kaspersky

Künstliche Intelligenz im Spannungsfeld von Datenschutz, Regulierung und Cybersicherheit: Was die Politik vorhat und wie die jungen Menschen in Deutschland über KI denken

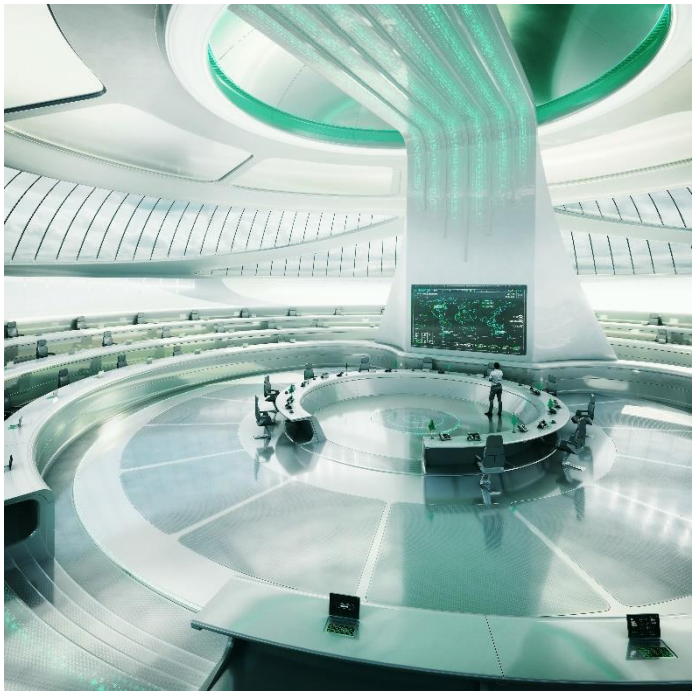
Teil 6 der Kaspersky-Report-Serie über die Generation KI

Dezember 2020

kaspersky

KI im Spannungsfeld von Datenschutz, Regulierung und Cybersicherheit: Was die Politik vorhat und wie die Jugend in Deutschland darüber denkt

Künstliche Intelligenz (KI), Algorithmen und Machine Learning bestimmen bereits heute den Alltag von uns Bürgerinnen und Bürgern. Was für uns heute schon sehr futuristisch anmutet, ist wohl nur ein Vorgeschmack auf die Welt der Zukunft. Kaspersky hat in seiner groß angelegten Studie unter 1.000 jungen Menschen in Deutschland (16 bis 30 Jahre) die Erwartungen der Generation KI – derjenigen also, die eine von KI stärker geprägte Welt wohl noch hautnah erleben werden – an die Politik in puncto Transparenz und Datenschutz sowie neuen Möglichkeiten durch KI bei Cyberschutz abgefragt. Derzeit adressieren sowohl die Europäische Union (EU) als auch die Bundesregierung die Themen KI, Internet der Dinge und Robotik intensiv. Das Ziel der Bundesregierung: die Etablierung eines auf europäischen Werten und Regeln



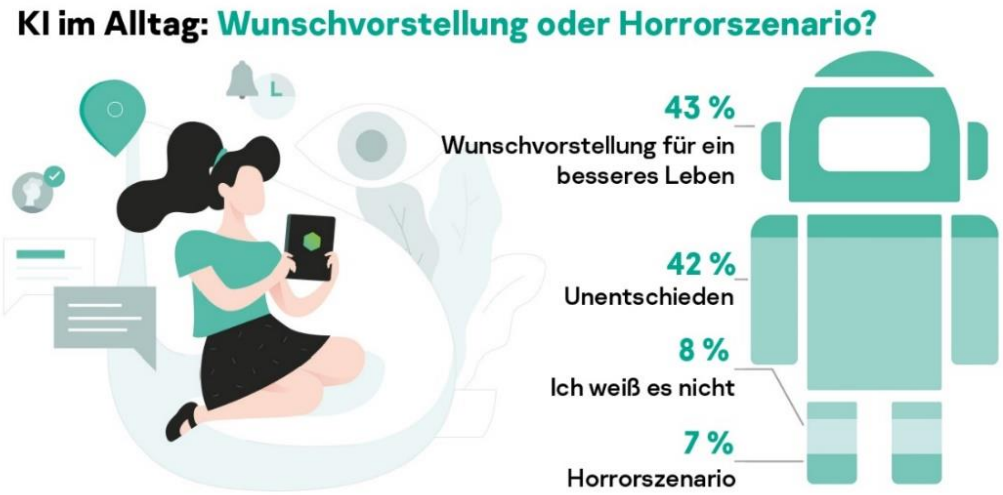
basierenden KI-Ökosystems, das bei gleichzeitiger Transparenz für die Bürgerinnen und Bürger die Vorteile dieser Technologie für Wirtschaft und Gesellschaft erschließt. Wie sollte Regulierung und Kontrolle für KI aussehen? Und wie steht die Generation KI dem zunehmenden Einfluss von Zukunftstechnologien gegenüber? Der folgende Bericht gibt einen aktuellen Überblick darüber, wie die Politik die Rolle und Regulierung von KI in Wirtschaft und Gesellschaft vermittelt – immer mit dem dazu passenden Wahrnehmungsbarometer der Generation KI, also der jungen Bundesbürger.

