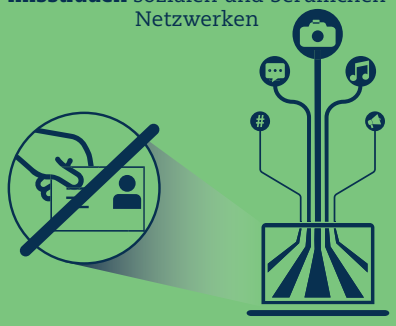
Kapitel 7

VERTRAUEN STÄRKEN

Fast 30% der **Internetnutzer misstrauen** sozialen und beruflichen Netzwerken



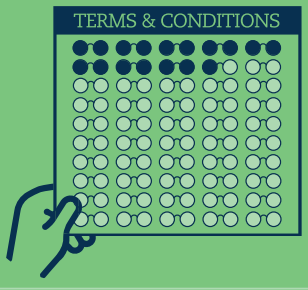
Bedenken über digitale Sicherheit, Daten- und Verbraucherschutz ausräumen, um das Vertrauen zu stärken

Jeder vierte Internetnutzer in der Europäischen Union ist **besorgt über die Zahlungssicherheit**

Alle Nutzer befähigen, digitale Sicherheitsrisiken zu beurteilen und besser zu steuern

VERTRAUEN

Nur 17% der Nutzer von Peer-to-Peer-Plattformen **lesen die Allgemeinen Geschäftsbedingungen** in voller Länge



Wirksamere Maßnahmen zum Schutz der Verbraucher im Internet entwickeln und umsetzen

Die meisten **Datenschutzmaßnahmen** zielen darauf ab, den **Einzelnen** zu sensibilisieren und **zu stärken**

Nationale Datenschutzstrategien mit gesamtgesellschaftlicher Perspektive entwickeln und umsetzen

VERTRAUEN STÄRKEN: WO LIEGEN DIE PRIORITÄTEN FÜR DIE POLITIK?

Durch Risikomanagement Vertrauen herstellen

- Vertrauensfördernde Politikmaßnahmen auf Basis eines Risikomanagementansatzes entwickeln – u.a. um die mit Technologien, Daten und grenzüberschreitenden Aktivitäten zusammenhängenden Risiken zu beurteilen und zu steuern.
- Kleinen und mittleren Unternehmen (KMU) durch öffentliche und private Anstrengungen zur stärkeren Sensibilisierung und Förderung empfehlenswerter Verfahrensweisen für das Risikomanagement dabei helfen, die Chancen der Digitalisierung zu nutzen.

Robuste, inklusive und interoperable Datenschutzregelungen entwickeln

- Datenschutzregelungen ermöglichen den freien Verkehr personenbezogener Daten und fördern dadurch das Wachstum und den gesellschaftlichen Wohlstand. Es bedarf Maßnahmen, die die Transparenz bezüglich des Zwecks und der Nutzung personenbezogener Datenbestände erhöhen und den Nutzern den Zugang zu ihren Daten sowie die Kontrolle darüber erleichtern. Technische Lösungen können durch „Privacy by design“ (Datenschutz durch Technikgestaltung) zur Stärkung des Vertrauens beitragen.
- Die nationalen Datenschutzpolitiken sollten auf höchster staatlicher Ebene unterstützt werden und eine gesamtgesellschaftliche Perspektive einnehmen. Gegenwärtig zielt über die Hälfte der Datenschutzmaßnahmen in den OECD-Ländern darauf ab, den Einzelnen zu sensibilisieren und zu stärken.
- Die Interoperabilität von Datenschutzregelungen in den verschiedenen Staaten fördern, u.a. durch nationale Datenschutzstrategien und andere praktische Ansätze.

Digitale Sicherheitsrisiken steuern (anstatt zu versuchen, sie zu beseitigen)

- Die Sorgen über digitale Sicherheitsrisiken – u.a. durch Cyberattacken – nehmen zu und halten nahezu 30% der Internetnutzer davon ab, personenbezogene Daten in sozialen oder beruflichen Online-Netzwerken preiszugeben. Jeder vierte Nutzer in der Europäischen Union ist zudem besorgt bezüglich der Sicherheit von Zahlungen im Internet.
- Digitale Sicherheit muss für jeden Einzelnen ebenso wie für Unternehmen und Regierungen eine strategische Priorität sein und darf nicht nur als technische Frage betrachtet werden. Die Steuerung digitaler Sicherheitsrisiken ist Aufgabe jedes einzelnen Internetnutzers.

Verbraucher in der zusammenwachsenden Online- und Offline-Welt schützen

- Die Herausforderungen für Verbraucher im digitalen Umfeld sind vielfältig. Sie betreffen u.a. die Offenlegung von Daten, irreführendes und unlauteres Geschäftsgebaren, die Bestätigung und Bezahlung von Einkäufen, Betrug und Identitätsdiebstahl, die Produktsicherheit sowie die Beilegung von Streitigkeiten und die Rechtsdurchsetzung. Dies gilt auch für die Nutzung vernetzter Geräte, bei denen die Grenzen zwischen Offline- und Online-Aktivitäten verschwimmen.
- Allgemeine Geschäftsbedingungen sind kein wirksames Mittel, um Verbraucher über wichtige Sachverhalte aufzuklären. So lesen nur 17% der Nutzer die Allgemeinen Geschäftsbedingungen von Peer-to-Peer-Plattformen (wie Airbnb und BlaBlaCar) in voller Länge. Um die Verbraucher online zu schützen, bedarf es anderer Ansätze.

Privatpersonen, Unternehmen und Regierungen müssen darauf vertrauen können, dass es ihnen mehr Vor- als Nachteile bringt, digitale Umgebungen für ihre sozialen und wirtschaftlichen Aktivitäten zu nutzen. Nur dann werden sie in vollem Umfang am digitalen Wandel teilhaben und davon profitieren. Nachteile können aus verschiedenen Unsicherheitsfaktoren resultieren, die bei digitalen Technologien, Daten und grenzüberschreitenden Aktivitäten bestehen. Viele davon hängen mit potenziellen Cyberangriffen zusammen (die sich z.B. gegen die Verfügbarkeit, Integrität oder Vertraulichkeit von Daten, Systemen oder Netzwerken richten können). Andere Nachteile ergeben sich aus Informationsasymmetrien, Machtungleichgewichten oder Fragen der staatlichen Zuständigkeit, die im digitalen Umfeld verstärkt auftreten. Sie können sich in Verstößen gegen Gesetze und sonstige Vorschriften äußern, mit denen derartige Ungleichgewichte und Herausforderungen verringert werden sollen, wie z.B. Datenschutz-, Verbraucherschutz- oder Produktsicherheitsbestimmungen. Vertrauen lässt sich nur dann erreichen, wenn solche Unsicherheiten weitmöglichst verringert werden.

Durch Risikomanagement Vertrauen herstellen

Unerwünschte Vorkommnisse wie der Diebstahl von Wirtschaftsgütern, Identitätsdiebstahl oder der Missbrauch personenbezogener Daten können sich negativ auf die Reputation, finanzielle Lage, Freiheit, Autonomie, Gesundheit, Lebensqualität, Sicherheit, Wettbewerbsfähigkeit bzw. Effizienz der Betroffenen auswirken. Dadurch sinkt ihre Bereitschaft, digitale Umgebungen umfassend zu nutzen. Auch die Funktionstüchtigkeit unserer Gesellschaft kann Schaden nehmen, da kritische Infrastrukturen und grundlegende Dienstleistungen etwa in den Bereichen Energie, Finanzen und Verkehr durch Cyberangriffe beeinträchtigt werden können.

In der Praxis ist es am effektivsten, derartigen Unsicherheiten durch Risikomanagement zu begegnen. Da sich die Unsicherheiten nicht vollständig beseitigen lassen, muss ein gewisses Risiko akzeptiert werden. Anders ausgedrückt: Das digitale Risiko muss auf ein Niveau gesenkt werden, das vor dem Hintergrund der angestrebten Zielsetzungen und Vorteile akzeptabel ist. Dies setzt voraus, dass wir lernen, Risiken zu beurteilen und zu steuern. Letztlich müssen wir entscheiden, ob wir Risiken akzeptieren, verringern, übertragen oder vermeiden. Letzteres würde bedeuten, auf digitale Aktivitäten zu verzichten.

