STIFTUNG DATENSCHUTZ

Kurzgliederung

1. Kurze begriffliche Einordnungen
   - KI, Machine Learning, unüberwachtes Lernen, Data mining
2. Datafizierung der Gesellschaft
3. **Generative Adversarial Networks & synthetic data**
4. **Datenschutzrechtliche Bewertung der Synthetisierung**
5. Ausblick

Begriffliche Einordnungen 1

Künstliche Intelligenz

The AI-Effect

“AI is whatever machines haven´t done yet.”

Larry Tesla´s Theorem

Quelle: https://commons.wikimedia.org/wiki/File:Freilichtmuseum_Finsterau_Kapplhof_7.jpg; Urheber: Aconcagua, Lizenz: GFDL, Cc-by-sa-3.0

Begriffliche Einordnungen 2

Der Algorithmus:

Eine eindeutige Handlungsvorschrift zur Lösung eines Problems oder einer Klasse von Problemen. Ein Algorithmus besteht aus endlich vielen, wohldefinierten Einzelschritten

9	1
8	2
6	3
7	4
1 →	5
5	6
2	7
3	8
4	9
10	10

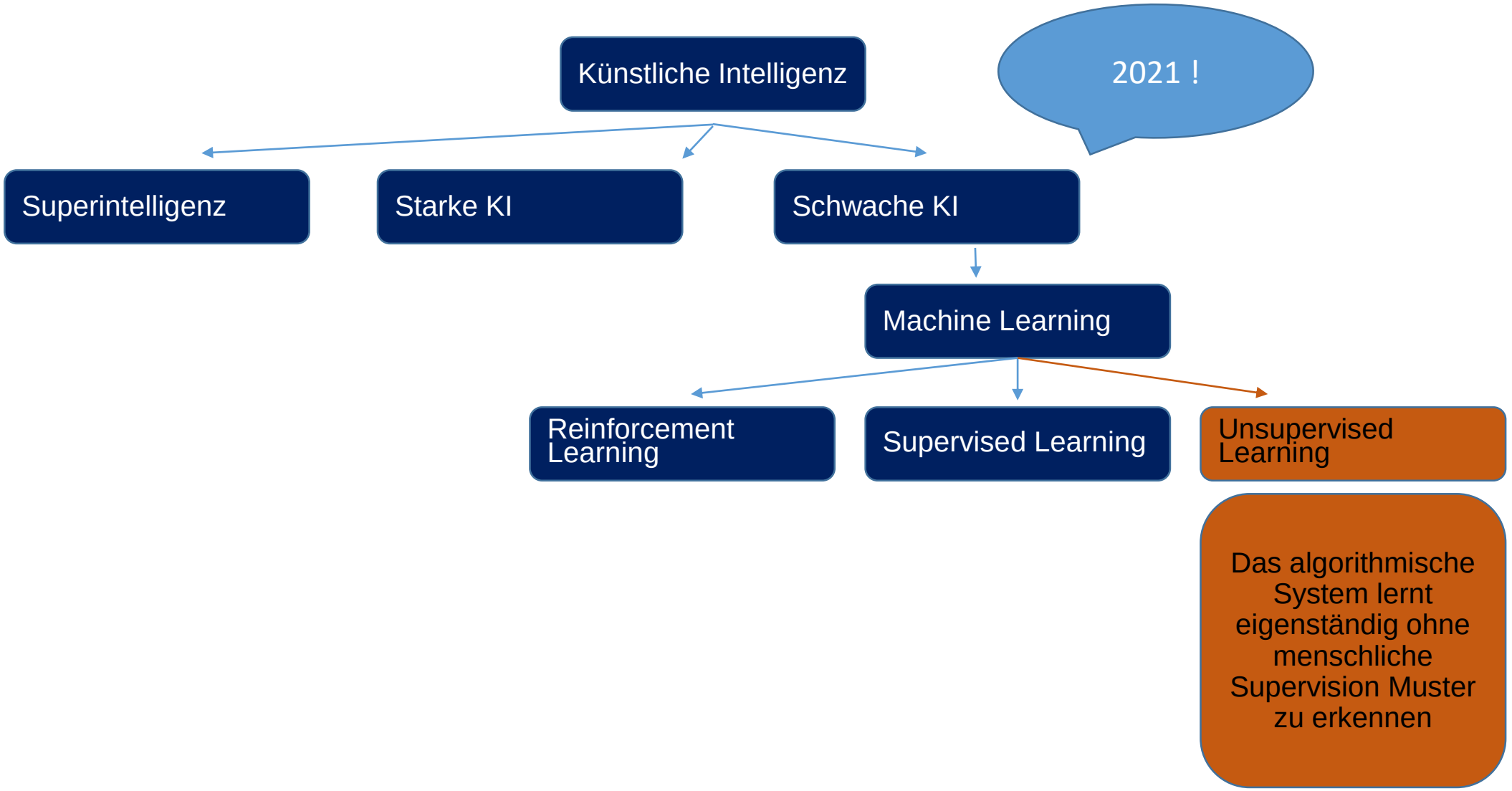
ZUTATEN
7 cl weißer Rum
3 cl frischer Limettensaft
2 BL feiner, weißer Rohrzucker
ZUBEREITUNG
1. Zutaten in den Shaker geben
2. Mit Eiswürfeln auffüllen und sehr kräftig (mind. 20 Sekunden) schütteln
3 Ins vorgekühlte Glas abseihen.
GLAS
Coupette
GARNITUR
Keine

