Digitalisierung – Phänomen, Gefährdung, Chancen und Vision

Das DPT-Gutachten zu Smart Prevention im Überblick

Wolfgang Kahl

„Smart Prevention – Prävention in der digitalen Welt" lautet das Schwerpunktthema des 25. Deutschen Präventionstages. Seit 2007 lässt der DPT zu jedem Kongress ein wissenschaftliches Gutachten erstellen, das Analysen und wissenschaftliche Stellungnahmen zum jeweiligen Schwerpunktthema aufbereitet. Das diesjährige Gutachten entfernt sich von der rein textlichen Gestaltung und ist multimedial aufgebaut. 17 Experten/-innen aus den sechs Fachdisziplinen Kriminologie, Pädagogik, Psychologie, Rechtswissenschaft, Informatik und Geisteswissenschaften kommen zu Wort. Entstanden sind 68 kurze Videoclips mit Statements zu den vier Bereichen Phänomen, Gefährdung, Chancen der Digitalisierung und Vision der Smart Prevention. Wer lieber liest, findet auch ein Transkript zu jeder Videoaufzeichnung. Es entsteht für den Betrachter zunächst ein Mosaik von eher unverbundenen Beiträgen, bei dem ihre Singularität ins Auge fällt. Es folgt der Versuch, in verständiger Betrachtung die unterschiedlichen Perspektiven zu bündeln, Gemeinsamkeiten und Komplementarität aufzuzeigen und Differenzen zu benennen.

Phänomen der Digitalisierung

Die grundsätzlichen Charakterisierungen des Phänomens sind weitgehend übereinstimmend. Es handelt sich bei der Digitalisierung der menschlichen Lebensbereiche um einen gravierenden, geradezu revolutionären Umbruch in der Menschheitsgeschichte mit Auswirkungen in alle Funktionssysteme von Gesellschaft, Ökonomie, Politik, Wissenschaft, Infrastrukturen und Sicherheit. Unbestritten verändert sich der Alltag für jeden Einzelnen durch digitales Kommunizieren, Vernetzen, Lernen, Arbeiten (Schönbohm). Aufgaben und Verhaltensweisen, die bislang als typisch menschlich galten, werden von Rechnern übernommen (Gusy). Persönliche und kollektive Handlungsmöglichkeiten erweitern sich (Görgen).

Die Auswirkungen lassen sich in jedem Lebensbereich spüren, auch im Zwischenmenschlichen und im gesellschaftlichen Zusammenleben (Grund). Das Soziale wandert immer mehr ins Netz. Digitale Kommunikation verändert sich vom Informationsaustausch hin zu einer identitätsstiftenden Präsenz (Hajok). Eine neue Sozialisationsinstanz entwickelt sich (Ackermann). Der jugendliche Experimentierraum erweitert sich, der Schonraum Kindheit löst sich auf (Hajok). Digitalisierung strengt an, weil Kommunikation immer und überall möglich ist (Schirrmacher).

Der Wissenszuwachs steigert sich beträchtlich (Schieferdecker). Eine Herausforderung wird das entstehende Wissensgefälle. Das Verständnis über die Technik, die wir täglich nutzen, ist sehr ungleich verteilt (Demuth) mit Folgen auch für das Risikoverhalten. Menschen vernetzen sich untereinander, aber auch mit den Technologien (Wrede). Die damit bewirkten Veränderungen führen zu einer völlig neuen Arbeitsteilung zwischen Mensch und Umwelt, Mensch und Maschine sowie Mensch und Infrastruktur (Gusy). Die Vernetzung ist weltweit und schnell. Sie ermöglicht einen nahezu unbegrenzten Austausch von Daten und Informationen (Ungefuk) mit erheblichen Datenverarbeitungs- und Verknüpfungskapazitäten (Belina). Physische Grenzen sind aufgehoben. Das digitale Netz ist ein globaler Interaktions- und Kommunikationsraum (Rüdiger). Die Innovationsfähigkeit der Gesellschaften steigt. Künstliche Intelligenz ermöglicht autonome, selbstlernende Systeme (Schieferdecker).

Durch eine Datafizierung der Gesellschaft entstehen Prognosemöglichkeiten menschlichen Verhaltens (Heesen). In China wird bereits heute das Verhalten der Bürger/-innen erfasst, analysiert und durch Social Scoring in einem Wert abgebildet. Die individuellen Zukunftschancen sind damit Gegenstand der staatlichen Steuerung (Grund). Big Data ermöglicht ganz neue Überwachungssituation (Heesen), die in einem gesellschaftlichen und politischen Diskurs über die richtige Mischung von Sicherheit und Freiheit grundsätzlich und in praktischen Abwägungssituationen geklärt werden müssen (Gusy).