7.1 Was ist Vertrauen?

Vertrauen kommt in vielen Lebensbereichen zum Tragen – Vertrauen in politische Institutionen, Regierungen, Statistiken, Rechtsstaatlichkeit (institutionelles Vertrauen) oder Vertrauen in andere Menschen (interpersonales Vertrauen) (vgl. Kapitel 6). Zwar gibt es keine allgemeingültige Definition von Vertrauen, die OECD definiert Vertrauen jedoch als „Glaube einer Person daran, dass eine andere Person oder Institution ihren Erwartungen eines positiven Verhaltens entsprechen wird". Zur besseren Messung des Vertrauens hat die OECD Leitlinien für die nationalen statistischen Ämter herausgegeben (OECD, 2017[1]) und experimentelle Arbeiten durchgeführt (Murtin et al., 2018[2]).

Durch den digitalen Wandel erhält das Konzept des Vertrauens für den Einzelnen, die Gesellschaft und die Volkswirtschaft eine neue Dimension. In diesem Kapitel wird Vertrauen unter dem Aspekt der Unsicherheiten und Interdependenzen betrachtet (Mayer, Davis und Schoorman, 1995[3]), die durch digitale Umgebungen entstehen. Vertrauen in digitale Umgebungen ist kontextabhängig und variiert je nachdem, welche Chancen und Herausforderungen die jeweilige Situation mit sich bringt.

Für den Einzelnen geht es beim Vertrauen im digitalen Zeitalter um die Bereitschaft, Zeit, Geld und persönliche Daten bei geschäftlichen und sozialen Aktivitäten einzusetzen, und sich dadurch verwundbar zu machen, beispielsweise wenn es Probleme bei einem Einkauf gibt oder persönliche Daten gestohlen oder dazu missbraucht werden, das Verhalten der betreffenden Person zu beobachten, sie zu diskriminieren oder ihre Persönlichkeitsrechte zu verletzen. Für Unternehmen und andere Organisationen bedeutet Vertrauen auch, ein gewisses Risiko durch mögliche Gefährdungen der digitalen Sicherheit, des Daten- oder Verbraucherschutzes oder sonstige Bedrohungen in Kauf zu nehmen, um die Vorteile des digitalen Wandels zu nutzen. Vertrauen ist daher eine entscheidende Voraussetzung, um das Wachstumspotenzial und den sozialen Fortschritt im digitalen Zeitalter voll auszuschöpfen.

Digitales Risikomanagement ist ein Thema, das Privatpersonen ebenso betrifft wie größere Organisationseinheiten – von kleineren bis hin zu Großunternehmen und öffentlichen Stellen. Alle Akteure tragen gemäß ihrer Rolle, Handlungsfähigkeit und dem jeweiligen Kontext eine gewisse Verantwortung für die Steuerung der digitalen Risiken ihrer Aktivitäten. Hierfür benötigen sie entsprechende Kompetenzen. Da es sich bei den Risiken um grenz- und sektorübergreifende Belange mit zahlreichen Akteuren handelt, bietet das digitale Risikomanagement einen einheitlichen Bezugsrahmen für die verschiedenen Politikakteure, um Maßnahmen zur Steigerung des Vertrauens auf integrierte und ganzheitliche Art und Weise prüfen zu können. Als Basis dienen die grundlegenden Komponenten eines Risikomanagementzyklus, wie z.B.:

- die Ziele und den Kontext einer Tätigkeit bestimmen und festlegen, welche Risiken in Anbetracht der zu erwartenden Vorteile akzeptabel sind
- die Risiken durch Ermittlung der Risikofaktoren prüfen und ihre Eintrittswahrscheinlichkeit und Schwere bewerten
- die Risiken behandeln, u.a. indem bestimmte Risiken akzeptiert, durch geeignete Maßnahmen auf ein vertretbares Niveau gesenkt, verteilt oder übertragen und/oder gänzlich vermieden werden
- den Risikomanagementzyklus laufend überwachen und prüfen, um bei Bedarf Anpassungen an das sich ständig verändernde Umfeld vorzunehmen

Maßnahmen zur Förderung des digitalen Risikomanagements sind von entscheidender Bedeutung, um das Vertrauen zu steigern und die Bürgerinnen und Bürger, Unternehmen und sonstigen Stellen zu befähigen, ihre wirtschaftlichen und sozialen Ziele weitmöglichst zu verwirklichen. Zwar dürfte das praktische Risikomanagement je nach Zielsetzung – Cybersicherheit, Daten- bzw. Verbraucherschutz oder Produktsicherheit – unterschiedlich ausfallen, Politikmaßnahmen müssen jedoch den möglichen Wechselwirkungen zwischen den verschiedenen Risikokategorien Rechnung tragen. Maßnahmen zur Steuerung der digitalen Risiken sollten den jeweiligen Risiken angemessen sein und auf die Ziele der betroffenen Akteure abgestimmt sein. Für den Einzelnen eignen sich dabei möglicherweise andere Maßnahmen als für ein großes privatwirtschaftliches Unternehmen, selbst wenn dieselben Ziele verfolgt werden.

Im Unternehmenssektor sollten Start-ups und KMU besondere Aufmerksamkeit erhalten, da sie nicht nur eine Schlüsselrolle für die Wirtschaft spielen, sondern auch nur begrenzt in der Lage sind, größeren Angriffen standzuhalten und die digitalen Risiken effektiv zu steuern. KMU, und vor allem Start-ups in der Frühphase, spielen eine entscheidende Rolle für das Wirtschaftswachstum. Sie sorgen für Wettbewerb, Innovationen und neue Arbeitsplätze. Allerdings stehen sie bei der Steuerung digitaler Risiken auch vor besonderen Herausforderungen. So ist ein Cyberangriff, der zu einem Vertrauensverlust bei den Verbrauchern, Reputationsschäden oder Umsatzrückgängen führt, für KMU u.U. schädlicher als für größere Unternehmen, weil sie vorübergehende Einnahmeausfälle möglicherweise schwerer verkraften können.

In der Regel mangelt es KMU zudem an Problembewusstsein, Mitteln und Fachkompetenz, um die Risiken effektiv zu bewerten und zu steuern. Positiv ist wiederum, dass ihnen die Sensibilisierung für digitale Risiken und ein solides Risikomanagement Wettbewerbsvorteile verschaffen können, wenn sie Partnerschaften mit größeren Unternehmen anstreben. Damit die KMU diese Chancen wahrnehmen können und weder die KMU noch ihre Geschäftspartner durch ungesteuerte Risiken in Gefahr gebracht werden, ist es von grundlegender Bedeutung, das Problembewusstsein zu erhöhen und empfehlenswerte Vorgehensweisen zu fördern.

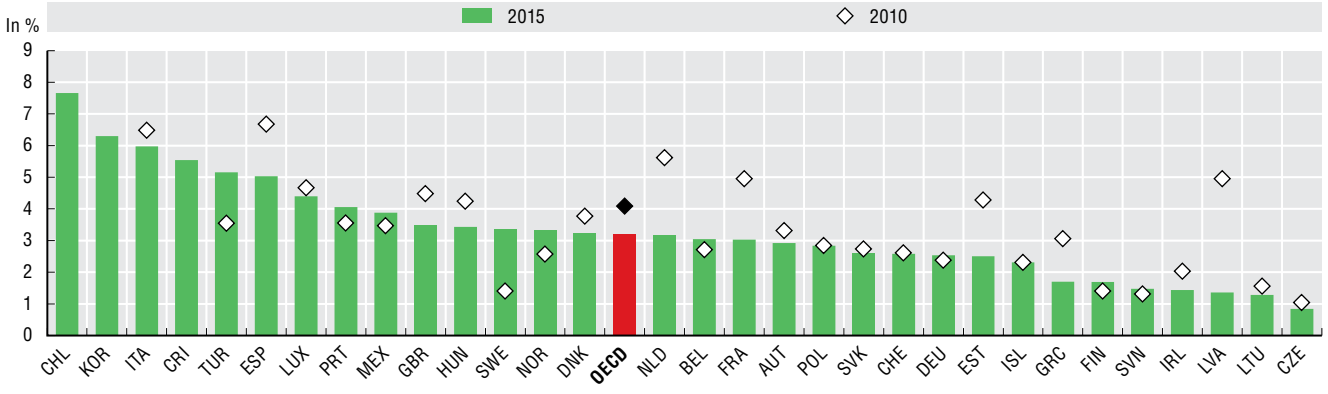
Robuste, inklusive und interoperable Datenschutzregelungen entwickeln

Im Zuge des fortschreitenden digitalen Wandels wird der Schutz der Persönlichkeitsrechte, insbesondere der Schutz personenbezogener Daten, immer stärker zum entscheidenden Faktor für das Vertrauen. Personenbezogene Daten spielen eine zunehmend wichtige Rolle in unseren Volkswirtschaften, Gesellschaften und im Alltag, und neue Technologien und ein verantwortungsvoller Umgang mit Daten führen zu großen gesellschaftlichen und wirtschaftlichen Nutzeffekten. Zugleich hat die Vielfalt an personenbezogenen Daten, die gesammelt, verarbeitet und ausgetauscht werden, die Risiken einer Verletzung der Persönlichkeitsrechte erhöht.