Kaspersky-Studie zur Generation KI

Die Online-Umfrage wurde von Arlington Research im Auftrag von Kaspersky im Februar 2020 durchgeführt. Dabei wurden 1.000 deutsche Nutzer im Alter von 16 bis 30 Jahren zu ihrer Wahrnehmung und gegenwärtigen, beziehungsweise zukünftigen Verwendung von Geräten oder Systemen mit Künstlicher Intelligenz (KI) befragt. Die Umfrage ist repräsentativ für Deutschland nach Geschlecht und Wohnort (Bundesland). Mehr unter https://www.kaspersky.de/KI

Ziel der Befragung war es, diejenigen Menschen zu befragen, die privat und beruflich voraussichtlich am meisten mit Künstlicher Intelligenz (KI) zu tun haben werden – die unter 31-Jährigen, also die **Generation KI.**

Generell scheinen die jungen Bundesbürger Künstlicher Intelligenz gegenüber überwiegend positiv eingestellt zu sein. So ist für viele (42,6 Prozent) KI sogar eine Wunschvorstellung für ein besseres Leben. Für lediglich 7,2 Prozent ist es ein Horrorszenario. 41,8 Prozent sind hier noch unentschlossen und 8,4 Prozent wissen es nicht.



KI, Transparenz und Datenschutz im Blick der Politik und der Jungwähler

Die **EU-Kommission** hat sich Anfang des Jahres 2020 auf Grundprinzipien für die Regulierung von Künstlicher Intelligenz (KI) im Rahmen eines **Weißbuchs** verständigt. In Einsatzbereichen mit hohem Risiko wie Gesundheit, Polizei oder Verkehr sollen KI-Systeme transparent und nachvollziehbar sein, heißt es im europäischen KI-Konzept. Laut dem Weißbuch werden die Gefahren von KI für die Cybersicherheit, die Privatsphäre und den Schutz persönlicher Daten vom EU-Gesetzgeber bislang nicht ausreichend adressiert. Auch bei der Haftung müsse noch nachgebessert werden.

Die **Bundesregierung** reagierte am 29. Juni 2020 mit einer nationalen Stellungnahme. Im Zentrum des Papieres steht der geplante EU-Rechtsrahmen beim Einsatz Künstlicher Intelligenz. Das Thema ist dringlich: Schon heute werden KI-Systeme in Industrie, Wirtschaft und bei staatlichen Institutionen eingesetzt: Etwa in Form virtueller Assistenten, beim Einsatz von Spamfiltern, bei der Personalauswahl, im Kreditscoring oder in der medizinischen Diagnostik.

- ➔ **Das Potential von KI in der Medizin sehen auch die jungen Bundesbürger unter 31 Jahre**. So ist laut der Kaspersky-Befragung die Mehrheit (54,4 Prozent) der Generation KI der Meinung, dass der Einsatz von KI-Technologien in der Medizin (zum Beispiel bei der Früherkennung) mehr Leben retten könnte als es heute der Fall ist. Auch ist nahezu die Hälfte der Befragten (49,9 Prozent) der Auffassung, dass die Medizin künftig stark von KI beeinflusst werden wird, Diagnosen frühzeitiger getroffen und Medikamente schneller entwickelt werden können.

