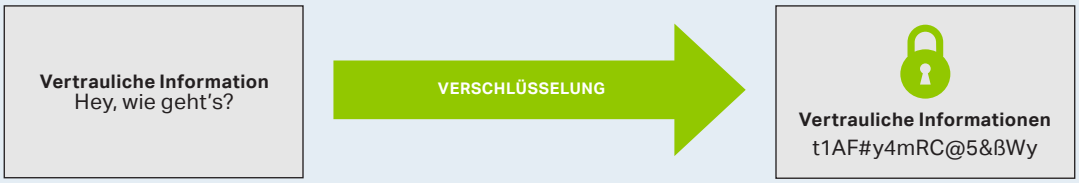
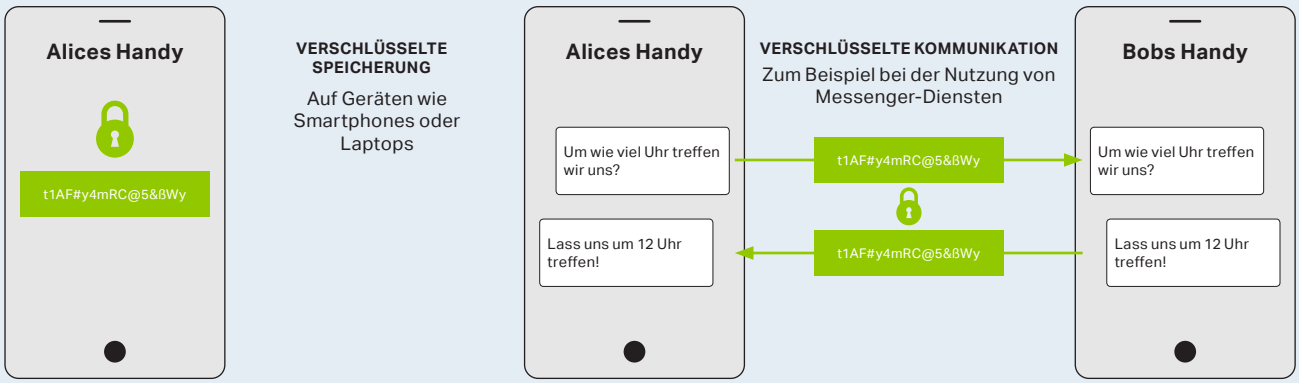
Die Kontroverse um Verschlüsselung: Worum geht es?

Was bedeutet Verschlüsselung?

Durch Verschlüsselungsverfahren werden lesbare Daten („Klartext") in unlesbare Daten („Geheimtext") umgewandelt. Nur der Besitzer des korrekten Schlüssels kann den Klartext lesen. Dieser Prozess schützt eine Vielzahl von Online-Aktivitäten und wird zum Beispiel genutzt, um private Unterhaltungen, Zahlungsdaten oder Banktransfers zu sichern.

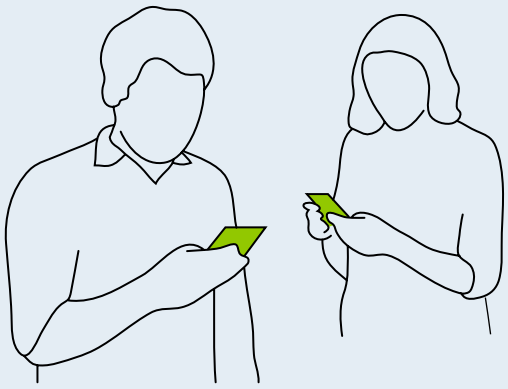


Wo findet Verschlüsselung statt?



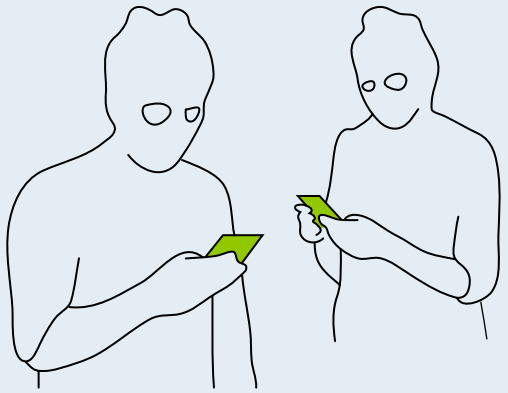
Was ist so kontrovers daran?

Verschlüsselungstechnologien schützen Bürger/innen bei fast allen Aktivitäten im Netz, vom Online-Banking bis zum Online-Shopping.



Bob: „Lass uns um 12 Uhr treffen!"

Aber: Verschlüsselungstechnologien schützen auch die Online-Aktivitäten von Spion/innen, Terrorist/innen und Kriminellen.