Mit der zunehmenden Erhebung und Speicherung personenbezogener Daten durch Unternehmen, Internetdiensteanbieter und Staaten steigen auch die Datenschutzrisiken. Im Rahmen einer Umfrage gaben im Durchschnitt rd. 3% der Internetnutzer in den OECD-Ländern an, dass ihre Persönlichkeitsrechte in den drei Vormonaten verletzt worden seien (Abb. 7.1), wobei allerdings große Unterschiede zwischen den einzelnen Ländern bestehen. Beispielsweise sahen sich in Chile rd. 7,5% der Befragten von Verletzungen der Persönlichkeitsrechte betroffen, in der Tschechischen Republik hingegen weniger als 1%. Datenschutzverstöße sind eine der Hauptursachen für Verletzungen der Persönlichkeitsrechte, und immer öfter werden digitale Technologien eingesetzt, um personenbezogene Daten durch Abgleich und Auswertung von Datensätzen abzuleiten (OECD, 2017[4]).

7.1 Verletzungen der Persönlichkeitsrechte variieren im Ländervergleich erheblich

Personen, die Verletzungen der Persönlichkeitsrechte erlebten, in Prozent der Internetnutzer, 2015



Anmerkung: Vgl. Kapitelanmerkungen.[1]

Quelle: OECD (2019[5]), *Measuring the Digital Transformation, https://dx.doi.org/10.1787/9789264311992-en*, auf der Grundlage von OECD[6], *ICT Access and Usage by Households and Individuals* (Datenbank), *http://oe.cd/hhind* (Abruf: September 2018).

StatLink https://doi.org/10.1787/888933915411

Personenbezogene Daten werden zunehmend für Zwecke verwendet, die zum Zeitpunkt ihrer Erhebung gar nicht vorgesehen waren. Hierzu zählen auch Nutzungsarten, durch die sensible Informationen ans Licht kommen oder vermeintlich anonyme Daten konkreten Personen zugeordnet werden. In dem Maße, wie die Nutzung und der Wert von Daten zunehmen, häufen sich auch die Verletzungen des Schutzes personenbezogener Daten (OECD, 2017[4]). Diese Risiken haben nicht nur Folgen für die betroffenen Personen, sondern auch für die grundlegenden Werte und Prinzipien, die durch den Schutz der Persönlichkeitsrechte und der personenbezogenen Daten gefördert werden sollen – u.a. das Recht auf Selbstbestimmung, Gleichheit und Meinungsfreiheit –, was weitreichendere Auswirkungen auf die Gesellschaft als Ganzes haben könnte. Daher müssen die Risiken in Bezug auf die Persönlichkeitsrechte und die personenbezogenen Daten besser gesteuert werden, um einen wirksamen Schutz zu gewährleisten.

Der Schutz der Persönlichkeitsrechte ist nicht nur ein anerkannter und schützenswerter Grundwert, sondern auch eine Bedingung für den freien Verkehr personenbezogener Daten über Organisations- und Ländergrenzen hinweg – und damit auch für datengestützte Innovationen, Wirtschaftswachstum und gesellschaftlichen Wohlstand (OECD, 2016[7]). Sowohl im Privatleben als auch im Beruf geben die Menschen heute mehr personenbezogene Daten preis als je zuvor – teils absichtlich in sozialen Netzwerken und andernorts, teils aber auch unwissentlich durch Webtracking oder Smartphones. Folglich dient über die Hälfte der Datenschutzmaßnahmen in den OECD-Ländern dazu, den Einzelnen zu sensibilisieren und zu stärken (OECD, erscheint demnächst[8]). Zugleich möchten die Menschen mehr Sicherheit und Kontrolle im Hinblick auf den Umgang mit ihren Daten: Sie möchten wissen, ob und welche personenbezogenen Daten über sie gesammelt und gespeichert werden, wie diese verwendet werden und ob sie die Daten löschen bzw. korrigieren oder Zweitnutzungen kontrollieren können.

Anders ausgedrückt: Die Menschen möchten wissen, wem sie ihre Daten anvertrauen können. Maßnahmen, die für mehr Transparenz bezüglich der Zwecke und Nutzung personenbezogener Datenbestände sorgen und es den Nutzern erleichtern, auf ihre Daten zuzugreifen und diese zu kontrollieren,

sind für das Vertrauen im digitalen Zeitalter besonders wichtig. Der technische Fortschritt kann durch Privacy by Design (Datenschutz durch Technikgestaltung) zur Stärkung des Vertrauens beitragen, indem Datenschutzfragen gleich bei der Entwicklung eines Produkts oder einer Dienstleistung berücksichtigt werden anstatt erst im Nachhinein. So ließe sich der Datenschutz von vornherein technisch integrieren bzw. einprogrammieren oder die Sammlung personenbezogener Daten auf ein Mindestmaß begrenzen. Angesichts der zunehmenden Verbreitung mobiler Geräte und des Internets der Dinge kann z.B. die Verschlüsselung eine wichtige Rolle für den Datenschutz spielen (OECD, 2017[4]). Eine weitere Reaktion auf Datenschutzbedenken könnte die erneute Dezentralisierung des Internets sein; Grundlage ist eine Reihe von technischen Innovationen, die anstatt einer zentralisierten Speicherung personenbezogener Daten bei einigen wenigen Unternehmen eine verteilte Speicherung bei den Internetnutzern selbst ermöglichen.

Auch wenn Technologie eine positive Rolle dabei spielen kann, Persönlichkeitsrechte und personenbezogene Daten zu schützen, bedarf es nationaler Datenschutzstrategien, die auf höchster Regierungsebene unterstützt werden und eine gesamtgesellschaftliche Perspektive verkörpern, um das richtige Gleichgewicht zwischen den verschiedenen individuellen und kollektiven Interessen zu finden. Diese Strategien sollten klare Vorgaben dafür liefern, gesellschaftlichen und wirtschaftlichen Nutzen aus einer umfassenderen Weiterverwendung und einem besseren Austausch von Daten zu ziehen und zugleich den Bedenken über den Schutz der Persönlichkeitsrechte und personenbezogenen Daten sowie der Rechte des geistigen Eigentums Rechnung zu tragen. Sie würden auch die Interoperabilität der nationalen Regelungen und damit den freien Datenverkehr begünstigen.

Förderung interoperabler Regelungen für den Schutz der Persönlichkeitsrechte und den Datenschutz

Die Länder wenden zwar unterschiedliche Datenschutzregelungen an, streben aber im Großen und Ganzen dieselben Ergebnisse an und verfolgen häufig ähnliche Ansätze, wie die Vereinbarung allgemeiner Leitprinzipien und Regeln guter Praxis bzw. Rechtsvorschriften zeigen. Auch die Notwendigkeit von Mechanismen, die die Interoperabilität zwischen den Regelungen für den Privatsphären- und Datenschutz fördern, wird allgemein anerkannt (OECD, 2016[7]; OECD, 2013[9]). Bestimmungen über die Interoperabilität sollten daher zwar Bestandteil der nationalen Datenschutzstrategien sein, die meisten OECD-Länder haben solche Strategien allerdings noch gar nicht eingeführt (OECD, 2017[4]). Zudem lässt sich die Interoperabilität auch durch andere Maßnahmen sicherstellen.