Die Bundesregierung hat es sich laut der Stellungnahme zum Ziel gemacht, eine verantwortungsvolle, gemeinwohlorientierte und menschenzentrierte Entwicklung und Nutzung von KI sowie die Förderung von Wettbewerbsfähigkeit und Innovation in der Europäischen Union voran zu bringen. Um möglichen Risiken wirksam zu begegnen, seien konkrete Anforderungen an die Entwicklung und den Einsatz von KI-Systemen zu stellen. Hierzu gehören insbesondere ein risikoadäquates Maß an Transparenz, Nachvollziehbarkeit und Datenschutz sowie, falls erforderlich, eine angemessene Kontrollstruktur und Überprüfbarkeit von KI-Anwendungen und ihren Ergebnissen. Normung und Standardisierung können dabei zur Beschleunigung von Entwicklungsprozessen, zur Rechtssicherheit für Unternehmen und zur weiteren Vertrauensbildung der Menschen in die Technologie beitragen.

- ➔ Diese Maßgabe deckt sich mit den Erkenntnissen der Kaspersky-Studie. Die befragten Millenials und die Generation Z sind sich einig: Sollten KI, smarte Geräte und Roboter zunehmend Teil des privaten wie des beruflichen Lebens werden, sind politische Regulierung, Transparenz und Datenschutz essenziell. **So sind 43 Prozent der Meinung, Deutschland benötige ein eigenes Ministerium für Künstliche Intelligenz.** Die überwiegende Mehrheit (55,5 Prozent) ist zudem der Auffassung, dass eine weitreichende Akzeptanz für KI nur im Falle kompletter Transparenz hinsichtlich deren Aufgaben und Einsatzgebieten erreicht werden kann. Nichtsdestotrotz ist sich bereits heute fast die Hälfte (43,9 Prozent) sicher, dass durch den Einsatz von KI zukünftig eine genauere und schnellere Erkennung sowie Bekämpfung von IT-Bedrohungen möglich sein wird – sich die Cybersicherheit also generell durch einen verstärkten Einsatz von KI-Technologien verbessern würde.

Die Bundesregierung begrüßt in ihrer Stellungnahme zum Weißbuch der Europäischen Kommission die darin enthaltenen Ansätze. Federführend haben die drei für die nationale KI-Strategie zuständigen Ministerien für Forschung (BMBF), Wirtschaft (BMWi) und Arbeit (BMAS) sowie die „Datenethikministerien“ des Inneren (BMI) und für Justiz und Verbraucherschutz (BMJV) die Stellungnahme verfasst. Bei der konkreten Umsetzung zeigen sich jedoch Unterschiede. So hatte die Europäische Kommission vorgeschlagen, spezielle Anforderungen nur an KI-Systeme mit „hohem Risiko“ zu legen. Dagegen „erachtet die Bundesregierung ein Klassifikationsschema aus mehr als zwei Stufen für angebracht“.

Die **Enquete-Kommission „Künstliche Intelligenz** – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“ hatte in ihren Empfehlungen der Bundesregierung ein Modell mit fünf Stufen vorgeschlagen. Dabei sollte ein Großteil der KI-Systeme mit voraussichtlich geringem Schädigungspotenzial keiner Regulierung unterliegen, weitere drei Risikoklassen abgestuften Regulierungen und nur KI-Systemen mit extrem hohem Schädigungspotenzial die Marktzulassung generell verwehrt bleiben. Der **Abschlussbericht der Enquete Kommission** wurde am 28. Oktober 2020 an Bundestagspräsident Wolfgang Schäuble übergeben. Der Bericht steht unter dem Leitbild „menschzentrierte KI“. Für die Kommission bedeutet das, „dass KI-Anwendungen vorrangig auf das Wohl und die Würde der Menschen ausgerichtet sein und einen gesellschaftlichen Nutzen bringen sollen“. Auch fordert sie den Aufbau einer europäischen Infrastruktur und weist auf die Gefahr der

Diskriminierung hin. Die Vorlage wurde vom Parlament mit großer Mehrheit angenommen. Die Ergebnisse und Empfehlungen können nun für die Arbeit der Fraktionen herangezogen werden.

Am 20. Oktober 2020 hat das **Europäische Parlament drei Berichte** angenommen, in denen dargelegt wird, wie die EU Künstliche Intelligenz am besten regulieren kann, um Innovationen, ethische Standards und das Vertrauen in neue Technologien zu fördern. Darin werden Vorschläge zu den Aspekten Ethik, Haftung bei KI-bedingten Schäden und das Recht des geistigen Eigentums dargelegt. Das Europäische Parlament will so den Weg für erste EU-Regeln zu Künstlicher Intelligenz ebnen.

