

# ÖFIT-Trendschau

Öffentliche Informationstechnologie in der digitalisierten Gesellschaft

Trendthema 17:

## **Digitale Unversehrtheit**

Stand: Juli 2017



**Herausgeber:**

Mike Weber  
Kompetenzzentrum Öffentliche IT  
Fraunhofer-Institut FOKUS  
Kaiserin-Augusta-Allee 31, D-10589 Berlin  
Telefon: +49 30 3463 - 7173  
Telefax: + 49 30 3463 - 99 - 7173  
info@oeffentliche-it.de  
www.oeffentliche-it.de  
www.fokus.fraunhofer.de

**Autorinnen und Autoren der Gesamtausgabe:**

Mike Weber, Stephan Gauch, Faruch Amini, Tristan Kaiser, Jens Tiemann, Carsten Schmoll, Lutz Henckel, Gabriele Goldacker, Petra Hoepner, Nadja Menz, Maximilian Schmidt, Michael Stemmer, Florian Weigand, Christian Welzel, Jonas Pattberg, Michael Rothe, Oliver Schmidt, Nicole Opiela, Florian Friederici, Jan Gottschick, Jens Fromm

**Autorinnen und Autoren einzelner Trendthemen:**

Michael Rothe, Oliver Schmidt

ISBN: 978-3-9816025-2-4

Juli 2017

**Autorinnen/Autoren:**

Tristan Kaiser et al.

**Bibliographische Angabe:**

Tristan Kaiser et al. 2019, Digitale Unversehrtheit, In: Jens Fromm und Mike Weber, Hg., 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, <http://www.oeffentliche-it.de/-/digitale-unversehrtheit>

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung 3.0 Deutschland Lizenz (CC BY 3.0 DE) <http://creativecommons.org/licenses/by/3.0 de/legalcode>. Bedingung für die Nutzung des Werkes ist die Angabe der Namen der Autoren und Herausgeber.

---

# Digitale Unversehrtheit

Körperliche Unversehrtheit ist die Voraussetzung für den Zusammenhalt eines jeden Gemeinwesens. Im Digitalen erscheint diese Sicht weit weniger selbstverständlich. Neue Qualitäten von Identitätsdiebstahl und Cybermobbing wirken wie Auswüchse einer digitalisierten Gesellschaft, die ihr Wertegerüst noch nicht abschließend gebaut hat. Die öffentliche Hand ist diesem Aufbau nicht immer förderlich, wenn beispielsweise ihre Datenbegehrlichkeiten als unverhältnismäßig angesehen werden. Digitale Unversehrtheit bedarf einer allgemeinen Ethik für den zwischenmenschlichen Umgang im digitalen öffentlichen Raum. Dies erfordert einen gesellschaftlichen Diskurs.

## Jeder dritte Schüler wird Opfer von Cybermobbing

Das Recht auf körperliche Unversehrtheit zählt zu den grundlegenden Persönlichkeitsrechten. Mit der zunehmenden Digitalisierung und Vernetzung der Gesellschaft stellt sich die Frage, wie das Grundrecht der körperlichen Unversehrtheit auf die digitale Welt übertragen werden kann und welche faktische Schutzwirkung die Übertragung entfaltet. Körperliche Versehrungen sind in der Regel durch den Betroffenen unmittelbar erfahrbar und oft auch für das soziale Umfeld erkennbar. Im Digitalen sind Verletzungen nicht immer leicht zu erfassen. Sie passieren mitunter über Jahre unbemerkt vom Betroffenen. Das bedeutet aber keinesfalls, dass diese Versehrungen nicht mit beträchtlichen Folgen verbunden sein können. Die digitale Identität kann gestohlen und missbraucht werden. Digitale Identitäten sind auch aus anderer Perspektive relevant, nämlich wenn Anonymität genutzt wird, um die digitale Persona zu schädigen. Zum Teil werden für das Cybermobbing digitale Identitäten auch absichtlich fingiert und in diffamierender Weise genutzt. Jeder dritte Schüler wurde bereits einmal Opfer von Cybermobbing. Trotz der virtuellen Natur der Demütigungen und Drohungen sind die Auswirkungen auf das Leben der Opfer gravierend real. Der Dreiklang digitaler Versehrungen – die Nutzung gestohlener Identitäten, die Vortäuschung von Urhebererschaft und die anonyme Beschämung anderer – eröffnet ein weites Feld für solche Beeinträchtigungen wie Demütigungen, Verleumdungen, ungesetzliche Überwachung und Spionage.