Regionale Konvergenz und Harmonisierung der Datenschutzregelungen

Zu den Instrumenten mit harmonisierender Wirkung zählen das vor Kurzem aktualisierte Übereinkommen 108 des Europarats, das für die 47 Mitgliedstaaten des Europarats verbindlich ist, aber auch Nichtmitgliedstaaten offensteht. Ein weiteres Beispiel ist die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, mit der die Datenschutzgesetze aller Staaten des Europäischen Wirtschaftsraums harmonisiert wurden. Auch unverbindliche Vereinbarungen können die Konvergenz von Datenschutzgesetzen fördern und einen datenschutzkonformen Datenverkehr erleichtern. Die Asiatisch-Pazifische Wirtschaftskooperation (APEC) hat ein freiwilliges, aber durchsetzbares System grenzüberschreitender Datenschutzregelungen (Cross-Border Privacy Rules – CBPR) eingeführt, das den teilnehmenden APEC-Volkswirtschaften dazu dient, die allgemeinen Datenschutzstandards in der Region zu stärken. Die verschiedenen Ansätze unterscheiden sich durchaus voneinander: So werden beim CBPR-System der APEC Mindeststandards für den Datenschutz aufgestellt, ohne die einzelstaatlichen Gesetze zu ändern, wohingegen die Datenschutz-Grundverordnung der EU die Gesetze durch eine unmittelbar anwendbare Verordnung harmonisiert.

Anerkennung der „Äquivalenz" bzw. der „Angemessenheit" von Datenschutzmaßnahmen

Die für den Daten- und Privatsphärenschutz zuständigen nationalen Behörden können zertifizieren, dass die Datenschutzprinzipien anderer Staaten einen angemessenen bzw. den inländischen Datenschutzregelungen entsprechenden Schutz bieten. So gestattet beispielsweise Artikel 45 der DSGVO die Übermittlung personenbezogener Daten aus der Europäischen Union an Drittländer, deren Schutzniveau als angemessen betrachtet wird – wie z.B. Israel und Neuseeland. Andere mögliche Maßnahmen sind Musterverträge, verbindliche Unternehmensregelungen für multinationale Unternehmen und Zertifizierungsmechanismen, die die grenzüberschreitende Übermittlung von Daten gestatten und den Personen, deren Daten übermittelt werden, zugleich rechtswirksamen Schutz bieten. Ein Beispiel

für einen solchen Zertifizierungsmechanismus ist der zwischen der EU und den Vereinigten Staaten vereinbarte Schutzschild für die Privatsphäre (Privacy Shield), der den teilnehmenden Unternehmen die Übertragung von Daten zwischen den beiden Wirtschaftsräumen gestattet, nachdem sie sich rechtswirksam dazu verpflichtet haben, einen Grundsatzkatalog einzuhalten, der mit den Datenschutzbestimmungen der EU im Einklang steht.

Grenzüberschreitende Zusammenarbeit zwischen Datenschutzbehörden

Durch gemeinsam vereinbarte allgemeine Grundsätze, wie etwa jene in der *OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy* (OECD, 2007[23]), lässt sich gewährleisten, dass die Datenschutzbehörden personenbezogene Daten unabhängig davon, wo sie sich befinden, nach einheitlichen Kriterien schützen. Die Teilnahme an Foren wie dem Global Privacy Enforcement Network, das Informationsaustausch und Zusammenarbeit ermöglicht und auch schon zu einigen gemeinsamen Initiativen geführt hat, und bilaterale Zusammenarbeit zwischen Datenschutzbehörden sind ebenfalls hilfreich, um die grenzüberschreitende Zusammenarbeit zu verbessern. Durch effektive Interoperabilitätsmechanismen wird die Bedeutung der Zusammenarbeit und der grenzüberschreitenden Rechtsdurchsetzung zusätzlich unterstrichen. Damit eine Volkswirtschaft beispielsweise an dem CBPR-Mechanismus der APEC teilnehmen kann, muss sie auch die Regeln der APEC für die Zusammenarbeit bei der Durchsetzung verbindlich anwenden. Andere Formen der Zusammenarbeit sind z.B. Grundsatzvereinbarungen und Vereinbarungen über die Weitergabe von Daten (Casalini und López González, 2019[8]).

Regionale Handelsabkommen

Fragen der Datenübermittlung werden zunehmend auch in bilateralen bzw. regionalen Handelsabkommen berücksichtigt, deren Datenschutzbestimmungen in der Regel dazu dienen, den grenzüberschreitenden Datenverkehr zu erleichtern. So ist beispielsweise im USA-Mexiko-Kanada-Abkommen (Art. 19 Abs. 8) – das noch nicht von den Gesetzgebern ratifiziert wurde – die Einführung bzw. Beibehaltung eines Rechtsrahmens vorgesehen, der den Schutz personenbezogener Daten regelt. Gleichzeitig wird darauf hingewiesen, dass keine Vertragspartei die grenzüberschreitende Übermittlung von Daten beschränken sollte – mit begrenzten Ausnahmen, die der Verwirklichung ihrer legitimen Politikziele dienen (Art. 19 Abs. 11) (Casalini und López González, 2019[10]).

Maßnahmen für Unternehmen und Rechtsträger in Staaten, die die Datenschutzsysteme anderer Staaten nicht anerkennen

Die Datenschutz-Grundverordnung der EU sieht vor, dass multinationale Unternehmen „verbindliche interne Datenschutzvorschriften" in allen Mitgliedern der Unternehmensgruppe umsetzen müssen, um die Übermittlung von Daten zwischen ihnen zu ermöglichen – selbst dann, wenn die Mitglieder der Unternehmensgruppe ihren Sitz in Staaten haben, die keine spezifischen Mechanismen eingerichtet oder Vereinbarungen getroffen haben. Dies ist ein praktisches Beispiel dafür, wie Datenschutzregeln für Länder funktionieren können, die die Datenschutzgesetze anderer Staaten nicht anerkennen. Einige Datenschutzbehörden haben zudem Standardvertragsklauseln ausgearbeitet, die in jedem Vertrag bzw. in jeder Vereinbarung verwendet werden können, die die Übermittlung von Daten zwischen Unternehmen in Staaten zum Gegenstand haben, die ihre Regelungen im Bereich des Datenschutzes bzw. der Persönlichkeitsrechte gegenseitig nicht anerkennen. Manche Unternehmen vertreten allerdings die Auffassung, dass solche Klauseln belastende Verpflichtungen enthalten und zu einem hohen Verwaltungsaufwand führen können (Casalini und López González, 2019[10]).

Digitale Sicherheitsrisiken steuern (anstatt zu versuchen, sie zu beseitigen)

Ein wichtiges Thema im Zusammenhang mit dem digitalen Wandel ist die Gefahr von Cyberattacken. Um die Beeinträchtigung wirtschaftlicher und sozialer Aktivitäten durch solche Angriffe zu verringern, müssen die Resilienz und Cybersicherheit verbessert werden. Bei Cyberangriffen wird die globale Reichweite des Internets ausgenutzt, um eine rasche Ausbreitung über Staats-, Organisations- und Sektorgrenzen hinweg zu erreichen, wie Wannacry, NotPetya und Dyn unlängst gezeigt haben. Cyberangriffe können die Tätigkeiten aller Unternehmen – vom KMU bis zum Großunternehmen –, Staaten und Bürger beeinträchtigen und Finanz- und Reputationsschäden verursachen. So sorgte etwa NotPetya bei mehreren weltweit tätigen Unternehmen für vorübergehende Produktionsausfälle. Merck beispielsweise musste