Quelle: https://cocktails.mixology.eu/cocktail/daiquiri-rezept/

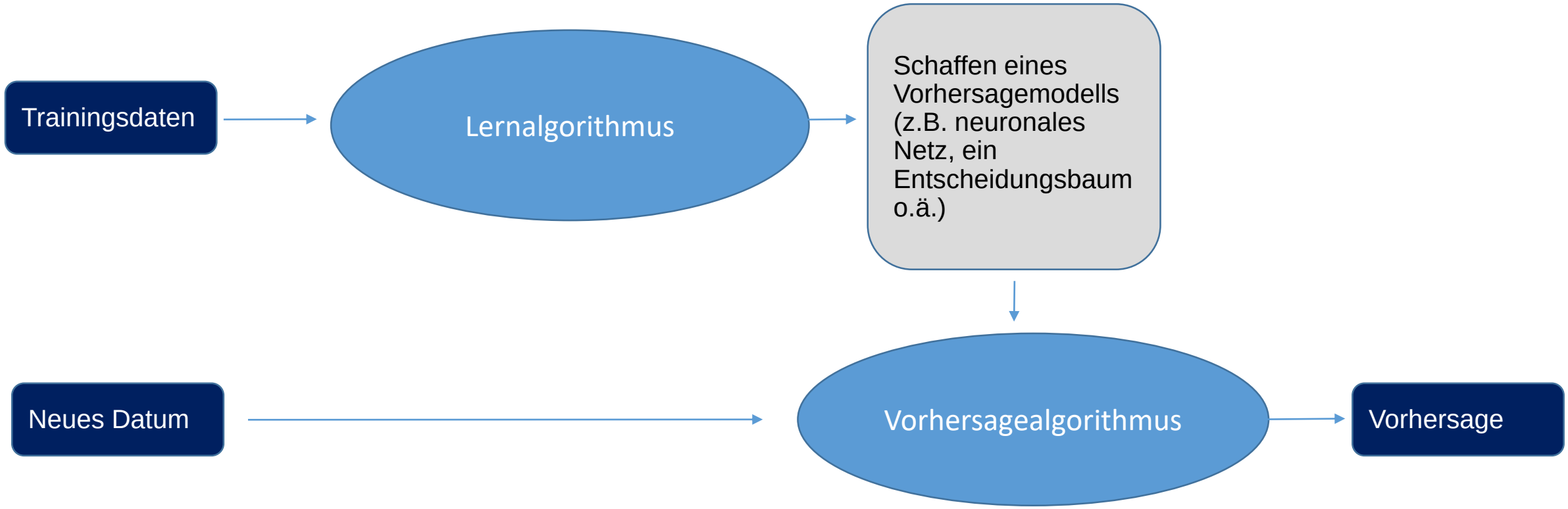
Das Polanyi – Paradoxon

„Wir können mehr wissen, als wir sagen können“

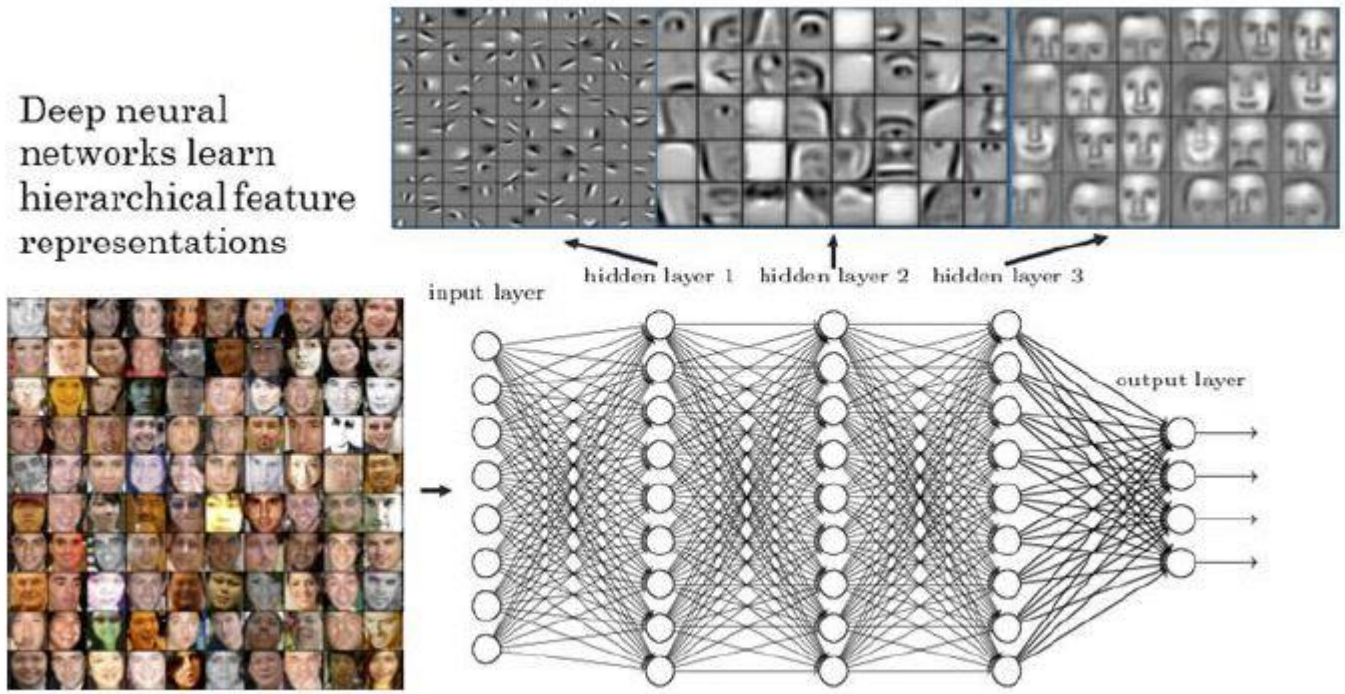
Übersicht KI & Lernstile



KI ist ein algorithmisches System

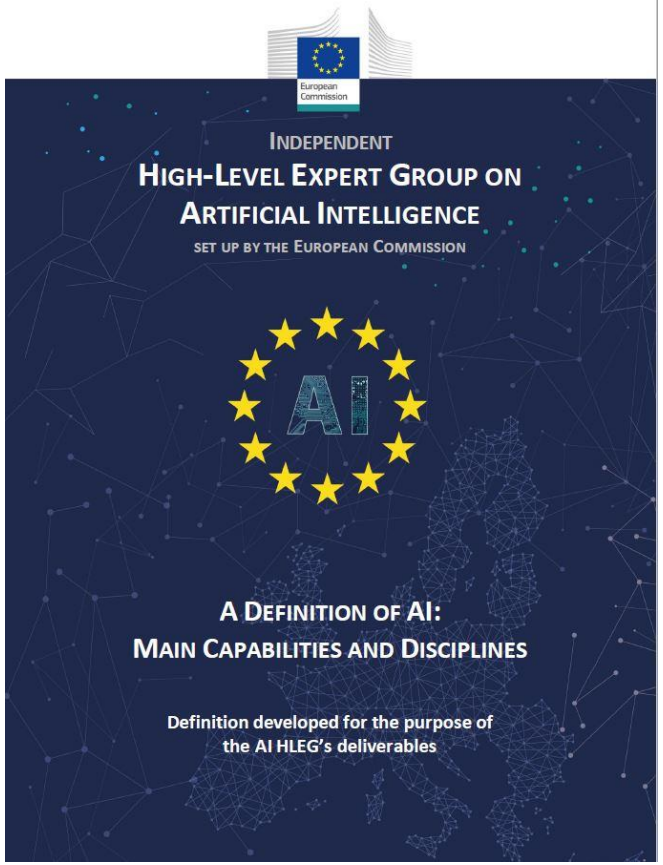


Deep neural networks learn hierarchical feature representations



