ethos

Ethos Engagement Paper

Digitale Verantwortung der Unternehmen

>20 JAHRE | NACHHALTIGE ANLAGEN

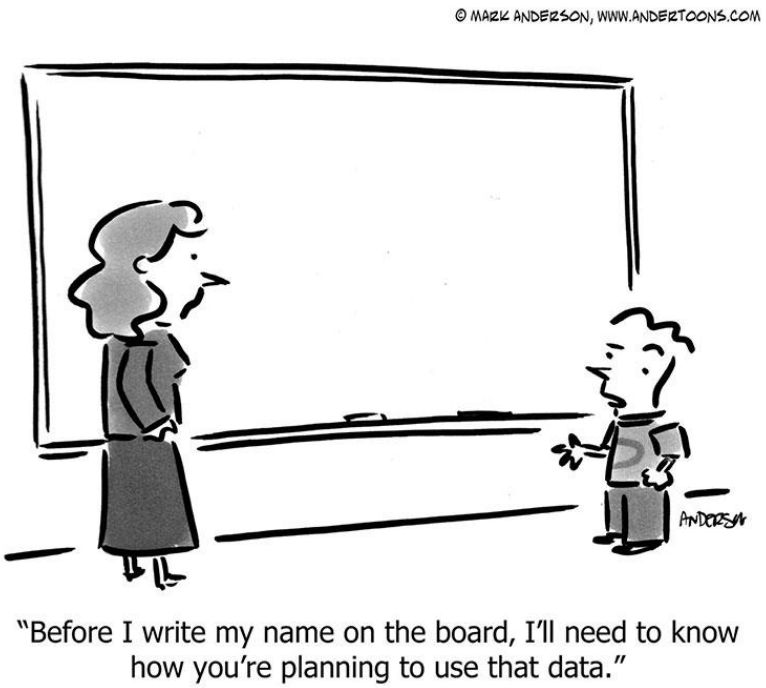
November 2020

Die Ethos Stiftung schliesst mehr als 220 schweizerische Pensionskassen und andere steuerbefreite Institutionen zusammen. Sie wurde 1997 zur Förderung einer nachhaltigen Anlagetätigkeit und eines stabilen und gesunden Wirtschaftsumfelds gegründet.

Das Unternehmen Ethos Services betreut Beratungs- und Vermögensverwaltungsmandate für nachhaltige Anlagen. Ethos Services bietet institutionellen Investoren nachhaltige Anlagefonds, Analysen von Generalversammlungen mit Stimmempfehlungen, ein Programm für den Aktionärsdialog mit Unternehmen sowie Nachhaltigkeits-Ratings und -Analysen von Unternehmen an. Ethos Services ist Eigentum der Ethos Stiftung und mehrerer Mitgliedsinstitutionen der Stiftung.

www.ethosfund.ch

Dieses Engagement Paper stützt sich insbesondere auf die von Jean-Henry Morin (Universität Genf), Johan Rochel (Ethix Lab for Innovation Ethics) und Eva Thelisson (AI Transparency Institute) geleiteten Arbeiten. White paper, *Towards a Digital Responsibility Index*, Veröffentlichung im Dezember 2020 vorgesehen.



«Bevor ich meinen Namen auf die Tafel schreibe, muss ich wissen, wie Sie beabsichtigen, diese Daten zu verwenden.»

Gedruckt auf «RecyStar»,100% Altpapier ohne optische Aufheller.

Inhalt

1 Einführung 2

1.1 Kontext 2

1.2 Überblick über die Erwartungen von Ethos 2

2 Herausforderungen der Digitalisierung 3

2.1 Digitale Governance 3

2.2 Digitale Transparenz 3

2.3 Datenverwaltung und Cybersicherheitspolitik 3

2.4 Algorithmen und künstliche Intelligenz 5

2.5 Sensible Produkte und Dienstleistungen 6

2.6 Soziale Auswirkungen 7

2.7 Umweltauswirkungen 7

3 Erwartungen von Ethos 9

Grundsatz 1: Implementierung eines Kodex für digitale Verantwortung 9

Grundsatz 2: Sicherstellung der Transparenz gegenüber den Anspruchsgruppen 10

Grundsatz 3: Einhaltung der höchsten Standards der Datenverarbeitung und des Datenschutzes 10