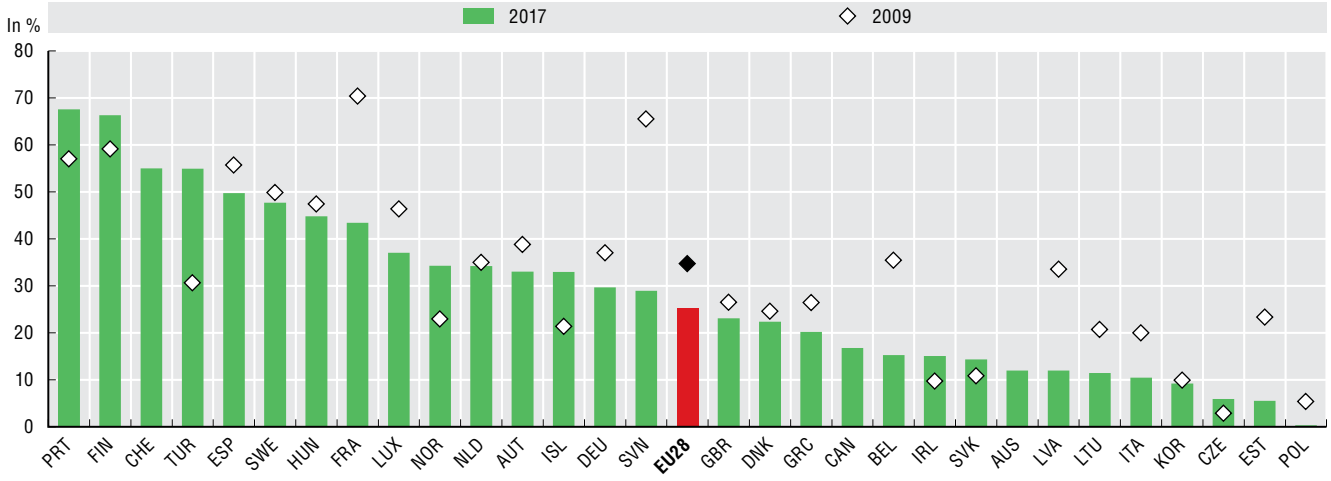
sich seinen eigenen Impfstoff aus Vorräten des Center for Disease Control and Prevention der Vereinigten Staaten besorgen, um Kundenaufträge zu erfüllen, wodurch sich der Quartalsumsatz des Unternehmens um 240 Mio. USD verringerte (Merck, 2017[11]; Hufford und Loftus, 2017[12]).

Diese Attacken können auch Sachschäden verursachen, wie ein Cyberangriff im Jahr 2015 zeigte, der in der Ukraine bei rd. 225 000 Kunden zu Stromausfällen führte (NCCIC, 2016[13]; Popescu und Secrieru, 2018[14]). Derartige Angriffe könnten sich zu umfassenden Krisen ausweiten, bei denen kritische Infrastrukturen beeinträchtigt werden, die für die Funktionsfähigkeit von Wirtschaft und Gesellschaft wesentlich sind, z.B. Finanz-, Energie- und Verkehrsinfrastrukturen und grundlegende staatliche Dienstleistungen. Abgesehen von solchen Katastrophenszenarien können Cyberangriffe auch eine subtile, aber langfristige negative Wirkung haben, indem sie das Vertrauen in digitale Infrastrukturen beeinträchtigen, die Innovationstätigkeit einschränken, die Einführung neuer Technologien verlangsamen und den digitalen Wandel behindern, sodass die damit verbundenen Vorteile nicht voll zum Tragen kommen können.

Das Risiko von Cyberangriffen nimmt mit fortschreitendem digitalen Wandel zu. Bedenken in Bezug auf digitale Sicherheit halten nahezu 30% der Internetnutzer davon ab, persönliche Daten in sozialen oder beruflichen Online-Netzwerken preiszugeben (OECD, 2017[4]). In vielen Ländern besteht nach wie vor weit verbreitete Besorgnis bezüglich der Sicherheit von Zahlungen und des Datenschutzes. Im Jahr 2017 äußerten über die Hälfte der Internetnutzer in Portugal (68%), Finnland (66%), der Schweiz (55%) und der Türkei (55%) entsprechende Bedenken (Abb. 7.2). Am wenigsten besorgt zeigten sich die Internetnutzer in Polen (unter 1%), Estland (6%), der Tschechischen Republik (6%) und Korea (9%).

7.2 Sorgen über die Zahlungssicherheit und den Datenschutz schrecken immer noch viele Nutzer ab

Personen, die aufgrund von Zahlungssicherheits- oder Datenschutzbedenken nicht online einkaufen, in Prozent der Internetnutzer, die zuletzt vor über einem Jahr oder noch nie Waren oder Dienstleistungen im Internet bestellt haben, 2017



Anmerkung: Vgl. Kapitelanmerkungen.[2]

Quelle: OECD-Berechnungen auf der Grundlage von Eurostat[15], *Digital Economy and Society Statistics* (Datenbank), *https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database;* nationale Quellen (Abruf: Dezember 2018).

StatLink https://doi.org/10.1787/888933914917

Es ist unmöglich, vollkommen sichere digitale Umgebungen zu schaffen. Unternehmen, sonstige Organisationen und Privatpersonen gehen also immer ein gewisses Sicherheitsrisiko ein, wenn sie digitale Technologien nutzen. Daher sollten sie sich damit auseinandersetzen, wie sie die Risiken dieser Technologien steuern können, ohne den mit ihnen verbundenen wirtschaftlichen und gesellschaftlichen Nutzen zu schmälern. Dies kann beispielsweise die Umsetzung von Sicherheitsstandards umfassen (z.B. die ISO-27000-Reihe), um die Resilienz zu erhöhen und die Unternehmenskontinuität zu wahren, indem die Folgen eventueller Cyberangriffe abgeschwächt werden. Aufgrund der gegenseitigen Abhängigkeiten aller Akteure im digitalen Umfeld – auch grenzüberschreitend – sind Partnerschaften zwischen den Akteuren entscheidend, um die Risiken zu verringern und empfehlenswerte Risikomanagementpraktiken zu fördern. Dabei sollten vor allem Informationen über Bedrohungen, Gefährdungen, Angriffe und Risikomanagementpraktiken ausgetauscht und auch KMU miteinbezogen werden.

Politikmaßnahmen zur Förderung der digitalen Sicherheit können in diesem Zusammenhang eine wichtige Rolle spielen. Sie können die Voraussetzungen dafür schaffen, dass Organisationen Risikomanagementkonzepte für digitale Risiken einführen, dass Unternehmen weniger störanfällige und sicherere Technologien entwickeln und dass die Menschen die Risiken besser verstehen und digitale Geräte verantwortungsvoller nutzen. Durch Politikmaßnahmen ließe sich außerdem den zunehmenden Kompetenzengpässen im Bereich der digitalen Sicherheit entgegenwirken, die neben Fachkräften für digitale Sicherheit auch Führungskräfte betreffen. Zudem könnten entsprechende Maßnahmen die Innovationstätigkeit auf diesem Gebiet fördern und eine dynamische digitale Sicherheitsindustrie aufbauen helfen. Cyberversicherungen können ein wichtiger Bestandteil des Risikomanagements sein, da sie die Übertragung bestimmter digitaler Sicherheitsrisiken ermöglichen und Anreize für eine bessere Risikomanagementpraxis schaffen.

Cybersicherheit und die Resilienz kritischer Infrastrukturen und Dienstleistungen, die die Funktionsfähigkeit von Wirtschaft und Gesellschaft gewährleisten, sind ein besonders wichtiger Aspekt der digitalen Sicherheitspolitik an der Schnittstelle zwischen wirtschaftlichem Wohlstand und nationaler Sicherheit. Aufgrund des digitalen Wandels nehmen die Interdependenzen und die Komplexität dieser entscheidenden Systeme erheblich zu, ebenso wie das Risiko, dass Systemversagen zu einer Kaskadenwirkung über Sektor- und Ländergrenzen hinweg führt. Die Regierungen müssen die Betreiber kritischer Infrastrukturen und Dienstleistungen durch geeignete Maßnahmen dazu veranlassen, ihre digitale Sicherheit zu verbessern. Hierfür müssen diese in die Lage versetzt werden, sich den digitalen Wandel bestmöglich zunutze zu machen – u.a. durch die Einführung von Technologien wie dem Internet der Dinge, künstlicher Intelligenz, Big Data und Blockchain. Dabei müssen auch bestehende sektorspezifische Marktgegebenheiten sowie regulatorische und kulturelle Besonderheiten berücksichtigt werden. Kritische Infrastrukturen und grundlegende Dienstleistungen werden zwar oft von großen, häufig privatwirtschaftlichen Anbietern betrieben, der digitale Wandel ermöglicht aber auch KMU die Beteiligung an den Wertschöpfungsketten grundlegender Dienstleistungen (OECD, 2019[16]).

Eine große Herausforderung des digitalen Wandels im Finanz-, Energie- und Verkehrssektor ist die zunehmende Bedeutung kleinerer Marktteilnehmer wie KMU, da sich digitale Sicherheitsrisiken dadurch über die großen zentralen Akteure wie Banken oder Stromversorgungsunternehmen hinaus verbreiten. Solche KMU sind z.B. Start-ups, die innovative Zahlungssysteme, blockchainbasierte Technologien für den Energiehandel oder Mobilitätsdienste anbieten. Neben Start-ups spielen an der Erbringung grundlegender Dienstleistungen beteiligte etablierte KMU eine immer wichtigere Rolle, um die Risiken im Bereich der digitalen Sicherheit zu steuern und so die Risiken abzuschwächen, die größeren Unternehmen in ihren Wertschöpfungsketten entstehen.