Gefahren der Digitalisierung

In den 17 Stellungnahmen werden überwiegend Risiken und Gefahren der Digitalisierung im Sinne neuer Kriminalitätsformen, Tatmöglichkeiten und -gelegenheiten sowie Begehungsformen erörtert. Die dadurch entstehenden Herausforderungen für Prävention, Gefahrenabwehr und Strafverfolgung sind ein weiteres Thema sowie das Übermaßpotenzial von Überwachung und die Manipulationsgefahren durch Provider sozialer Medien.

Exemplarisch für die Erfordernisse im digitalen Alltag zeigt sich beim Online-Banking, wie neue Tatbegehungen (Phishing, Hacking, Manipu-

lationen) möglich werden (Görgen). Schadprogramme können Computerdaten verschlüsseln und unbrauchbar machen (Schönbohm). Für die Gesellschaft existenziell bedrohlich sind Gefährdungen kritischer Infrastrukturen (Görgen, Schieferdecker, Grund) wie etwa digitale Sabotage der Energieversorgung von Krankenhäusern oder anderen Einrichtungen der öffentlichen sowie privaten Daseinsvorsorge und gehören mittlerweile zum Spektrum des Denkbaren.

Im Alltag dominieren die „Kommunikationsdelikte" wie Cybermobbing, Beleidigungen, Hatespeech, Cyberstalking, aber auch Cybergrooming und Sexting (Stückmann, Hajok). Strafrechtlich sind viele Sachverhalte nicht immer eindeutig, zudem gibt es Grenzverlagerungen des Normalitätsempfindens insbesondere bei Kindern und Jugendlichen (Rüdiger). Weiterhin senken Anonymität und Distanz zum Geschädigten die Hemmschwelle für kriminelles Handeln (Görgen, Wrede).

Weitere Delikte werden genannt: Kinderpornografie im Netz, Identitätsdiebstähle, Handel mit illegalen Gütern, Morddrohungen, Spionage (Heesen, Ungefuk). Die verschlüsselten Vernetzungsmöglichkeiten der Täter sind eine ständige Herausforderung für die Sicherheitsbehörden (Roggenkamp).

Die Digitalisierung hat also viele neue Herausforderungen für die Sichehreitsbehörden geschaffen. Kriminalitätsformen haben sich durch die Digitalisierung verändert. Kriminelle setzen Mittel der Informationstechnologie ein, um herkömmliche Straftaten zu begehen. Zudem sind neue Straftaten hinzugekommen, die ohne Digitalisierung nicht möglich wären (Ungefuk).

Auch Gefährdungen der Freiheitsrechte bleiben nicht unerwähnt (Belina). Probleme, die eigentlich gesellschaftlicher Natur sind, sollten nicht mit technischer Überwachung gelöst werden, bei der zudem das Gewinninteresse von Unternehmen eine Rolle spielen kann. Durch blinden Technikglauben werden eher neue Probleme geschaffen als gelöst (Demuth).

Chancen der Digitalisierung

Die Experten/-innen betonen die Chancen von Digitalisierung für den Einzelnen und die Gesellschaft insgesamt, verweisen dabei auf die Aspekte der Phänomenbeschreibung und wenden sich schwerpunktmäßig den neuen Möglichkeiten für die Prävention und Gefahrenabwehr zu. Das Spannungsfeld von Sicherheit und Freiheit kommt dabei nicht zu kurz.

Digitale Kompetenz der Nutzer/-innen, sichere Schutzsoftware/Antivirenscanner für Computer und smarte Anwendungen sowie angemessene Überwachungstechnik und -maßnahmen der Sicherheitsbehörden umfassen den Handlungsrahmen.

Digitalisierung ermöglicht Wohlfahrtsgewinne (Schönbohm), persönliche Autonomie sowie frühzeitige Chancen zu Partizipation und Mitbestimmung (Hajok). Hier gilt es anzuknüpfen, um Kinder und Jugendliche z. B. im schulischen Kontext untereinander zu möglichen Risiken bzw. Gefährdungen in Diskurs zu bringen. Durch gezielte Informationen über die Tragweite und die Folgen insbesondere des eigenen digitalen Handelns wird Selbstreflexion sowie ein kritischer Medienumgang angeregt. Dabei helfen Peer-to-Peer-Ansätze (Hajok) oder Gamification (Schönbohm). Auch Webinare z. B. zur Prävention von Cybermobbing erzielen Reichweite (Stückmann).