Grundsatz 4: Implementierung ethischer Grundsätze bei der Nutzung der künstlichen Intelligenz (KI) ... 10

Grundsatz 5: Ausschluss sensibler Aktivitäten im Zusammenhang mit der Digitalisierung 11

Grundsatz 6: Gewährleistung einer gerechten und verantwortungsvollen sozialen Transformation 11

Grundsatz 7: Beitrag zur Reduzierung des ökologischen Fussabdrucks der digitalen Technologien 12

1 Einführung

1.1 Kontext

Die Digitalisierung ist neben dem Klimawandel und den zunehmenden sozialen Ungleichheiten eine der drei grossen gesellschaftlichen Herausforderungen des 21. Jahrhunderts. Sie bietet den Unternehmen und ihren Aktionären ein beträchtliches Potenzial an wirtschaftlicher Entwicklung, das oft als vierte industrielle Revolution bezeichnet wird. Über die Produktivitätssteigerungen traditioneller Industrien hinaus hat die Digitalisierung innerhalb von 20 Jahren zur Entwicklung der Technologiegiganten geführt, die in den USA allgemein GAFAM genannt werden (Google, Amazon, Facebook, Apple und Microsoft). Ende September 2020 erreichte deren kumulierte Marktkapitalisierung annähernd 6000 USD, was 14% des Weltindexes MSCI World ausmacht, während die Kapitalisierung der 54 Unternehmen des Energiesektors weniger als 3% dieses Indexes beträgt.

Diese digitale Revolution bringt auch neue Herausforderungen für Unternehmen und ihre Aktionäre mit sich. Unter den zahlreichen Skandalen hat besonders der Fall Cambridge Analytica aufgezeigt, was für Missbräuche sich aus der Nutzung privater Daten für kommerzielle und politische Zwecke ergeben können. Das bringt neue ethische, rechtliche, finanzielle und reputationsbezogene Risiken mit sich.

Angesichts der Auswirkungen der Digitalisierung auf die Wirtschaft und die Gesellschaft im Allgemeinen ist Ethos der Ansicht, dass dieses Thema ein wichtiges Element von verantwortungsbewussten Investitionen und Analysen im Bereich Umwelt, Soziales und Governance (ESG) geworden ist. Unternehmen aus allen Branchen müssen proaktiv sein und Richtlinien für die digitale Verantwortung erlassen. Dieses Konzept setzt voraus, dass die Unternehmen die Herausforderungen der Digitalisierung breit und umfassend identifizieren und Management-und Übergangsstrategien einführen, welche die Interessen all ihrer Anspruchsgruppen (Stakeholder) berücksichtigen.

1.2 Überblick über die Erwartungen von Ethos

Die Ethos Stiftung hat zum Ziel, nachhaltige Investitionen sowie ein stabiles und gesundes Wirtschaftsumfeld zu fördern. Deshalb misst sie Fragen der Wirtschaftsethik und der guten Corporate Governance besondere Bedeutung bei.

Ethos plädiert für die Umsetzung einer Strategie für die digitale Verantwortung der Unternehmen, die umfassend ist und alle in Kapitel 2 dieses Dokuments aufgeführten Punkte berücksichtigt. Die verschiedenen Erwartungen von Ethos an die Unternehmen werden in Kapitel 3 detailliert beschrieben.