Digitale Sicherheit ist ein facettenreicher Politikbereich, der Fragen im Zusammenhang mit wirtschaftlichem und gesellschaftlichem Wohlstand, Technologie und Strafverfolgung sowie nationaler und internationaler Sicherheit umfasst. Aus wirtschaftlicher und gesellschaftlicher Sicht wurden digitale Sicherheitsrisiken zunächst im Allgemeinen als technisches Problem betrachtet, das technische Lösungen verlangt. Nachdem sich Qualität und Ausmaß dieser Risiken jedoch verändert haben, überdenken die Regierungen nunmehr ihre Strategien und rufen zu einem Kulturwandel auf diesem Gebiet auf.

Verbraucher in der zusammenwachsenden Online- und Offline-Welt schützen

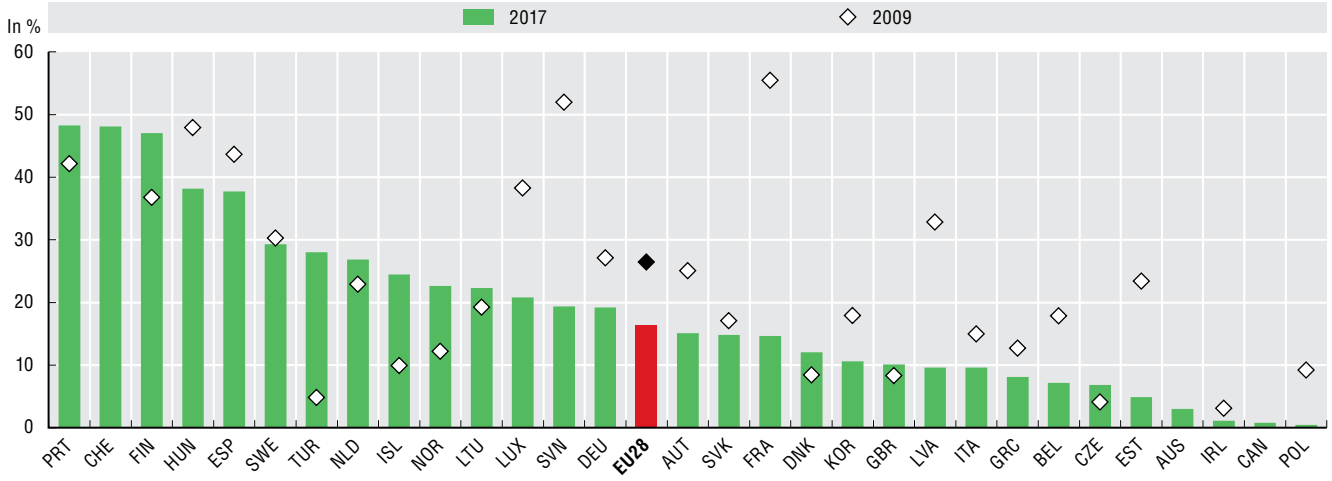
Ein weiterer wesentlicher Aspekt der Vertrauensförderung ist der Verbraucherschutz im digitalen Umfeld. Dies gilt für den elektronischen Handel ebenso wie für neue Technologien wie das Internet der Dinge (vgl. Kasten 7.2). Mit dem Verbraucherschutz verbindet sich nicht nur die Chance, neue Kunden und Märkte zu gewinnen, sondern auch ein allgemeinerer wirtschaftlicher Nutzen. Um einen erfolgreichen E-Commerce-Marktplatz aufzubauen, reichen Breitbandinfrastruktur, Hosting- und Zahlungsmöglichkeiten sowie Spezialsoftware nicht aus. Entscheidend ist auch die Bereitschaft der Verbraucher, diesen Marktplatz zu nutzen – trotz Bedenken gegenüber Fernabsatzgeschäften, bei denen die Waren nicht vorab geprüft werden können, potenziellen Risiken bei der Eingabe von Zahlungsdaten im Internet sowie der Sorge darüber, ob es im Falle von Schwierigkeiten möglich ist, Rechtsmittel einzulegen bzw. sein Recht durchzusetzen.

Zwar haben verbraucherschutzbezogene Bedenken bezüglich des Empfangs bzw. der Rückgabe von Waren, Reklamationen und Rechtsdurchsetzung in den vergangenen zehn Jahren im Durchschnitt nachgelassen, sie sind jedoch nach wie vor groß (Abb. 7.3). Am größten waren solche Bedenken in

Portugal (48%), der Schweiz (48%), Finnland (47%) und Ungarn (38%). In Polen und Kanada hingegen sorgten sich weniger als 1% der Internetnutzer um Verbraucherschutzbelange. In Irland und Australien waren die entsprechenden Werte mit 1% bzw. 3% ebenfalls niedrig.

7.3 Sorgen über den Verbraucherschutz bei Online-Bestellungen sind immer noch weit verbreitet

Personen, die aufgrund von Bedenken bezüglich des Empfangs oder der Rückgabe von Waren, Reklamationen oder der Rechtsdurchsetzung nicht online einkaufen, in Prozent der Internetnutzer, die zuletzt vor über einem Jahr oder noch nie Waren oder Dienstleistungen im Internet bestellt haben, 2017



Anmerkung: Vgl. Kapitelanmerkungen.[3]

Quelle: OECD-Berechnungen auf der Grundlage von Eurostat[15], *Digital Economy and Society Statistics* (Datenbank), *https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database;* nationale Quellen (Abruf: Dezember 2018).

StatLink https://doi.org/10.1787/888933914936

Besorgniserregend ist auch das zunehmende Angebot an nicht den Normen entsprechenden und unsicheren Produkten, die trotz Verkaufsverboten oder Rückrufen bei in- und ausländischen Online-Händlern erhältlich sind. Im Rahmen ihrer jährlichen weltweiten Informationskampagnen zur Sicherheit von Verbraucherprodukten führte die OECD 2018 eine Sensibilisierungskampagne zur Sicherheit von online verkauften Produkten durch.[4] Ziel der Kampagne war es, Online-Plattformen, Online-Verkäufer und Verbraucher darüber zu informieren, wie sie Produktsicherheitsrisiken erkennen und sich einen Überblick über die Produktsicherheitsvorschriften in verschiedenen Ländern verschaffen können.

Für den Erfolg der digitalen Wirtschaft ist es wichtig, die Verbraucher, die am elektronischen Handel teilnehmen und anderen Online-Tätigkeiten nachgehen, wirkungsvoll zu schützen. Geschäftsvorfälle, die digitale Inhalte zum Gegenstand haben und bei denen die Grenzen zwischen Verbrauchern und Unternehmen verwischt sind, können im Hinblick auf die traditionellen Konzepte von Eigentum, Haftung, Rechten und Pflichten ebenfalls zu Komplikationen führen. Die entscheidenden Herausforderungen beziehen sich auf die Offenlegung von Daten, irreführendes und unlauteres Geschäftsgebaren, Bestätigung und Bezahlung, Betrug und Identitätsdiebstahl, Produktsicherheit sowie die Beilegung von Streitigkeiten und Rechtsdurchsetzung.

Beispielsweise erhalten Verbraucher im Rahmen nichtmonetärer Transaktionen zunehmend „unentgeltlich" Waren und Dienstleistungen, für die sie aber im Gegenzug persönliche Daten zur Verfügung stellen. Dies kann die herkömmlichen Mechanismen zur Beilegung von Verbraucherrechtsstreitigkeiten infrage stellen (OECD, 2016[17]). Zudem wird es durch neuartige Formen der Nutzung von Vermögenswerten und Inhalten, u.a. durch Vermietung bzw. Verleih, gemeinsame Nutzung und Abonnements, für Verbraucher schwieriger, ihre Rechte und Pflichten zu verstehen (Kasten 7.2). Häufig ist unklar, inwiefern Einschränkungen in Bezug auf die Funktionalität und Interoperabilität digitaler Produkte bestehen. Auch die Preisgestaltung kann für Verbraucher problematisch sein, wenn Unternehmen beispielsweise nicht alle Preisbestandteile vorab offenlegen („Drip Pricing") oder irreführende Referenzpreise nutzen, um Verhaltensverzerrungen auf Seiten der Verbraucher auszunutzen.