Sartor, 2020

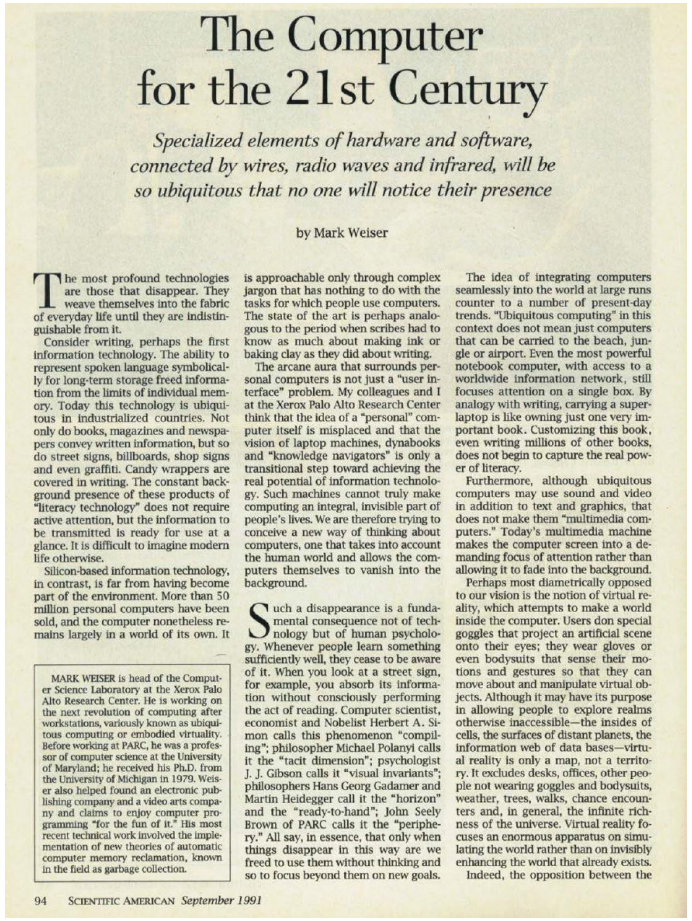
Definitionen



HLEG 08.04.2019

"We propose the following updated definition of AI: AI systems are software (and possibly hardware) systems **designed by humans** that, given **a complex goal**, act in the physical or digital dimension **by perceiving their environment through data acquisition**, interpreting the collected structured or unstructured data, reasoning on knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they **can also adapt their behavior by analysing how the environment is affected by their previous actions.** As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, and the integration of all other techniques into cyber-physical systems)."