Die Grundsätze von Ethos für die digitale Verantwortung

1. Einen Kodex für digitale Verantwortung umsetzen
2. Die Transparenz gegenüber den Anspruchsgruppen bezüglich der digitalen Praktiken und des digitalen Fussabdrucks sicherstellen
3. Die höchsten Standards der Datenverarbeitung und des Datenschutzes einhalten
4. Ethische Grundsätze für die Nutzung der künstlichen Intelligenz (KI) festlegen
5. Sensible Aktivitäten in Zusammenhang mit der Digitalisierung ausschliessen
6. Eine gerechte und verantwortungsvolle soziale Transformation gewährleisten
7. Zur Verringerung des ökologischen Fussabdrucks der digitalen Technologien beitragen

2 Herausforderungen der Digitalisierung

2.1 Digitale Governance

Bei der Definition der Strategie und der Identifizierung geschäftlicher Risiken muss die Digitalisierung berücksichtigt werden. Voraussetzung dafür ist eine Anpassung der Corporate Governance und die regelmässige Überwachung der technologischen Entwicklungen, die sich auf das Unternehmen auswirken können, durch den Verwaltungsrat. Dies betrifft sowohl die Produkte und Dienstleistungen des Unternehmens als auch die Herstellungs-, Liefer- und Vertriebsmethoden. Dies setzt voraus, dass die Relevanz der Strategie überwacht wird, indem die mit der Digitalisierung verbundenen Risiken und Chancen regelmässig berücksichtigt werden.

Wegen des disruptiven Charakters und der raschen Entwicklung der Technologien muss der Verwaltungsrat sicherstellen, dass das Unternehmen ausreichende Mittel in diesen Bereich investiert und dabei die höchsten ethischen, ökologischen und sozialen Standards respektiert. Angesichts der Komplexität der Fragen muss der Verwaltungsrat dafür sorgen, dass er über die notwendigen Kenntnisse verfügt. Er muss auch darauf achten, dass die Geschäftsleitung diese verschiedenen Fragen regelt sowie Richtlinien und Verfahren einführt, die den besten Praktiken entsprechen.

2.2 Digitale Transparenz

Unternehmen müssen Benutzer und Betroffene über die Erhebung personenbezogener Daten informieren. Diese Transparenz ist unverzichtbar, aber keineswegs allgemein üblich. Die Benutzer sind sich der Speicherung und Verwendung ihrer Daten nicht immer bewusst. Unternehmen sollten diese Transparenz deshalb proaktiv nutzen, um ein Vertrauensverhältnis herzustellen. Die gespeicherten Daten sollten durch freie und informierte Zustimmung («opt in») erhalten werden.

Unternehmen müssen es den Benutzern ihrer Dienstleistungen und Produkte ermöglichen, die über sie gesammelten Daten leicht abzurufen und mit ihnen zu interagieren (sie also zu ändern oder zu löschen). Diese Nutzerautonomie muss von den Unternehmen so weit wie möglich erleichtert werden.

Bestimmte Daten können sehr wertvoll sein. Es ist daher unerlässlich, dass die Unternehmen, die diese Daten besitzen, die höchsten Sicherheitsstandards anwenden, um zu verhindern, dass sie vermarktet, weitergegeben oder gestohlen werden.

Sollten die Daten trotz allem von einem unbefugten Dritten genutzt worden sein, müssen sich die Unternehmen verpflichten, die Inhaber dieser Daten unverzüglich zu informieren. Letztere müssen nämlich in der Lage sein, Massnahmen zu ergreifen, um zu verhindern, dass sie Opfer eines Missbrauchs ihrer persönlichen Daten werden (Betrug, Lösegelderpressung, Verwendung von Passwörtern oder Kreditkarten, Profilerstellung usw.).

2.3 Datenverwaltung und Cybersicherheitspolitik

Daten sind heute ein zentrales Element für den Erfolg vieler Unternehmen. Das gilt vor allem für Unternehmen aus dem Technologie- und Werbesektor, sie sind jedoch bei weitem nicht die einzigen. Tatsächlich ist jedes Unternehmen, das Daten über seine Kunden, Mitarbeiter, Lieferanten, Aktionäre oder Konkurrenten besitzt, in die Verwendung oder gegebenenfalls die Vermarktung der Daten involviert.

Die Bedeutung der Daten für Unternehmen und die Wirtschaft wird zu einer Herausforderung für die Cybersicherheit und die Regulierung.