Technischer Selbstschutz beginnt etwa mit Biometrie zur Entsperrung des Smartphones sowie durch die

17 Experten/-innen aus sechs Fachdisziplinen

Kriminologie

Professor Dr. **Bernd Belina** ist kritischer Kriminologe und forscht und lehrt am Institut für Humangeographie an der Goethe Universität in Frankfurt a. M. Professor Dr. **Thomas Görgen** leitet das Fachgebiet „Kriminologie und interdisziplinäre Kriminalprävention" an der Deutschen Hochschule der Polizei in Münster. Dr. **Thomas-Gabriel Rüdiger** ist Cyberkriminologe und Dozent am Institut für Polizeiwissenschaft (IfP) der Hochschule der Polizei des Landes Brandenburg.

Informatik

Professorin Dr.-Ing. **Ina Schieferdecker** leitet die Abteilung „Forschung für technologische Souveränität und Innovationen" beim Bundesministerium für Bildung und Forschung (BMBF). **Dennis Schirrmacher** ist Redakteur von Europas größtem Magazin für Computertechnik c't und schreibt vor allem zu Sicherheitsthemen. **Arne Schönbohm** ist Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Professorin Dr.-Ing. **Britta Wrede** lehrt an der Universität Bielefeld und leitet die Forschungsgruppe „Angewandte Informatik" am Exzellenzcluster Kognitive Interaktionstechnologie (CITEC).

Geisteswissenschaften

Kerstin Demuth ist Campaignerin und Redakteurin beim Digitalcourage e. V. Sie setzt sich für den Schutz persönlicher Daten ein und ist netzpolitisch engagiert. Prof. Dr. **Daniel Hajok** ist Honorarprofessor an der Universität Erfurt und ausgewiesener Experte und Gutachter im Bereich des Kinder- und Jugendmedienschutzes. Privatdozentin Dr. **Jessica Heesen** ist Leiterin des Forschungsschwerpunkts Medienethik und Informationstechnik an der Eberhard-Karls-Universität Tübingen. Sie beschäftigt sich mit Problemen der Meinungsfreiheit in sozialen Medien ebenso wie mit Fragen nach einer wertorientierten Entwicklung von künstlicher Intelligenz.

Pädagogik

Gregory Grund ist Erziehungswissenschaftler und seit 2010 mit Florian Borns und Jörg Schüler selbstständig im Bereich Medienerziehung aktiv. Seit 2013 begleitet er das Projekt Digitale Helden. 2013 veröffentlichte er mit Barbara Kettl-Römer das Buch „99 Tipps Social Media". **Gesa Stückmann** ist Rechtsanwältin in Rostock und bearbeitet seit 2007 Fälle von Cybermobbing und hält daneben ehrenamtlich Vorträge an Schulen in Mecklenburg-Vorpommern, seit 2013 via Webinar bundesweit: rund 1200 Webinare mit ca. 70 000 Teilnehmer/-innen.

Psychologie

Professorin Dr. **Judith Ackermann** forscht und lehrt zu digitalen und vernetzten Medien in der sozialen Arbeit an der Fachhochschule Potsdam. Professorin Dr. **Pia Knoeferle** – Direktorin des Instituts für deutsche Sprache und Linguistik an der Humboldt Universität zu Berlin – forscht zum Sprachverstehen.

Rechtswissenschaften

Professor Dr. **Christoph Gusy** von der Universität Bielefeld ist unter anderem Experte für Informations- und Datenschutzrecht und war einer der Beschwerdeführer der Verfassungsbeschwerde gegen die Vorratsdatenspeicherung. Professor Dr. **Jan Dirk Roggenkamp** von der HWR Berlin ist Prozessbevollmächtigter bei der Verfassungsbeschwerde gegen die Online-Durchsuchung. Sein Forschungsschwerpunkt liegt in den rechtlichen Implikationen der IT-gestützten Polizeiarbeit, insbesondere im Bereich der Bekämpfung/Verhütung von Cybercrime. **Georg Ungefuk** ist Oberstaatsanwalt und Sprecher der Generalstaatsanwaltschaft Frankfurt am Main.

Nutzung von Warn- und Hilfs-Apps (Görgen). Sicherheitsgefühl, Rechtswahrung und Anzeigebereitschaft der Nutzer/-innen können etwa durch „sichtbare" Polizeipräsenz im Netz angehoben werden (Rüdiger). Über digitale Medien lassen sich zudem Präventionsempfehlungen mit großer Reichweite in die Öffentlichkeit multiplizieren (Ungefuk)

Die Sicherheitsbehörden erweitern ihr Portfolio von intelligenter biometrischer Videoüberüberwachung, Ortungstechnik, algorithmischer Datenanalyse, Predictive Policing bis hin zu heimlicher Kommunikations- und Endgeräteüberwachung (Roggenkamp) und vernetzen sich dabei zunehmend (Ungefuk). Zentrale Sicherheitsbehörden wie Bundeskriminalamt (BKA) oder Bundesamt für Sicherheit in der Informationstechnik (BSI) gewinnen durch ihr gebündeltes Know-How, ihre personelle sowie technische Ausstattung an Bedeutung und auch private Internetprovider werden stärker einbezogen (Gusy).