Treibstoff der Maschine: Daten



The Computer for the 21st Century

Specialized elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence

by Mark Weiser

The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

Consider writing, perhaps the first information technology. The ability to represent spoken language symbolically for long-term storage freed information from the limits of individual memory. Today this technology is ubiquitous in industrialized countries. Not only do books, magazines and newspapers convey written information, but so do street signs, billboards, shop signs and even graffiti. Candy wrappers are covered in writing. The constant background presence of these products of "literacy technology" does not require active attention, but the information to be transmitted is ready for use at a glance. It is difficult to imagine modern life otherwise.

Silicon-based information technology, in contrast, is far from having become part of the environment. More than 50 million personal computers have been sold, and the computer nonetheless remains largely in a world of its own. It is approachable only through complex jargon that has nothing to do with the tasks for which people use computers. The state of the art is perhaps analogous to the period when scribes had to know as much about making ink or baking clay as they did about writing.

The arcane aura that surrounds personal computers is not just a "user interface" problem. My colleagues and I at the Xerox Palo Alto Research Center think that the idea of a "personal" computer itself is misplaced and that the vision of laptop machines, dynabooks and "knowledge navigators" is only a transitional step toward achieving the real potential of information technology. Such machines cannot truly make computing an integral, invisible part of people's lives. We are therefore trying to conceive a new way of thinking about computers, one that takes into account the human world and allows the computers themselves to vanish into the background.

Such a disappearance is a fundamental consequence not of technology but of human psychology. Whenever people learn something sufficiently well, they cease to be aware of it. When you look at a street sign, for example, you absorb its information without consciously performing the act of reading. Computer scientist, economist and Nobelist Herbert A. Simon calls this phenomenon "compiling"; philosopher Michael Polanyi calls it the "tacit dimension"; psychologist J. J. Gibson calls it "visual invariants"; philosophers Hans Georg Gadamer and Martin Heidegger call it the "horizon" and the "ready-to-hand"; John Seely Brown of PARC calls it the "periphery." All say, in essence, that only when things disappear in this way are we freed to use them without thinking and so to focus beyond them on new goals.

The idea of integrating computers seamlessly into the world at large runs counter to a number of present-day trends. "Ubiquitous computing" in this context does not mean just computers that can be carried to the beach, jungle or airport. Even the most powerful notebook computer, with access to a worldwide information network, still focuses attention on a single box. By analogy with writing, carrying a superlaptop is like owning just one very important book. Customizing this book, even writing millions of other books, does not begin to capture the real power of literacy.

Furthermore, although ubiquitous computers may use sound and video in addition to text and graphics, that does not make them "multimedia computers." Today's multimedia machine makes the computer screen into a demanding focus of attention rather than allowing it to fade into the background.

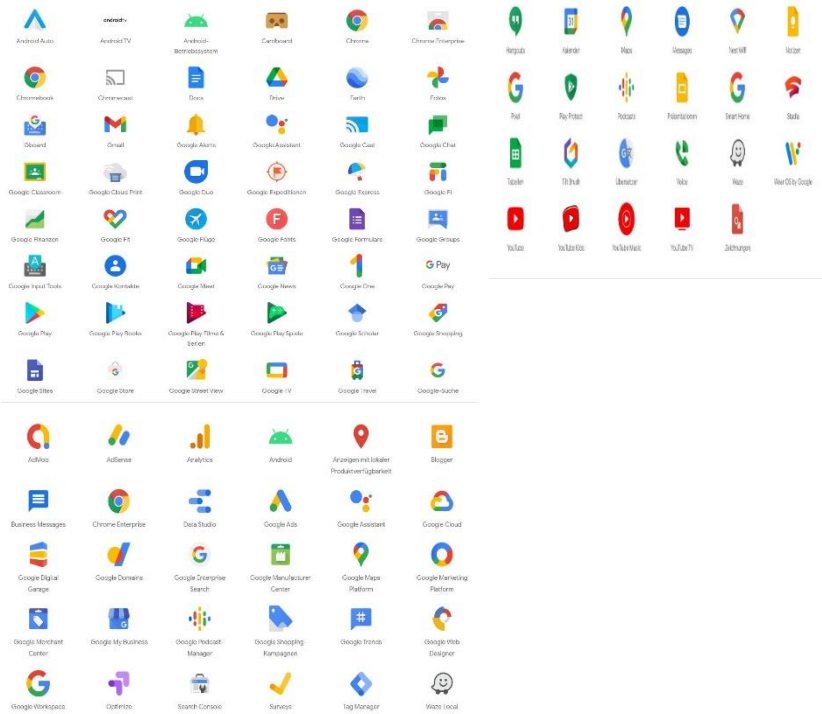
Perhaps most diametrically opposed to our vision is the notion of virtual reality, which attempts to make a world inside the computer. Users don special goggles that project an artificial scene onto their eyes; they wear gloves or even bodysuits that sense their motions and gestures so that they can move about and manipulate virtual objects. Although it may have its purpose in allowing people to explore realms otherwise inaccessible—the insides of cells, the surfaces of distant planets, the information web of data bases—virtual reality is only a map, not a territory. It excludes desks, offices, other people not wearing goggles and bodysuits, weather, trees, walks, chance encounters and, in general, the infinite richness of the universe. Virtual reality focuses an enormous apparatus on simulating the world rather than on invisibly enhancing the world that already exists.