A. Reglementierung in Sachen Datenschutz

Der Missbrauch privater Daten hat einige Staaten dazu veranlasst, neue Regeln dafür aufzustellen, wie Daten gespeichert, verwaltet und genutzt werden. So ist in Europa 2018 die «Datenschutz-Grundverordnung»[1] (DSGVO) in Kraft getreten. Dieses europäische Gesetz geht viel weiter als die

[1] http://gdpr-text.com/de/read/article-1/

meisten entsprechenden Gesetzgebungen weltweit und erkennt die Sensibilität des Themas an. Unternehmen, die innerhalb der EU tätig sind oder Daten von EU-Bürgern verarbeiten, müssen darauf achten, dass sie diese Gesetzgebung einhalten. Verstösse gegen die DSGVO können mit erheblichen Geldbussen von bis zu 20 Millionen Euro oder 4% des Gesamtumsatzes geahndet werden.

Nach mehr als dreijähriger Diskussion hat das Schweizer Parlament im September 2020 eine Modernisierung des Bundesgesetzes über den Datenschutz (DSG)[2] mit dem Ziel verabschiedet, es mit dem System der DSGVO kompatibel zu machen. Das Schweizer Gesetz verstärkt den Rahmen des Nutzerschutzes und die Informationspflicht der Unternehmen. Beide Texte stimmen bezüglich der 7 Prinzipien im Zusammenhang mit der Datenerhebung überein. Diese betreffen Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Zweckbindung, Genauigkeit, Sicherheit und Transparenz. Die beiden Gesetze unterscheiden sich jedoch in mehreren Aspekten, insbesondere im Hinblick auf die Sanktionen. Das DSG sieht auch finanzielle Sanktionen vor, die weit niedriger als jene der EU sind. Es ist zum jetzigen Zeitpunkt ungewiss, ob die EU eine Äquivalenz akzeptieren wird. Schweizer Unternehmen haben deshalb ein klares Interesse daran, die Best Practices sowie die höchsten regulatorischen Standards einzuhalten und die DSGVO freiwillig zu übernehmen.

Kalifornien hat mit dem am 1. Januar 2020 in Kraft getretenen California Consumer Privacy Act[3] ebenfalls ein Datenschutzgesetz erlassen, das mehrere Schlüsselelemente der DSGVO übernimmt, darunter vor allem die Bestimmungen zur Transparenzpflicht bei der Erhebung von Daten, bei Datendiebstahl und zum Schutz der privaten Daten.

B. Schutz der Privatsphäre

Die Nutzung der Daten ermöglicht es Unternehmen, den Benutzern personalisierte Dienstleistungen anzubieten oder diese Daten Dritten zu kommerziellen Zwecken zur Verfügung zu stellen. Die Auswertung privater Daten hat denn auch einigen Unternehmen die Entwicklung neuer Geschäftsmodelle ermöglicht und insbesondere den Dienstleistungssektor revolutioniert. Die daraus resultierende Personalisierung der Dienstleistungen kann positiv und vorteilhaft für die Benutzer sein, birgt aber häufig die Gefahr, dass sie auf Kosten des privaten Charakters gewisser Daten erfolgt. Gezielte Werbung ist ein Beispiel dafür, dass Daten oft unter Verletzung der Privatsphäre der Anspruchsgruppen eines Unternehmens verwendet werden. In weniger als einem Jahrzehnt sind Google und Facebook durch die privaten Daten, die ihnen zur Verfügung stehen, zu führenden Akteuren der Werbung geworden und teilen sich heute einen Grossteil der Einnahmen in diesem Sektor.

Die Personalisierung von Dienstleistungen auf der Grundlage privater Daten sollte eine Entscheidung des betroffenen Benutzers sein und nicht die Standardoption für Dienste («privacy by default»). Geräte und Dienste, die private Daten verwenden, sollten so konzipiert sein, dass sie die Privatsphäre respektieren und die Daten nicht automatisch nutzen können («privacy by design»). Dieses Konzept ist übrigens ein Schlüsselelement der DSGVO.