7.2 Vertrauen in Peer-to-Peer-Plattformen

Peer-to-Peer-Transaktionen spielen seit Langem eine Rolle im Geschäftsleben, aber dank Online-Plattformen sind sie nun in einem viel größeren Maßstab möglich als zuvor. Am Anfang dieser Entwicklung standen u.a. Plattformen für den Verkauf von Waren (z.B. Online-Auktionshäuser). Neuere Geschäftsmodelle umfassen Unterkunfts-, Beförderungs- und Mobilitätsdienstleistungen. Andere Bereiche, die durch Plattformen grundlegend verändert werden, sind beispielsweise der Markt für haushaltsnahe Dienstleistungen, Essensdienste und Finanzdienstleistungen. Diese Geschäftsmodelle werden häufig als „Sharing Economy" oder „kollaborativer Konsum" bezeichnet, was jedoch der kommerziellen Dimension dieser Märkte nicht gerecht wird.

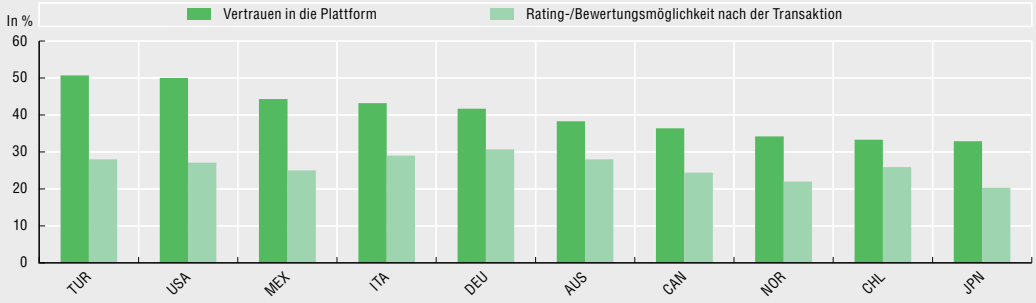
Diese Geschäftsmodelle bieten den Personen, die Waren oder Dienstleistungen anbieten („Peer-to-Peer-Anbieter"), ebenso wie den Plattformen, die die Geschäfte vermitteln („Peer-to-Peer-Plattformen"), neue Geschäftschancen. Die Nutzung von Peer-to-Peer-Plattformen kann für Verbraucher in vielfacher Hinsicht Vertrauensfragen aufwerfen: Vertrauen in die Zuverlässigkeit und Qualifikationen des Peer-to-Peer-Anbieters, Vertrauen in den Vermögenswert oder die Dienstleistung und Vertrauen in die Garantien und Schutzmechanismen der Peer-to-Peer-Plattform. Allgemeine Geschäftsbedingungen reichen u.U. nicht immer aus, um Verbraucher über wichtige Sachverhalte aufzuklären, da nur 17% der Nutzer die Allgemeinen Geschäftsbedingungen von Peer-to-Peer-Plattformen (wie Airbnb und BlaBlaCar) in voller Länge lesen.

Die Plattformen haben eine Reihe praktischer, innovativer Mechanismen entwickelt, um die Bedenken der Verbraucher auszuräumen und Nutzungshemmnisse abzubauen. Die wichtigsten Vertrauensmechanismen sind Bewertungs- und Reputationssysteme. Auch Garantien bzw. Versicherungen, überprüfte Identitäten, Vorprüfungen, sichere Zahlungssysteme sowie Aufklärung, Checklisten und Formulare können zur Vertrauensbildung beitragen (OECD, 2016[18]).

Um besser zu verstehen, welche Faktoren das Vertrauen der Verbraucher in Peer-to-Peer-Plattformen beeinflussen, führte die OECD eine Online-Umfrage unter 10 000 Verbrauchern in zehn OECD-Mitgliedsländern durch (OECD, 2017[19]). Die Umfrage ergab u.a., dass Verbraucher Peer-to-Peer-Plattformen im Allgemeinen vertrauen – häufig sogar mehr als konventionellen Unternehmen auf demselben Markt. Mindestens 30% der Verbraucher, die trotz Unsicherheit bezüglich der Vertrauenswürdigkeit des Verkäufers einen Kauf tätigten, führten ihr Vertrauen in die Plattform als Grund an (Abb. 7.4)

7.4 Großes Vertrauen in Peer-to-Peer-Plattformen

Gründe für den Kauf auf einer Peer-to-Peer-Plattform trotz Unsicherheit bezüglich der Vertrauenswürdigkeit des Verkäufers/Anbieters, in Prozent aller Nutzer, die den Kauf trotz dieser Unsicherheit durchgeführt haben, 2017



Quelle: OECD (2019[5]), *Measuring the Digital Transformation, https://dx.doi.org/10.1787/9789264311992-en,* auf der Grundlage von OECD-Berechnungen auf Basis von OECD (2017[19]), "Trust in peer platform markets: Consumer survey findings", *https://dx.doi.org/10.1787/1a893b58-en.*

StatLink https://doi.org/10.1787/888933915430

Es gibt verschiedene Wege, das Vertrauen der Verbraucher zu gewinnen. Besonders wichtig sind jedoch sichere Zahlungsverfahren, Datensicherheit und Bilder, mit denen sich die Verbraucher einen Eindruck von den angebotenen Waren und Dienstleistungen verschaffen können. Seltsamerweise machen sich die Kunden von Peer-to-Peer-Plattformen nicht immer die Mühe, die Allgemeinen Geschäftsbedingungen oder Datenschutzerklärungen genau zu lesen, obwohl sie behaupten, dass Datenschutz und -sicherheit für sie wichtig seien. Ihr Vertrauen auf einen verantwortungsvollen Umgang der Plattformen mit ihren persönlichen Daten scheint aber davon nicht nennenswert beeinträchtigt zu werden. Dies gilt insbesondere dann, wenn Peer-to-Peer-Plattformen anderen Arten von Online-Geschäften gegenübergestellt werden.

Quelle: OECD (2017[19]) "Trust in peer platform markets: Consumer survey findings", *https://dx.doi.org/10.1787/1a893b58-en.*

Auch auf den Finanzmärkten hat die Digitalisierung neue Produkte und Dienstleistungen hervorgebracht. Um sie effektiv nutzen zu können und zu verstehen, welche Auswirkungen die Übermittlung von Daten an die Institute haben kann, benötigen die Menschen (insbesondere diejenigen mit geringer digitaler Grundbildung) neue Kompetenzen und Kenntnisse. Da sich die Verbraucher außerdem zunehmend auf automatisierte Verfahren und auf nichtmenschliche Unterstützung verlassen (z.B. automatisierte Anlageberatung, Chatbots), müssen Governance- und Kontrollmechanismen eingeführt werden, um den finanziellen Verbraucherschutz zu gewährleisten, wie dies auch im Offline-Geschäftsverkehr der Fall ist.

Nahtlose Transaktionen werfen verstärkt die Frage auf, inwieweit sich die Verbraucher über die Bedingungen und die Art der getätigten Transaktionen im Klaren sind. Dies spielt zwar auch im reinen Offline-Geschäftsverkehr eine Rolle, gewinnt jedoch weiter an Bedeutung, je mehr digitale Tätigkeiten auf Mobiltelefonen durchgeführt werden.

7.3 Die Verbraucher und das Internet der Dinge

Die Verbraucher kaufen und nutzen immer mehr vernetzte Geräte in ihrem Haushalt und im Alltag, die dem Internet der Dinge zuzurechnen sind. Dazu gehören die sogenannten Wearables, am Körper getragene Geräte (z.B. Fitnesstracker, Smartwatches und Datenbrillen), Smart-Home-Geräte und -Systeme (wie intelligente Schlösser oder Thermostate, die die Verbraucher über ihren Energieverbrauch informieren können), vernetzte Spielzeuge und Kinderartikel.

Komfort, individuelle Anpassung und die Möglichkeit, vernetzte Geräte über ein Smartphone fernzusteuern, gehören zu den zahlreichen Vorteilen des Internets der Dinge für die Verbraucher (OECD, 2018[20]). Darüber hinaus wird erwartet, dass dieser Markt die kontinuierliche Verbesserung des Produktdesigns, der Fertigung und der Lieferprozesse revolutionieren und sich zudem positiv auf die Produktsicherheit auswirken wird. Beispielsweise können vernetzte Geräte wie intelligente Thermostate oder Rauchmelder aus der Ferne überwacht und neu eingestellt oder deaktiviert werden. Dies erleichtert den Umgang mit Produktsicherheitsrisiken, die nach der Installation festgestellt werden, einschließlich der Rückrufabwicklung (OECD, 2018[21]; OECD, 2018[22]).

