Kaufen? Nur mit Identitätsnachweis!

Dawid Snowden · Veröffentlicht: 13.03.2026

Wer heute einen Computer, ein Smartphone oder ein anderes hochwertiges elektronisches Gerät bei MediaMarkt oder einer anderen großen Elektronikkette kauft, stößt zunehmend auf eine Praxis, die vielen zunächst banal erscheint: Der Händler verlangt personenbezogene Daten. Ein Name, eine Adresse, manchmal sogar die Vorlage eines Ausweises. Für viele Käufer wirkt dies wie eine nebensächliche Formalität innerhalb eines gewöhnlichen Kaufvorgangs. Schließlich scheint es sich lediglich um einen simplen Tausch zu handeln – Geld gegen Ware.

Doch genau hier beginnt eine Entwicklung, deren Bedeutung weit über den klassischen Verkaufsvorgang hinausgeht.

Der moderne Elektronikhandel ist längst nicht mehr nur ein Ort, an dem Produkte verkauft werden. Er ist Teil eines Systems aus Sicherheitsmechanismen, wirtschaftlichen Interessen und digitalen Verwaltungsstrukturen. Hochwertige Geräte wie Computer, Laptops oder Smartphones gehören zu den wertvollsten und zugleich mobilsten Produkten im Einzelhandel. Ihr hoher Wiederverkaufswert, ihre geringe Größe und ihre leichte Transportierbarkeit machen sie zu einem bevorzugten Ziel organisierter Diebstahlstrukturen. Händler reagieren darauf mit immer umfassenderen Dokumentationsmechanismen.

Im Zentrum dieser Strategie stehen die Seriennummern moderner Geräte. Jedes elektronische Produkt besitzt heute eine eindeutige Identifikation. Diese Seriennummer macht ein Gerät technisch unverwechselbar und ermöglicht es, seine Existenz über Jahre hinweg nachzuverfolgen. Beim Verkauf wird diese Kennung häufig mit dem Kaufvorgang verknüpft. Für Händler entsteht dadurch eine Form der Kontrolle über den Lebenszyklus eines Produkts. Wird ein Gerät später als gestohlen gemeldet oder taucht es in einer Reklamation auf, lässt sich rekonstruieren, wann es verkauft wurde und unter welchen Umständen der Verkauf stattfand.

Der Kauf hinterlässt damit eine digitale Spur, die weit über den eigentlichen Moment der Transaktion hinausreicht.

Hinzu kommt ein weiteres Problem des Handels: Rückgabebetrug. Immer wieder versuchen Betrüger, gestohlene oder manipulierte Geräte gegen neue Ware umzutauschen oder Reklamationen für Produkte einzureichen, die nie im entsprechenden Geschäft gekauft wurden. Durch die Dokumentation von Verkaufsdaten versuchen Händler, solche Vorgänge zu kontrollieren und wirtschaftliche Schäden zu begrenzen. Auch Garantiesysteme spielen dabei eine Rolle. Elektronikprodukte werden über Jahre hinweg genutzt, repariert oder ersetzt, weshalb Händler zunehmend daran interessiert sind, den Ursprung eines Gerätes eindeutig nachvollziehen zu können.

Doch diese Praxis ist nur die sichtbare Oberfläche eines deutlich größeren Wandels.

Sie fügt sich in eine globale Transformation ein, die seit einigen Jahren unter Begriffen wie Nachhaltigkeit, Kreislaufwirtschaft und digitaler Nachverfolgbarkeit von Ressourcen diskutiert wird. Programme wie die Agenda 2030 der Vereinten Nationen formulieren das Ziel, wirtschaftliche Prozesse grundlegend neu zu organisieren. Ressourcen sollen effizienter genutzt, Produktionsketten transparenter gestaltet und Konsummuster besser steuerbar werden.

Ein zentrales Element dieser Vision ist die lückenlose Dokumentation von Produkten über ihren gesamten Lebenszyklus hinweg. Ein Gegenstand soll nicht mehr einfach produziert, verkauft und irgendwann entsorgt werden. Stattdessen soll er digital verfolgt werden können – von der Herstellung über den Verkauf bis zur Nutzung, Reparatur und Wiederverwertung. Jedes Produkt erhält damit eine Art digitale Biografie.

Wenn Produkte eindeutig identifizierbar sind und Verkaufsdaten systematisch erfasst werden, lassen sich Materialströme, Besitzverhältnisse und Nutzungszyklen präzise analysieren. Diese Informationen bilden die Grundlage für das Konzept der sogenannten Kreislaufwirtschaft, in der Ressourcen nicht mehr linear verbraucht, sondern dauerhaft im Umlauf gehalten werden sollen.