# Begriffliche Verordnung



---

## **Digitale Unversehrtheit geht über Datenschutz hinaus**

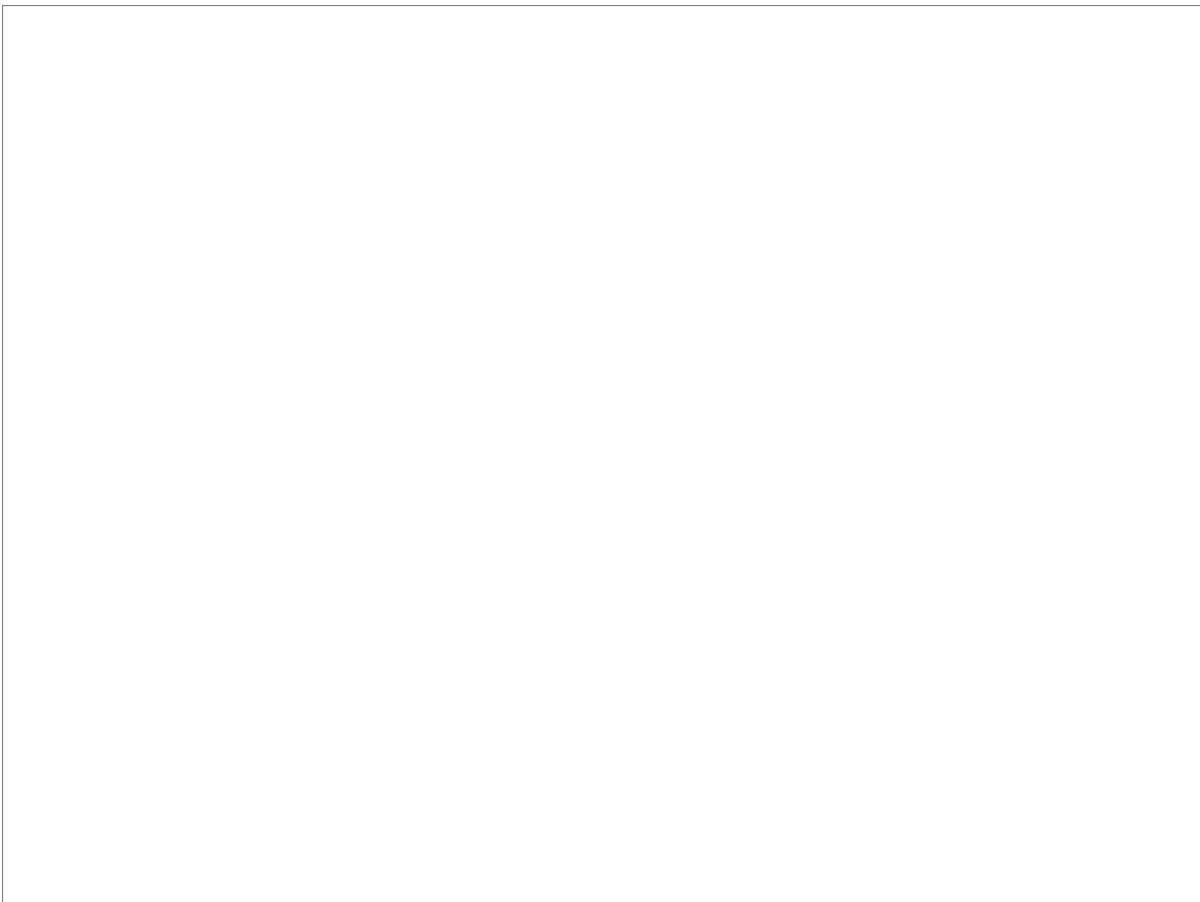
Eine notwendige aber nicht zwingend hinreichende Voraussetzung für die Gewährleistung digitaler Unversehrtheit ist die Einhaltung der technischen Anforderungen für Datenschutz und IT-Sicherheit (siehe [Security by Design](#)): Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität. Digitale Unversehrtheit geht aber darüber hinaus. Digitale Selbstbestimmung, also einen souveränen Umgang mit den eigenen Daten, gilt es anzustreben (siehe [Post Privacy](#)). Daraus ergibt sich beispielsweise auch die Notwendigkeit, Daten wieder löschen zu können. Digitales Vergessen und digitaler Radiergummi bezeichnen so bislang nicht abschließend bewältigte, gesellschaftliche und technische Herausforderungen. Die Wahrnehmung der staatlichen Verantwortung zeigt sich in diesem Themenfeld in vielfacher Weise. Mit dem Recht auf informationelle Selbstbestimmung und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, kurz IT-Grundrecht, hat das Bundesverfassungsgericht Grundsätze des allgemeinen Persönlichkeitsrechts auf das Digitale anwendbar gemacht. Auf europäischer Ebene finden sich Regelungen und Initiativen für ein Recht auf digitales Vergessen und Beschränkungen der Datenbegehrlichkeiten öffentlicher Stellen. Mit neuem Personalausweis und sicheren Kommunikationswegen werden zugleich technische Lösungen bereitgestellt.