C. Minimierung der Daten

Der Grundsatz des Schutzes der Privatsphäre erfordert, Datenverarbeitungssysteme so zu konzipieren, dass sie so wenig personenbezogene Daten wie möglich verarbeiten (Datenminimierung). Die Standardeinstellungen sind daher datenschutzfreundlich zu gestalten, der Zugang zu personenbezogenen Daten auf das für die Bereitstellung der Dienstleistung unbedingt erforderliche Mass zu beschränken und Instrumente zur Verfügung zu stellen, die es den Benutzern ermöglichen, ihre persönlichen Daten besser zu schützen (z.B. durch Zugangskontrollen, Verschlüsselung).

D. Cybersicherheit

Cyberkriminalität ist eines der grössten Risiken, mit denen Organisationen jeder Grösse und in allen Sektoren derzeit konfrontiert sind. Cyberangriffe können sogar das Überleben mancher Unternehmen beeinträchtigen und

[2] https://www.parlament.ch/centers/eparl/curia/2017/20170059/Schluzssabstimmungstext%203%20NS%20D.pdf

[3] http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

erfordern die Mobilisierung erheblicher Ressourcen, um die Cybersicherheit und die Pläne für die Systemwiederherstellung zu gewährleisten.

Cyberkriminalität kann verschiedene Ursprünge haben, die von böswilliger Absicht bis hin zur Spionage reichen. Die häufigsten Ziele sind Organisationen, die von finanziellem Interesse sein können, wie Banken oder Organisationen, die grosse Datenmengen sammeln und speichern. Allerdings können alle Unternehmen Opfer von Veruntreuung, Datenverschlüsselung gegen Lösegeld, Missbrauch von Zahlungssystemen oder Zerstörung von wichtigen Firmendatenbanken und -programmen werden.

Die Cybersicherheits-Strategie von Unternehmen muss auch eine schnelle Information der Behörden und Benutzer im Falle eines Cyberangriffs vorsehen, der die Sicherheit und Vertraulichkeit von Daten gefährden könnte. So sieht die DSGVO vor, dass jedes Datenleck innerhalb von 72 Stunden der Aufsichtsbehörde gemeldet werden muss.

2.4 Algorithmen und künstliche Intelligenz

Die künstliche Intelligenz (KI) vereint eine Reihe von Theorien und Techniken für die Entwicklung komplexer Computerprogramme, die bestimmte Merkmale der menschlichen Intelligenz wie logisches Denken, Lernen, natürliche Sprache, Bewegung usw. simulieren können. Die künstliche Intelligenz basiert heute hauptsächlich auf den sehr weit fortgeschrittenen Technologien des maschinellen Lernens. Sie zielen darauf ab, Computern die Fähigkeit zu geben, aus Daten zu «lernen», also ihre Leistung beim Lösen von Aufgaben zu verbessern, ohne explizit für jede einzelne Aufgabe programmiert zu werden. Die Methode, die heute die wichtigsten Ergebnisse erzeugt, ist das «deep learning». Dieses vertiefte oder mehrschichtige Lernen ist eine Methode des maschinellen Lernens mittels einer Klasse von Algorithmen, die mehrere verborgene Schichten künstlicher neuronaler Netze nutzen, welche fähig sind, immer abstraktere Charakteristiken der ihnen präsentierten Daten zu extrahieren, analysieren und klassifizieren.

Die künstliche Intelligenz kann in den Bereichen Gesundheit, Produktivität und Umwelt einen hohen Mehrwert bieten. In der Medizin hat man sich beispielsweise in der Radiologie als hochtechnologischer Sparte schon früh mit «intelligenter» Technik beschäftigt. So ermöglicht sie seit mehr als zehn Jahren, mit Hilfe eines Computeralgorithmus Tumore in der Lunge zu entdecken.[4]

Der rasante Fortschritt dieser Technologien in den letzten Jahren wurde durch die explosionsartige Zunahme der Rechenleistung der Computer und der Datenmengen ermöglicht, die zur Speisung der Algorithmen zur Verfügung stehen.