Auch die EU-Abgeordneten stellen klar, dass der Mensch im Zentrum der neuen Regeln stehen solle. Im Vorfeld eines **Vorschlags der Europäischen Kommission** zu KI, der für Anfang 2021 erwartet wird, hat das Parlament einen „Sonderausschuss für künstliche Intelligenz im digitalen Zeitalter“ eingesetzt, um die Auswirkungen Künstlicher Intelligenz auf die europäische Wirtschaft zu analysieren.

Um die Auswirkungen von KI – in diesem Fall auf die Arbeitswelt – zu prüfen, wurde bereits im Auftrag des Bundesministeriums für Arbeit und Soziales in Berlin ein KI-Observatorium eröffnet, das sich umfänglich mit dieser Thematik beschäftigt.

- **Arbeitswelt 5.0 aus Sicht der Generation KI**: Knapp die Hälfte (48,6 Prozent) der von Kaspersky befragten jungen Menschen in Deutschland glaubt, dass KI mehr Raum für Kreativität und Kommunikation schaffen könnte, weil sie monotone und sich ständig wiederholende Tätigkeiten im Job übernehmen kann. Im selben Atemzug sind die Befragten jedoch auch überwiegend (39,7 Prozent) der Meinung, in zehn Jahren für dasselbe Gehalt weniger arbeiten zu müssen, da KI unliebsame Aufgaben für sie übernehmen könne (ebenfalls 23,8 Prozent sind unentschlossen). Allerdings sehen die Befragten auch die Gefahr, von einer KI im eigenen Berufsumfeld wegrationalisiert zu werden. Ebenfalls eine Mehrheit (54,5 Prozent) ist der Auffassung, dass KI die Art und Weise künftiger Arbeit revolutionieren und neue Jobprofile schaffen wird.

Ein sensibles Thema seien laut Stellungnahme der Deutschen Bundesregierung KI-Anwendungen für die so genannte „biometrische Fernidentifikation“, umgangssprachlich Gesichtserkennung. Die Bundesregierung begrüßt, dass Systeme für biometrische Fernidentifikation aufgrund ihrer besonderen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger besondere Aufmerksamkeit erfahren. Soweit sie eingesetzt werden sollen, müssten zuvor klare gesetzliche Anforderungen formuliert werden.

- Die von Kaspersky befragte Generation KI in Deutschland begrüßt zum Beispiel mehrheitlich die Vorzüge einer durch KI immer intelligenter werdenden städtischen Infrastruktur. **Sie hätten keine Bedenken, Gesichtserkennung zur Verbesserung der öffentlichen Sicherheit in Kauf zu nehmen** (37,2 Prozent).

Ein weiterer Punkt, den die deutsche Regierung in ihrer Stellungnahme hervorhebt: Die Erreichung der Ziele des europäischen Green Deals mithilfe von KI.

- Die Hälfte der befragten Menschen zwischen 16 und 30 Jahre (51,2 Prozent) fände es sehr positiv, wenn **durch Technologien wie KI die Umwelt geschont** würde.

kaspersky

Haupterkenntnisse der Kaspersky-Studie von eintausend Befragten in Deutschland zwischen 16 und 30 Jahre: Sowohl auf europäischer als auch auf nationaler Ebene werden die Themen Transparenz und Datenschutz für KI adressiert. Damit kommt die Politik der Einstellung der jungen Bundesbürger unter 31 Jahre entgegen. Denn sowohl die Generation Z als auch die Millenials sind sich einig: Sollten KI, smarte Geräte und Roboter zunehmend Teil des privaten wie beruflichen Lebens werden, sind politische Regulierung, Transparenz und Datenschutz essenziell. Gleichzeitig sehen sie die Chance einer durch KI verbesserten Umwelt.

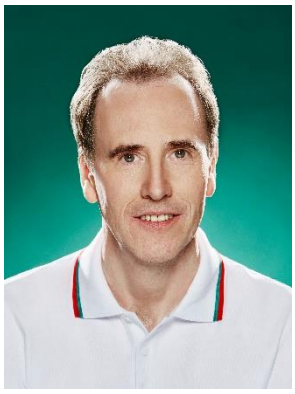
Übrigens: Das Zutrauen in die KI-Kompetenz der Bundesrepublik könnte größer sein. So sagen 44,3 Prozent, dass KI-Technologie in anderen Ländern weiter fortgeschritten sei, und sie dadurch Deutschland im weltweiten Wettbewerb im Nachteil sähen.