## **Gesamtgesellschaftlicher Diskurs notwendig**

Durch diese Aktivitäten kann allerdings nur ein Ausschnitt der Problematik adressiert werden, während etwa anonymen Demütigungen und Verleumdungen so nicht begegnet werden kann. Zudem nähren datenschutzrechtlich kritisierte Vorhaben und die Aufdeckung von Geheimdienstaktivitäten Zweifel an der Angemessenheit staatlicher Lösungen. Zugleich stellt sich die Frage, inwieweit gesetzliche Regelungen die digitale Unversehrtheit der Bürgerinnen und Bürger überhaupt schützen können respektive wie weit staatlicher Eingriff gehen sollte. Auch zur Beantwortung dieser Fragen bedarf es eines gemeinsame Werte schärfenden, gesamtgesellschaftlichen Diskurses.

Ziel eines solchen Diskurses muss die Bewusstseinschärfung für, im Digitalen oft schwerer zu identifizierende, Regelverletzungen und die notwendige Anpassung bewährter Regeln sein. Dass dieser Diskurs letztlich ein globaler ist, entbindet weder Wirtschaft noch Staat von der Verantwortung, ihn zu begleiten und zu unterstützen.

## **Themenkonjunkturen**



---

## Folgenabschätzung

### Möglichkeiten

- Digitale Unversehrtheit bildet die Grundlage für jedes digitale Gemeinwesen
- Die Sicherstellung digitaler Unversehrtheit könnte auch Skeptiker von der Nutzung öffentlicher digitaler Räume überzeugen
- Junge Menschen fühlen sich im Umgang mit digitalen Medien oft sehr sicher. Dies bietet die Grundlage für eine kritische Reflexion des eigenen Verhaltens
- Transparenz und relevante Informationen können Fehlverhalten verhindern

### Wagnisse

- Herausfordernde Selbstbeschränkung bei der Nutzung der technischen Möglichkeiten und stete Versuchung zu deren anonymer Nutzung
- Schwieriger Aushandlungsprozess gemeinsam respektierter Regeln
- Anhaltende Ungleichheit durch Relevanz von Technologiekenntnissen und Medienkompetenz (siehe [Digitale Gräben](#))
- Wachsende Bedeutung des Digitalen für gesellschaftliche Teilhabe und Digitalisierung des Alltags (siehe [Ambient World](#))
- Fehleranfälligkeit und immerwährende Versuchungen

# **Handlungsräume**

## **Vorbildfunktion**

Staatliche Instanzen sollten eine Vorbildfunktion im sensiblen Umgang miteinander im Digitalen annehmen und ausgestalten.

## **Rechtssicherheit stärken**

Rechtssicherheit erhöht das Vertrauen. Die zu beobachtende Stärkung von Rechten des Einzelnen in digitalen Räumen durch den Europäischen Gerichtshof zeigt beispielhaft Möglichkeiten auf.

## **Abgestufte Werkzeuge bereitstellen**

Die öffentliche Hand kann als Hilfestellung für die Befähigung der Bürgerinnen und Bürger gezielt Instrumente etwa des Identitätsschutzes fördern, sollte dabei aber auf abgestufte und flexible Anwendung achten.

## **Medienkompetenz vertiefen**

Der kompetente Umgang mit digitalen Medien gehört weit oben auf die Agenden von Schulen und Einrichtungen der Erwachsenenbildung.