Indeed, the opposition between the

MARK WEISER is head of the Computer Science Laboratory at the Xerox Palo Alto Research Center. He is working on the next revolution of computing after workstations, variously known as ubiquitous computing or embodied virtuality. Before working at PARC, he was a professor of computer science at the University of Maryland; he received his Ph.D. from the University of Michigan in 1979. Weiser also helped found an electronic publishing company and a video arts company and claims to enjoy computer programming "for the fun of it." His most recent technical work involved the implementation of new theories of automatic computer memory reclamation, known in the field as garbage collection.

- Ubiquitäre Computerisierung
- Bereitwilligkeit „kostenlose“ Technologie zu nutzen
- Effizienzmaximierung

„The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.“



Datenschutzgebote und Diskriminierungsverbote

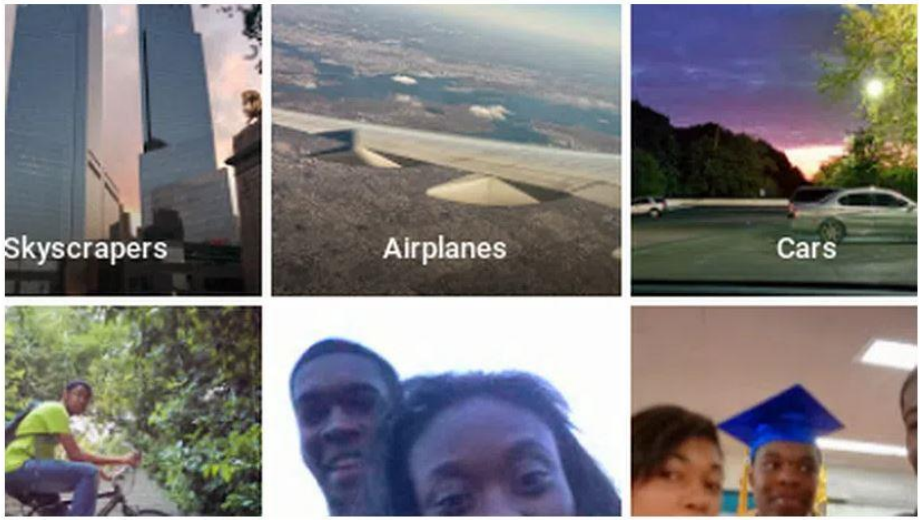
Gesichtserkennung

"Meine Freundin ist kein Gorilla"

Die Bilderkennung von Diensten wie Google und Flickr ist beeindruckend. Aber es ist schlimm, wenn aus falsch erkannten Bildern rassistische Beleidigungen werden.