KI ein Plus im Kampf für mehr Datenschutz und IT-Sicherheit?

Laut der Kaspersky-Befragung glauben 40,5 Prozent der jungen Menschen unter 31 Jahren in Deutschland, dass KI den Schutz persönlicher Daten und der eigenen digitalen Identität auf ein neues Level heben wird. Der Grund: KI sei weniger fehleranfällig als der Mensch (z.B. würde es voraussichtlich weniger durch Menschen verursachte Daten-Leaks geben). Auch würden 43,9 Prozent es befürworten, wenn eine KI alles, was mit Datenschutz und IT-Sicherheit im eigenen digitalen Leben zu tun hat, bestmöglich regelte. 43,9 Prozent sind zudem der Meinung, dass KI eine noch größere Cybersicherheit gewährleisten könne, da sie Hackerangriffe noch genauer vorhersehen und besser abwehren könnte als dies bisher der Fall sei.

- ➔ Der Abschlussbericht (Seite 238) der Enquete Kommission Künstliche Intelligenz sieht das ähnlich: „… Die Integrität und Sicherheit digitaler Strukturen, Technologien und Produkte ist zunehmend Grundlage allen öffentlichen und gesellschaftlichen Lebens. **Die IT-Sicherheit wird daher in immer mehr Bereichen zur staatlichen Aufgabe und Verantwortung**, für deren Wahrnehmung auch auf Lösungen aus dem Bereich KI und lernende künstliche Systeme zurückgegriffen werden kann. …“
- ➔ Weiter müssen laut dem Bericht (Seite 203) ADM-Systeme (Algorithmische Entscheidungssysteme) staatlicher Einrichtungen technisch robust sein und **hohen Anforderungen an die IT-Sicherheit (Security by Design)** erfüllen.
- ➔ Der Bericht (Seite 241) empfiehlt für die IT-Sicherheit folgendes: „… Die Analyse der Schwachstellen lernender künstlicher Systeme und möglicher Angriffsvektoren steht noch am Anfang. **Daher ist** hier **vor allem** dringend **mehr Forschung in diesem Bereich notwendig.** Zusätzlich sollte das Bundesamt für Sicherheit in der Informationstechnik (BSI) seine Kapazitäten in diesem Bereich weiter ausbauen (…). **Die Enquete-Kommission empfiehlt dem Deutschen Bundestag daher, die Forschungsförderung verstärkt auf die Frage der IT-Sicherheit von lernenden KI-Systemen auszurichten**. Außerdem sollte das BSI hierzu ausgebaut werden und **entsprechende Schutzvorgaben und Mindeststandards festschreiben.**

Ein Blick auf die IT-Sicherheitsbranche zeigt, dass die Vorstellung der jungen Bundesbürger und auch die Einschätzung der Enquete-Kommission Künstliche Intelligenz bezüglich des Einsatzes von KI-Einsatz im Bereich Cybersicherheit, sehr nahe an die Realität reicht. So spielen KI und auf Machine Learning basierende Algorithmen bereits heute eine bedeutende Rolle im Schutz vor Cyberbedrohungen und optimieren die Identifizierung von Online-Gefahren maßgeblich. Allerdings sollten sich Anbieter, Betreiber und Verantwortliche von Systemen, in denen Künstliche Intelligenz oder Machine Learning zum Einsatz kommen, darüber im Klaren sein, wo innerhalb dieser komplexen IT-Architekturen die zwingend zu schützenden Schwachpunkte liegen und diese dann direkt im Prozess der Entwicklung über einen Security-by-Design-Ansatz absichern.