Trotz seines Potenzials ist das Internet der Dinge auch mit Risiken und Herausforderungen verbunden, die das Vertrauen in diesen neu entstehenden Markt beeinträchtigen können. So können etwa Software-Aktualisierungen neue Probleme bei vernetzten Produkten verursachen oder Compliance-Fragen aufwerfen. Digitale Sicherheitsrisiken und Schwachstellen können auch Auswirkungen auf die Sicherheit verbundener Produkte haben. Die komplexen Lieferketten des Internets der Dinge können zu Unsicherheiten darüber führen, wer für Schäden verantwortlich ist, die den Verbrauchern durch ein verbundenes Produkt entstehen; außerdem stellt sich allgemein die Frage, ob die Regelungen für den Verbraucherschutz und die Produktsicherheit angepasst werden müssen, um diesen Herausforderungen zu begegnen.

Insgesamt ist es für die Stärkung des Vertrauens entscheidend, Risikomanagement als gemeinsamen Bezugsrahmen für die Entwicklung kohärenter Politikmaßnahmen zu etablieren. Hierfür ist die Beteiligung der Politikakteure in den Bereichen digitale Sicherheit, Daten- und Verbraucherschutz sowie Produktsicherheit erforderlich. Insbesondere sollten die Politikverantwortlichen die Wechselwirkungen zwischen den digitalen Risiken in diesen Bereichen berücksichtigen. So kann z.B. ein Cyberangriff, bei dem Verbraucherdaten zu Betrugszwecken gestohlen werden, den Datenschutz ebenso wie die Rechte der Verbraucher verletzen. Solche Wechselwirkungen unterstreichen, wie wichtig eine abgestimmte Politik in diesen Bereichen ist. Sie bildet die Grundlage für einen umfassenderen Ansatz zur Vertrauensbildung im digitalen Zeitalter.

Anmerkungen

Israel
Die statistischen Daten für Israel wurden von den zuständigen israelischen Stellen bereitgestellt, die für sie verantwortlich zeichnen. Die Verwendung dieser Daten durch die OECD erfolgt unbeschadet des völkerrechtlichen Status der Golanhöhen, von Ost-Jerusalem und der israelischen Siedlungen im Westjordanland.

1. Abbildung 7.1: Sofern nicht anders angegeben, sind Internetnutzer definiert als Personen, die das Internet in den letzten 12 Monaten genutzt haben. Für Chile beziehen sich die Daten auf 2014. Für Costa Rica beziehen sich die Daten auf Personen der Altersgruppe 18-74 Jahre statt 16-74 Jahre. Für Korea beziehen sich die Daten auf 2017 und umfassen sowohl private als auch geschäftliche Zwecke. Für Mexiko beziehen sich die Daten auf 2017 anstatt 2015. Ab 2015 wurden die Daten im Rahmen einer eigenständigen thematischen Umfrage erhoben – im Gegensatz zu den Vorjahren, als die Daten anhand eines in verschiedenen Erhebungen administrierten Moduls gewonnen wurden. Diese methodische Veränderung gilt es bei Vergleichen mit Daten vor 2015 zu bedenken. Die Daten für 2017 beziehen sich auf folgendes Item: „Betrug unter Nutzung von Daten (finanziellen, personenbezogenen usw.)". Für die Schweiz beziehen sich die Daten auf 2014 anstatt 2015. Die Daten für 2014 beziehen sich auf Personen, die „in den letzten 12 Monaten ein Sicherheitsproblem hatten".
2. Abbildung 7.2: Für Australien beziehen sich die Daten auf das Finanzjahr 2012/2013, das am 30. Juni 2013 endete. Die Daten für Kanada beziehen sich auf 2012. Für die Länder, die am Europäischen Statistischen System teilnehmen, umfassen „Bedenken in Bezug auf die Zahlungssicherheit und den Datenschutz" für 2017 keine „Bedenken in Bezug auf den Datenschutz".
3. Abbildung 7.3: Für Australien beziehen sich die Daten auf das Finanzjahr 2012/2013, das am 30. Juni 2013 endete. Die Daten für Kanada beziehen sich auf 2012.
4. *http://oe.cd/safe-products-online*.

Literaturverzeichnis

Casalini, F. und J. López González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, *https://doi.org/10.1787/b2023a47-en*. [10]

Eurostat (2018), *Digital Economy and Society Statistics* (Datenbank), *https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database* (Abruf: Dezember 2018). [15]

Hufford, A. und P. Loftus (2017), *Merck Swings to Loss as Cyberattack Hurts Sales*, *https://www.wsj.com/articles/merck-swings-to-loss-as-cyberattack-hurts-sales-1509107269*. [12]

Mayer, R., J. Davis und D. Schoorman (1995), "An integrative model of organizational trust", *The Academy of Management Review*, Vol. 20, No. 3, S. 709-734, *http://www.jstor.org/stable/258792*. [3]

Merck (2017), *Merck Announces Second-quarter 2017 Financial Results*, press release, 28 Juli, *https://www.mrknewsroom.com/news-release/corporate-news/merck-announces-second-quarter-2017-financial-results* (Abruf: 21. Februar 2019). [11]

Murtin, F. et al. (2018), "Trust and its determinants: Evidence from the Trustlab experiment", *OECD Statistics Working Papers*, No. 2018/2, OECD Publishing, Paris, *https://dx.doi.org/10.1787/869ef2ec-en*. [2]

NCCIC (2016), *Cyber-attack against Ukrainian Critical Infrastructure*, *https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01* (Abruf: 21. Februar 2019). [13]

OECD (erscheint demnächst), "Towards national privacy strategies", *OECD Digital Economy Policy Papers*, OECD Publishing, Paris. [8]

OECD (2019), "Digital security and resilience in critical infrastructure and essential services", *OECD Digital Economy Papers*, No. 281, OECD Publishing, Paris, *https://doi.org/10.1787/a7097901-en*. [16]

OECD (2019), "ICT Access and Usage by Households and Individuals", *OECD Telecommunications and Internet Statistics* (database), OECD, Paris, *https://dx.doi.org/10.1787/b9823565-en*. (accessed 28 January 2019) [6]

OECD (2019), *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264311992-en*. [5]

OECD (2018), "Consumer policy and the smart home", *OECD Digital Economy Papers*, No. 268, OECD Publishing, Paris, *https://dx.doi.org/10.1787/e124c34a-en*. [20]

OECD (2018), "Consumer product safety in the Internet of Things", *OECD Digital Economy Papers*, No. 267, OECD Publishing, Paris, *https://dx.doi.org/10.1787/7c45fa66-en*. [21]

OECD (2018), "Enhancing product recall effectiveness globally: OECD background report", *OECD Science, Technology and Industry Policy Papers*, No. 58, OECD Publishing, Paris, *https://dx.doi.org/10.1787/ef71935c-en*. [22]

OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264276284-en*. [4]

OECD (2017), *OECD Guidelines on Measuring Trust*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264278219-en*. [1]

OECD (2017), "Trust in peer platform markets: Consumer survey findings", *OECD Digital Economy Papers*, No. 263, OECD Publishing, Paris, *https://dx.doi.org/10.1787/1a893b58-en*. [19]

OECD (2016), *OECD Recommendation of the Council on Consumer Protection in E-Commerce*, OECD Publishing, Paris, *https://dx.doi.org/10.1787/9789264255258-en*. [17]

OECD (2016), "Protecting Consumers In Peer Platform Markets: Exploring The Issues", No. 253, OECD Publishing, Paris, *https://dx.doi.org/10.1787/5jlwvz39m1zw-en*. [18]

OECD (2016), *The OECD Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity*, OECD, Paris, *https://www.oecd.org/internet/Digital-Economy-Ministerial-Declaration-2016.pdf*. [7]

OECD (2013), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, *http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf*. [9]

OECD (2007), *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, *http://www.oecd.org/internet/ieconomy/38770483.pdf*. [23]

Popescu, N. und S. Secrieru (2018), "Hacks, leaks and disruptions: Russian cyber strategies", *Chaillot Paper* No. 148, *https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf*. [14]