Dank diesen simultanen Entwicklungen sind Maschinen auf manchen Gebieten, beispielsweise im Go-Brettspiel, dem Menschen überlegen. Wichtiger als die Leistung des Computers ist jedoch die Tatsache, dass das auf einem künstlichen neuronalen Netz basierende Programm lernte, selbständig zu spielen, was bezeichnend für die künstliche Intelligenz ist. Diese entwickelt sich auf der Basis ihrer Programmierung autonom weiter, was es ihrem Entwickler verunmöglicht, ihren Entscheidungsprozess zu erklären. Das kann dazu führen, dass die künstliche Intelligenz selbstständig Entscheidungen trifft, die ihrer Programmierung oder dem allgemeinen Interesse zuwiderlaufen.

Die möglichen Auswirkungen der Algorithmen auf unser tägliches Leben (autonome Fahrzeuge, Gesichtserkennung, Sprachassistenten usw.) sind Auslöser für eine wichtige Debatte über die Verantwortung und die Ethik im Zusammenhang mit diesen Maschinen.

Bis heute gibt es keine Vorschrift, die das Funktionieren der künstlichen Intelligenz regelt und verhindert, dass diese Programme, die autonom und unabhängig vom Menschen geworden sind, gegen ethische Regeln verstossen. Allerdings werden allmählich ethische Erwartungen in Bezug auf die künstliche Intelligenz formuliert. Diese stützen sich auf 4 Prinzipien (Transparenz, Unparteilichkeit, Verantwortung und positive Auswirkung).

[4] https://medicalforum.ch/article/doi/fms.2019.08035

A. Transparenz

Die Erwartungen der Gesellschaft an die Transparenz von Systemen mit künstlicher Intelligenz sind hoch. Von den Unternehmen wird nun erwartet, dass sie transparent informieren, welche Programme sie wo und wie einsetzen. Dies kann in zahlreichen Bereichen der Fall sein: Personalwesen, Kundendienst, medizinische Diagnose, Kredit- oder Versicherungszusagen oder die Auswahl der Anbieter von Dienstleistungen. Der Einsatz solcher Technologien sollte transparent sein. Insbesondere sollte man erfahren können, wie und warum ein System eine Entscheidung getroffen hat oder sich so verhält (erklärbare künstliche Intelligenz).

B. Gleichbehandlung / Unparteilichkeit

Die Funktionsweise von Systemen der künstlichen Intelligenz ist oft undurchsichtig, insbesondere im Bereich des «deep learning». Entscheidungen oder Empfehlungen, die mit Hilfe von Programmen der künstlichen Intelligenz getroffen werden, können mit moralischen und ethischen Dilemmas kollidieren. Die Nachvollziehbarkeit des Entscheidungsprozesses ist wesentlich, um sicherzustellen, dass die Entscheidungen der künstlichen Intelligenz frei von ethnischen, geschlechtsspezifischen oder anderen Vorurteilen sind («unvoreingenommene KI»). Diese Neutralität muss die Basis für die Gestaltung von Programmen sein, die zu autonomen Entscheidungsmechanismen führen können. Das hängt nicht nur vom Code des Algorithmus ab, sondern vor allem von den Daten, die in die Algorithmen eingespeist werden. Es liegt daher in der Verantwortung der Unternehmen, sicherzustellen, dass die Ergebnisse oder Vorhersagen der künstlichen Intelligenz nicht verzerrt sind, insbesondere weil die Quelldaten qualitativ ungenügend oder zu wenig repräsentativ sind. Kann diese Neutralität nicht gewährleistet werden, sollte eine solche Software gar nicht in Betrieb genommen werden können.

C. Verantwortung

Die Unparteilichkeit der künstlichen Intelligenz ist von zentraler Bedeutung, löst aber nicht unbedingt alle moralischen Dilemmas, mit denen die künstliche Intelligenz konfrontiert werden könnte. Deshalb muss menschliches Eingreifen jederzeit möglich bleiben. Bei Problemen muss auch die Frage der Verantwortlichkeit geklärt werden. Liegt diese beim Verkäufer, dem Eigentümer, dem Entwickler des Algorithmus oder geht sie direkt auf das System über?