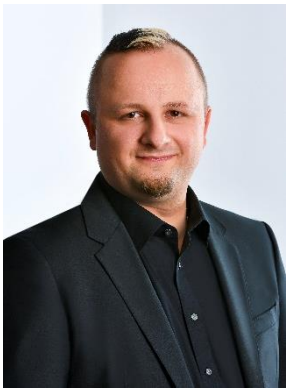


„Stellen Sie sich eine Zukunft vor, in der wir tatsächlich Technologie entwickeln können, die die Fähigkeit hat, Aufgaben nachzugehen, die wir nicht selbst erledigen können. Doch was passiert, wenn Künstliche Intelligenz über den Menschen hinausgeht, wir sie also nicht überwachen können und nicht über die Gehirnkapazität verfügen, um die Informationen zu speichern, so wie KI es kann? Dazu werden wir nicht in der Lage sein, wenn sie uns die richtige Antwort liefert. Bei einem Taschenrechner ist das in Ordnung; da wissen wir, wann eine Antwort falsch ist. Bei einigen dieser fortschrittlichen maschinellen Lernsysteme ist das nicht der Fall. Was ist, wenn Sie nicht feststellen können, ob die Ausgabe gültig ist oder nicht? Die Frage der Maschinensteuerung wird immer wichtiger und muss stets als Element jeder Weiterentwicklung von KI-Systemen betrachtet werden. Ab einem bestimmten Punkt müssen Menschen möglicherweise Abschaltmechanismen in KI einbauen, um die Sicherheit der Maschinen zu gewährleisten, ähnlich wie die Sicherheitsvorkehrungen bei Kernkraftwerken."

David Emm, Principal Security Researcher bei Kaspersky

„Wer KI nur im Bereich der Science-Fiction verortet, sollte sich bewusstmachen, dass bereits heute Machine Learning und Algorithmen – als Vorstufe zu starker, also kognitiver KI – in zahlreichen Anwendungen Standard sind. Als IT-Sicherheitsexperte liegen uns die Themen Cybersicherheit und Datenschutz bei einer so wichtigen Zukunftstechnologie wie Künstlicher Intelligenz besonders am Herzen – denn ohne adäquate digitale Schutzmaßnahmen ist sie zum Scheitern verurteilt. Bei KI-Systemen gilt, was beim Internet der Dinge (IoT) zum Teil verpasst wurde: Datenschutz und Security by Design, beziehungsweise Cyberimmunität, müssen von Beginn an ein Teil der Überlegungen sein. Um die Wichtigkeit von Security innerhalb der Diskussion rund um Machine Learning und Künstliche Intelligenz in den Vordergrund zu stellen, haben wir diejenige Gruppe in der Bevölkerung befragt, die privat wie beruflich voraussichtlich am meisten damit zu tun haben wird – die unter 31-Jährigen."

Marco Preuß, Leiter des europäischen Forschungs- & Analyseteams bei Kaspersky



Das Kaspersky-Whitepaper „AI under Attack" zeigt, was Anbieter von Machine Learning und KI aus Perspektive der IT-Sicherheit umsetzen sollten.

Aber auch für Verbraucher ist es wichtig, sich in naher Zukunft auf Datenschutzbelange und durch KI verstärkte Cyberangriffe vorzubereiten. Allein die zunehmende Verbreitung intelligenter Geräte zeigt verstärkt, dass Anwender – um deren vollen Funktionsumfang zu nutzen – dazu neigen, auch persönliche Daten preiszugeben. Die Konsequenz: Solange KI immer stärker in vielen Bereichen des täglichen Lebens Einzug hält, wächst auch das Bedrohungspotential. So sollten sich Nutzer darauf einstellen, dass es zu Social Engineering und Deep Fakes auf einem bislang nie gekannten Niveau kommen wird.

Im August 2019 wurde beispielsweise eine KI dazu genutzt, sich als die Stimme des CEO eines britischen Energieunternehmens auszugeben, um einen angeblich dringenden Geldtransfer zu fordern – ein sehr ausgefeilter Deep-Fake, der schwer von einer menschlichen Aktion zu unterscheiden war. Wenn immer intelligentere Roboter und smartere Systeme Teil des Alltags werden, hat das ebenfalls Auswirkungen auf die IT-Sicherheit und die Infrastruktur von Unternehmen (siehe Kaspersky-Report 2020 „Faceless workspaces? The effect of smart robotics on cybersecurity and business") .

Report-Reihe Generation KI

Kaspersky präsentiert seine Erkenntnisse aus der Umfrage im Rahmen einer Reihe thematischer Kurzreports, die unter https://kas.pr/generation-ki kostenfrei abrufbar sind und sich mit den folgenden Themen befassen:

- Generation KI - Nutzung, Wissen und Wahrnehmung
- Generation KI - Smart Cities und Klimaschutz
- Generation KI - Liebe und Privatleben
- Generation KI - Schöne neue Jobwelt?
- Generation KI - Auswirkungen auf die Zukunft
- Generation KI - Datenschutz, Regulierung und Cybersicherheit

www.kaspersky.de/
www.securelist.com