Damit die technischen Entwicklungen im Gemeinwohlinteresse bleiben, hat die Bundesregierung das Rahmenprogramm „Forschung für die zivile Sicherheit von 2018 bis 2023" aufgelegt (Schieferdecker). Bei Kriminalitätsprävention im Digitalen geht es schließlich immer um das Spannungsfeld zwischen Freiheit und Kontrolle. Die Fragen lauten: Wie viel Kontrolle wollen wir, brauchen wir, um uns zu schützen, und wie viel Freiheit können wir uns dabei erlauben? (Grund). In einem Rechtsstaat sind seine Amtsträger gehalten, dass der Einsatz dieser Überwachungstechnologien nur in einem Maße stattfindet, wie es die Verfassung und insbesondere die Persönlichkeitsrechte der Menschen zulassen (Roggenkamp). Risiken zum digitalen Totalitarismus (Schieferdecker) sind stets von allen politischen und gesellschaftlichen Akteuren im Auge zu behalten.

Vision Smart Prevention

Visionen beschreiben eine gewünschte mittel- bis langfristige Zukunft, die für die Visionäre gestaltbar scheint und ggf. für sie erlebbar sein kann (Kahl).

Digitalisierung ist zukünftig ein Thema, das in allen Kontexten von Bildung und Erziehung berücksichtigt werden muss (Hajok). Smart Prevention meint kluge Präventionsansätze sowohl im technischen als auch sozialen Sinne. Sie sollte auf gutes Wissen über Wirkungen und Nebenwirkungen von Präventionsansätzen gestützt sein. Es gibt in einigen Bereichen belastbare Erkenntnisse über evidenzbasierte Programme und Strategien (Görgen). Ihre systematische Verwendung wäre eine Vision. Smarte Individualkompetenz (Belina) meint, dass jeder Einzelne besser bewusste Risikoentscheidungen treffen und sich sicher und selbstbewusst in der digitalen Welt bewegen kann (Schönbohm, Schieferdecker, Schirrmacher).

KI-gestützte Anwendungen zur positiven Verhaltensunterstützung durch sogenannte Assistenztechnologie („technische Erziehung") könnte ausprobiert werden, ohne die Gefahren und Grenzverletzungen durch Manipulation zu vernachlässigen (Wrede). Es kommt darauf an, sich auf das zu konzentrieren, was für das soziale Zusammenleben wirklich Sinn macht (Hajok). Technik soll dabei dem Menschen dienen und nicht einschränken (Demuth). Digitale Medien und Technologien haben eine dienende Funktion zur gesellschaftlichen Integration und Wohlfahrt (Heesen).

Digitale Vernetzung ermöglicht Synergieeffekte der Präventionsakteure (Stückmann) und begünstigt auch einen globalen Level der funktionierenden Zusammenarbeit der zur Gefahrenabwehr und Straftatenverhütung berufenen Stellen (Roggenkamp). Sicherheitsherstellung und Freiheitsgewährleistung bedürfen ausgewogener Regulierung und einen öffentlichen Diskurs darüber (Gusy). Das Grundrecht auf informationelle Selbstbestimmung ist so wenig wie möglich einzuschränken (Roggenkamp).

Eine smarte Vision ist zuletzt, die Macht privater gewinnorientierter Akteure wie Internet- und Plattformprovider einzugrenzen und sich immer ihrer Einflussnahmen auf Politik, Gesellschaft und jeden Einzelnen bewusst zu sein. (Demuth).

Fazit

Der textlichen Zusammenführung ging eine synoptische Aufbereitung wesentlicher Aussagen (vgl. Online-Ausgabe) voraus. Die Auswahl der angeführten Argumente erfolgte nach verständiger Betrachtung in recht kurzer Zeit. Sie ist intuitiv-subjektiv und wird den Experten/-innen nicht immer gerecht, einige Aspekte sind untergegangen. Ich bitte dafür um Nachsicht. Alle Beiträge können in voller Länge gesehen, gehört und gelesen werden (https://www.smart-prevention.de/).

Aus meiner Sicht ist die größte Herausforderung, alle gesellschaftlichen Milieus in das digitale Zeitalter in einer Art und Weise mitzunehmen, dass sich digitales Gefälle abbaut und eine soziale Spaltung nicht weiter verschärft wird. Allen Verantwortlichen wünsche ich dabei gutes Gelingen und die notwendige gegenseitige Unterstützung.