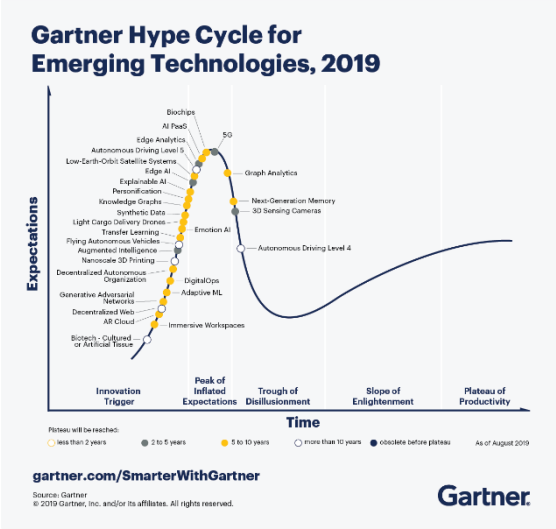
Von **Eike Kühl**

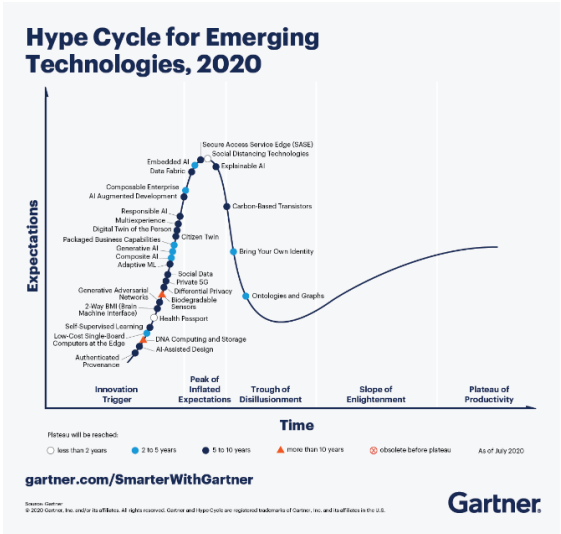
2. Juli 2015, 17:38 Uhr / 123 Kommentare /



Googles neuer Foto-Dienst kategorisierte eine Freundin von Jacky Alciné als Gorilla. © CC BY-ND 2.0 Jacky Alciné / Twitter

Synthetische Daten





Quelle: https://thispersondoesnotexist.com/

Generative Adversarial Networks (GAN)

A generative adversarial network (GAN) has two parts:

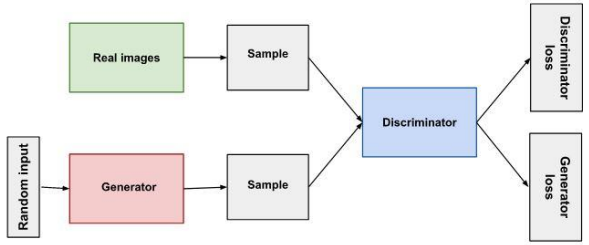
- The **generator** learns to generate plausible data. The generated instances become negative training examples for the discriminator.
- The **discriminator** learns to distinguish the generator's fake data from real data. The discriminator penalizes the generator for producing implausible results.

When training begins, the generator produces obviously fake data, and the discriminator quickly learns to tell that it's fake:

As training progresses, the generator gets closer to producing output that can fool the discriminator:

Finally, if generator training goes well, the discriminator gets worse at telling the difference between real and fake. It starts to classify fake data as real, and its accuracy decreases.

Here's a picture of the whole system:



Both the generator and the discriminator are neural networks. The generator output is connected directly to the discriminator input. Through backpropagation, the discriminator's classification provides a signal that the generator uses to update its weights.