Parallel dazu haben sich im globalen Finanzsystem neue Bewertungsmodelle etabliert, die unter dem Begriff ESG-Kriterien bekannt sind – Environmental, Social und Governance. Unternehmen werden zunehmend danach beurteilt, wie nachhaltig sie wirtschaften, wie transparent ihre Lieferketten sind und wie effizient sie mit Ressourcen umgehen. Auch die Nachverfolgbarkeit von Produkten spielt in diesen Bewertungen eine wachsende Rolle.

In diesem Kontext taucht ein weiterer Gedanke immer häufiger auf: die Verschiebung vom klassischen Besitz hin zur Nutzung. Produkte sollen künftig nicht mehr zwingend dauerhaft verkauft werden, sondern zunehmend als Dienstleistung bereitgestellt werden. Leasingmodelle, Mietsysteme oder Sharing-Strukturen sollen Geräte länger im Umlauf halten und Ressourcen effizienter nutzen.

Der Gedanke dahinter ist einfach: Wenn weniger Menschen Dinge besitzen, aber weiterhin Zugang zu ihnen haben, können Ressourcen besser verwaltet werden.

In wirtschaftlichen Diskussionen wurde diese Idee gelegentlich mit einer provokanten Formel beschrieben: In Zukunft könnten Menschen weniger besitzen und dennoch zufrieden sein. Unabhängig davon, wie man diese Vision politisch bewertet, lässt sich eine Entwicklung beobachten, die kaum noch zu übersehen ist.

Der klassische Kaufakt verändert sich.

Was früher ein einfacher Tausch war – Geld gegen Ware – wird zunehmend zu einem Vorgang, bei dem Identität, Daten und Nutzung miteinander verschmelzen. Käufer gewöhnen sich Schritt für Schritt daran, persönliche Informationen preiszugeben, Geräte zu registrieren und digitale Konten zu verwenden, um Produkte überhaupt nutzen zu können.

Besonders deutlich zeigt sich diese Entwicklung in der wachsenden Abhängigkeit moderner Geräte von Cloud-Systemen. Elektronik funktioniert immer seltener als vollständig eigenständiges Produkt. Stattdessen wird sie an Onlinekonten und zentrale Server gebunden.

Ein bekanntes Beispiel für diese Entwicklung ist das Ökosystem von Apple. iPhones, iPads oder Mac-Computer sind eng mit der sogenannten Apple-ID verknüpft. Ohne diese digitale Identität lassen sich viele Funktionen nicht aktivieren oder nutzen. Geht der Zugriff auf dieses Konto verloren oder kann der Besitzer seine Identität nicht mehr bestätigen, kann das Gerät im Extremfall nicht mehr aktiviert werden und wird faktisch zu einem funktionslosen Gegenstand.

Ähnliche Strukturen finden sich inzwischen auch im Ökosystem von Microsoft. Computer werden heute bereits mit Windows 11 ausgeliefert, das bei der Ersteinrichtung die Anmeldung mit einer Microsoft-ID verlangt. Diese digitale Identität wird zunehmend zur Voraussetzung für bestimmte Funktionen des Betriebssystems, für Cloud-Dienste, Softwarelizenzen oder Synchronisationsdienste. Auch hier verschiebt sich damit schrittweise die Kontrolle: Der Nutzer besitzt zwar das physische Gerät, doch zentrale Funktionen sind an ein Onlinekonto und die Infrastruktur des Herstellers gebunden.

Dieses Prinzip beschränkt sich jedoch längst nicht mehr auf Apple oder Microsoft. Auch Hersteller wie Samsung sowie zahlreiche Anbieter sogenannter „smarter“ Geräte verfolgen ähnliche Modelle. Saugroboter, Kameras, Fernseher oder Smart-Home-Systeme funktionieren oft nur noch in Verbindung mit einer registrierten Nutzeridentität und einer Cloud-Infrastruktur. Der Käufer erwirbt zwar die physische Hardware, doch zentrale Funktionen bleiben an digitale Konten und Server gebunden.

Dass solche Systeme reale Risiken bergen, hat sich bereits mehrfach gezeigt. In den vergangenen Jahren brachten mehrere Unternehmen vernetzte Geräte auf den Markt – etwa E-Bikes, Saugroboter oder Smart-Home-Produkte –, deren Betrieb vollständig von einer Cloud-Infrastruktur abhängig war. Diese Geräte konnten nur über Apps oder über eine Verbindung zu den Servern des Herstellers aktiviert werden.

Solange das Unternehmen existierte, funktionierten die Produkte. Meldete die Firma jedoch Insolvenz an oder stellte ihre Dienste ein, verschwand auch die technische Infrastruktur. Die Folge war drastisch: Geräte, die Käufer rechtmäßig erworben hatten, ließen sich plötzlich nicht mehr nutzen. E-Bikes konnten nicht mehr entsperrt werden, Staubsaugerroboter verloren zentrale Funktionen, Smart-Home-Systeme wurden unbrauchbar.