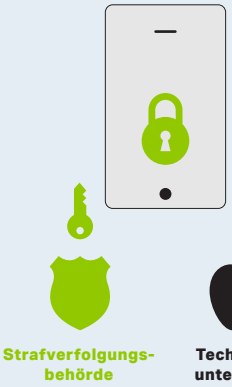


Bob: „Lass es uns für 12 Uhr planen! "

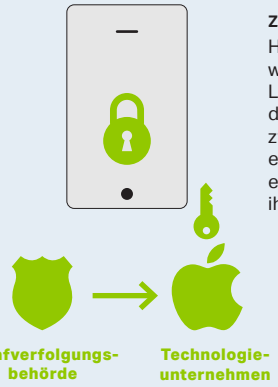
• • •

Strafverfolgungsbehörden argumentieren, dass sie aufgrund von zwei Trends immer häufiger „im Dunkeln tappen":
(1) Kommunikation findet zunehmend online statt und (2) immer mehr Unternehmen stärken die Sicherheit ihrer Technologien und Dienste durch standardmäßige Verschlüsselung. Dadurch steigt die Anzahl an Nutzer/innen – und Verbrecher/innen – deren Daten unlesbar sind.

Was schlagen Strafverfolgungsbehörden vor?



ZUGANG DURCH DIE „HINTERTÜR"
In den 1990er Jahren kam die Forderung auf, dass Unternehmen sogenannte Hintertüren in ihre Produkte einbauen sollten. Dieser „goldene Schlüssel" hätte Strafverfolgungsbehörden direkten Zugang zu verschlüsselten Daten gegeben. Dazu kam es nie.



ZUGANG DURCH DIE "VORDERTÜR"
Heutzutage sind die Forderungen weniger konkret. In verschiedenen Ländern werden Gesetze diskutiert, die Technologieunternehmen zwingen würden, Daten auf Vorlage eines Gerichtsbescheids hin zu entschlüsseln. Das „wie" bliebe dabei ihnen überlassen.

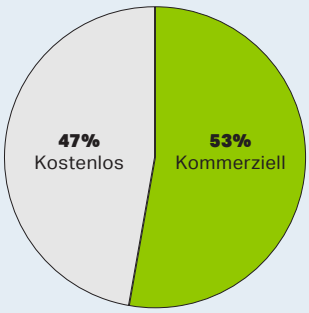
Was spricht gegen solche Forderungen?

NOTWENDIGKEIT
Dass Strafverfolgungsbehörden wie behauptet wirklich „im Dunkeln tappen" ist nicht belegt. Kritiker/innen sprechen im Gegenteil von einem „goldenen Zeitalter der Überwachung".

„Strafverfolgungsbehörden können zwar meine Nachrichten nicht lesen, aber sie wissen dank moderner Technologien oft sehr genau, wohin ich gehe und mit wem ich rede."

UMSETZBARKEIT
Für einzelne Regierungen wird es nahezu unmöglich sein, einen global Markt für Verschlüsselungstechnologien zu regulieren, vor allem da fast 50% davon kostenlos verfügbar sind.

Verfügbarkeit von Verschlüsselungstechnologien



NEGATIVE AUSWIRKUNGEN
Eine mögliche Regulierung hätte negative Externalitäten. Sie würde:

Die IT-Sicherheit durch Schaffung neuer Schwachstellen schmälern.

Das Vertrauen in die Technologieindustrie gefährden.

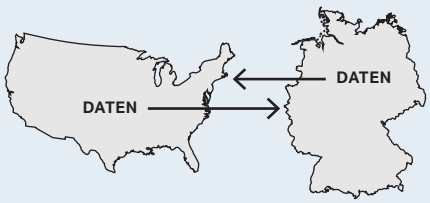
Menschenrechte weltweit bedrohen, da autoritäre Regime die gleichen Systeme nutzen werden.

Welche Alternativen gibt es, um Strafverfolgungsbehörden Zugang zu Daten zu verschaffen?

Aufbau und Regulierung nationaler Hacking-Kapazitäten, um auf einzelne Geräte zugreifen zu können.

Verstärkung und Weiterbildung von spezialisiertem Personal, um Ermittlungen besser durchführen zu können.

Reformierung des Systems der internationalen Rechtshilfe, um den zwischenstaatlichen Datenaustausch zu verbessern.



Andere Vorschläge sind der Ausbau der Vorratsdatenspeicherung oder sogar der gesetzlichen Datenlokalisierung, um so den Zugriff auf Daten zu verbessern. In beiden Fällen überwiegen jedoch technische und rechtliche Bedenken mögliche Vorteile.

Autoren: Mirko Hohmann & Oliver Read. Erstellt durch das Global Public Policy Institute (GPPi) für die Heinrich Böll Stiftung.
Angelehnt an: Segal, Adam (2016) Encryption Explained: A Council on Foreign Relations Infographic, Council on Foreign Relations.

GPPi