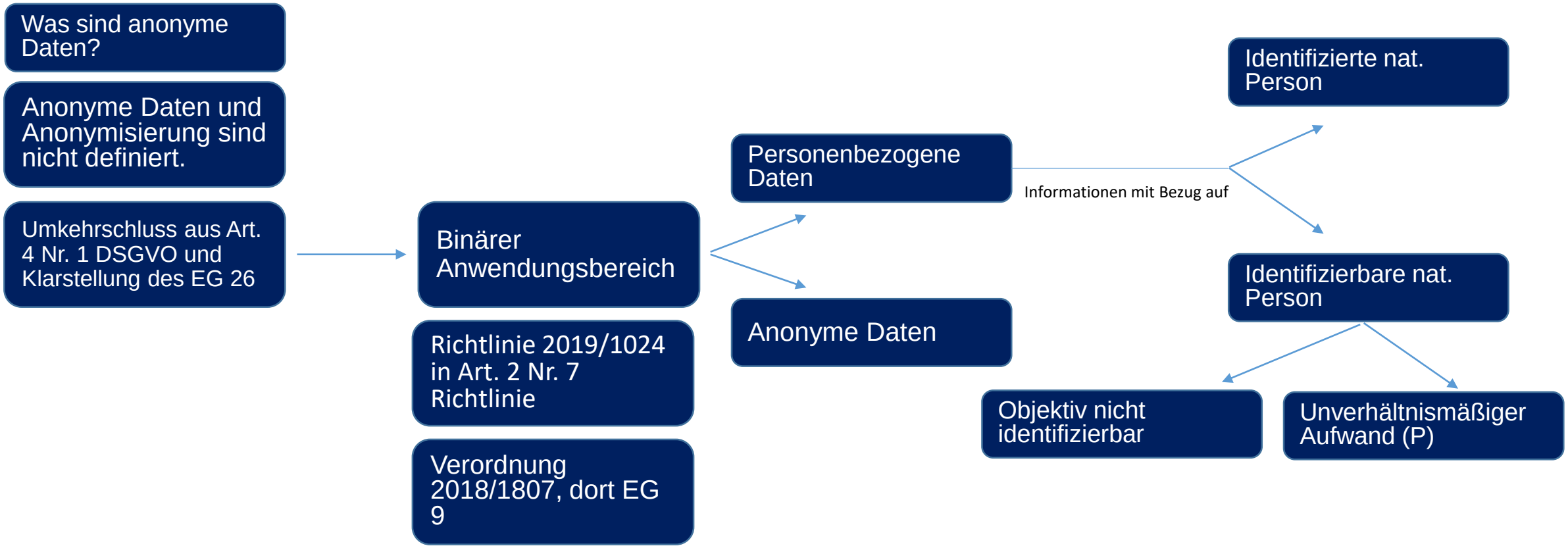
Ian Goodfellow et. al NiPS 2014

Portions of this page are reproduced from work created and shared by Google and used according to terms described in the Creative Commons 4.0 Attribution License, https://developers.google.com/machine-learning/gan/gan_structure

Vorteile und Herausforderungen synthetischer Daten

- Erhöhter Schutz für die Rechte und Freiheiten von Betroffenen
- Beliebiges Produzieren möglich, um z.B. ungewöhnliche Datenkonstellationen zu testen
- Weitergabe an Dritte ermöglicht Kollaborationen mit Geschäftspartnern
- Verbreitung von KI-Systemen hat Einfluss auf den Mittelstand
- Wert synthetischer Daten bleibt erhalten
- Herausforderung: Bewahrung der Anonymität

Synthetisierung als Anonymisierung



Anonymisierung als Verarbeitung

1. Entfernen des Personenbezugs ist eine Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO.
2. Privilegierung der Anonymisierung durch eine teleologische Reduktion des Art. 4 Nr. 2?
3. Es ist eine DSFA durchzuführen
4. Ist auch auf den Zweck der Nutzung in anonymer Form i.R.d. Art. 6 Abs. 4 DSGVO abzustellen?
5. Überführung in die Anonymität ist die zweckändernde Weiterverarbeitung, die an Art. 6 Abs. 4 DSGVO zu messen ist.
6. Daraus folgt kein grundrechtsfreier Raum
7. Rechtsgrundlagen können sich ergeben aus Art. 6, Art. 9 DSGVO sowie Art. 89 Abs. 2 DSGVO i.V.m. nationalen Vorschriften.

Ausblick

- **AI made in Europe soll werteorientiert sein**
- **Um emerging technologies nutzbar machen zu können, ist ein Ordnungsrahmen notwendig, der die Interessen von Betroffenen und Verantwortlichen im Blick hat**
- **Die DSGVO ermöglicht einen solchen Weg einzuschlagen**

Vielen Dank für Ihre Aufmerksamkeit.