Der Besitzer hatte zwar die Hardware bezahlt – doch die Kontrolle über ihre Funktion lag weiterhin bei der digitalen Infrastruktur eines Unternehmens.

Genau hier beginnt eine Entwicklung, deren Konsequenzen weit über einzelne Produkte hinausreichen.

Wenn immer mehr Geräte unseres Alltags dauerhaft mit Cloud-Systemen, Identitätskonten und zentralen Plattformen verbunden sind, verschiebt sich die Kontrolle über diese Technologien zunehmend weg vom Besitzer und hin zu den Betreibern der jeweiligen Infrastruktur.

Kommt es zusätzlich zu politischen Veränderungen oder neuen Regulierungssystemen, könnten solche technischen Strukturen eine völlig neue Bedeutung erhalten. In einer Welt, in der Geräte zentral gesteuert werden können, besteht grundsätzlich auch die Möglichkeit, Funktionen aus der Ferne einzuschränken oder zu deaktivieren.

Die Dynamiken, die sich aus einer solchen Infrastruktur ergeben, sind weitreichend. Technologien, die heute mit dem Versprechen von Komfort, Effizienz und Vernetzung eingeführt werden, können in anderen politischen Konstellationen ganz andere Funktionen erhalten. Politische Systeme verändern sich, Machtstrukturen verschieben sich – doch technologische Infrastruktur bleibt bestehen.

Mit der zunehmenden Digitalisierung wächst zugleich eine enorme Menge an Daten. Nutzungsverhalten, Geräteaktivitäten, Standortinformationen oder technische Diagnosedaten werden kontinuierlich an Server übertragen und ausgewertet. Die Kontrolle über solche Datenströme eröffnet Unternehmen neue Möglichkeiten der Marktanalyse, kann aber auch für staatliche Strukturen von erheblichem Interesse sein.

Auch im Drucker- und Zubehörmarkt sind solche Mechanismen bereits verbreitet. Einige Hersteller koppeln Geräte an Benutzerkonten oder verlangen Onlineverbindungen, um Funktionen freizuschalten oder Verbrauchsmaterial zu verwalten. Gleichzeitig entwickeln Softwareplattformen und Betriebssysteme immer umfangreichere Nutzungsbedingungen und Community-Richtlinien. Diese Regelwerke betreffen nicht nur Online-Dienste, sondern können auch Auswirkungen auf Geräte haben, die sich im Besitz der Nutzer befinden. In extremen Fällen eröffnen solche Strukturen theoretisch die Möglichkeit, Funktionen zu deaktivieren oder den Zugriff auf bestimmte Dienste einzuschränken.

Die langfristige Perspektive solcher Systeme wirft grundlegende Fragen über Eigentum, Kontrolle und digitale Souveränität auf. Wenn Geräte dauerhaft an Cloud-Systeme, Benutzerkonten und externe Server gebunden sind, besitzt der Käufer zwar die physische Hardware – jedoch nicht zwangsläufig die vollständige Kontrolle über deren Funktion.

Genau an dieser Stelle stellt sich eine entscheidende Frage: Wie sinnvoll ist es, Geräte zu erwerben, deren Nutzung dauerhaft an eine externe Infrastruktur gekoppelt ist? Denn in dem Moment, in dem ein Unternehmen Insolvenz anmeldet, seine Server abschaltet oder seine Dienste einstellt, kann ein zuvor voll funktionsfähiges Gerät innerhalb kürzester Zeit unbrauchbar werden. Noch problematischer wird diese Abhängigkeit, wenn man bedenkt, dass technische Infrastrukturen grundsätzlich auch von politischen oder staatlichen Strukturen beeinflusst werden können. In Szenarien, in denen staatliche Eingriffe oder autoritäre Entwicklungen eine Rolle spielen, könnten zentral gesteuerte Systeme theoretisch auch genutzt werden, um Funktionen aus der Ferne einzuschränken oder Geräte vollständig zu deaktivieren.

Der Kauf eines Computers oder eines anderen technischen Gerätes ist damit längst nicht mehr nur eine wirtschaftliche Handlung. Er wird zunehmend zu einem Eintrittspunkt in eine digitale Infrastruktur, in der Produkte, Daten, Identitäten und wirtschaftliche Prozesse miteinander verschmelzen.

Der Käufer steht deshalb nicht mehr ausschließlich vor einem Regal voller Elektronikprodukte. Er bewegt sich innerhalb eines Systems, dessen Nutzung an digitale Identitäten, Plattformen und Nutzungsbedingungen gebunden ist – Bedingungen, die nicht vom Käufer selbst festgelegt werden, sondern von den Betreibern der jeweiligen Infrastruktur.