Für die aktuellen ethischen Grundsätze rund um die künstlichen Intelligenz ist es eine unabdingbare Voraussetzung, dass ihre Entwicklung verantwortungsbewusst, sicher und nutzbringend erfolgt, dass die Maschinen den Status von Werkzeugen behalten und dass natürliche oder juristische Personen jederzeit die Kontrolle und Verantwortung für sie behalten.

D. Positive Auswirkung

Die künstliche Intelligenz kann bei der Lösung gewisser aktueller Herausforderungen wie Klimawandel, Verlust der biologischen Vielfalt, Gesundheit oder Ungleichheiten eine zentrale Rolle spielen. Sie sollte vor allem mit dem Ziel entwickelt werden, dass sie Umwelt und Gesellschaft positiv beeinflusst.

2.5 Sensible Produkte und Dienstleistungen

Die rasante Entwicklung der neuen Technologien ermöglicht Aktivitäten, die Ethos als unvereinbar mit ihrer Charta und den Grundlagen der nachhaltigen Entwicklung erachtet. Dies betrifft insbesondere Überwachungsaktivitäten, welche die Gesichtserkennung nutzen, die Meinungsfreiheit einschränken, auf die Entwicklung oder den Einsatz autonomer Waffen, die Verbreitung sensibler oder verbotener Inhalte, ja sogar auf Aktivitäten abzielen, die das Verhalten auf versteckte Weise zu beeinflussen suchen.

A. Überwachung

Die neuen Analyse- und Bearbeitungstechnologien für Bilder können dazu beitragen, die Verbreitung gewalttätiger oder sensibler Inhalte im Internet zu verhindern und Angriffe im öffentlichen Raum zu entdecken. Diese Systeme können jedoch auch für die Überwachung der Bürger eingesetzt werden und so bei der Nutzung durch autoritäre Regime die Meinungsfreiheit und die Menschenrechte beeinträchtigen. Unternehmen müssen deshalb überwachen, wie ihre Technologien und Dienstleistungen von den Kunden genutzt werden. Sie sollten akzeptable Grenzen festlegen, um sicherzustellen, dass die Menschenrechte weder direkt noch indirekt beeinträchtigt werden.

B. Autonome Waffen

Die künstliche Intelligenz ermöglicht die Entwicklung neuer Arten von autonomen Waffen, die Ziele ohne menschliches Eingreifen auswählen und bekämpfen. Es steht viel auf dem Spiel: autonome Waffen wurden auch schon als die dritte Revolution der Kriegsführung beschrieben, nach Schiesspulver und Atomwaffen.

Im Gegensatz zu Atomwaffen sind für autonome Waffen keine teuren oder schwer zu beschaffenden Rohstoffe erforderlich, so dass sie schnell den Weg auf den Schwarzmarkt finden und so etwa von Terroristen, Diktatoren, die eine bessere Kontrolle über ihre Bevölkerung anstreben, sowie Kriegsherren beschafft werden könnten, die ethnische Säuberungen durchführen wollen. Da autonome Waffen keine Gefühle kennen, eignen sie sich ideal für Verbrechen wie Mord, Destabilisierung von Nationen, Unterwerfung von Bevölkerungen und Genozid[5].

Die Unternehmen müssen sicherstellen, dass ihre Produkte, Technologien und ihr geistiges Eigentum weder direkt noch indirekt auf spezifische Weise zur Entwicklung autonomer Rüstungsgüter beitragen.

2.6 Soziale Auswirkungen

Die technologischen Entwicklungen haben jetzt und in Zukunft einen grossen Einfluss auf die Arbeitsplätze und Sozialwerke. Mit der weiteren Entwicklung von Systemen mit künstlicher Intelligenz werden neue Geschäftsmodelle entstehen und Arbeitsplätze oder Aufgabentypen verschwinden oder sich tiefgreifend verändern. Die Nutzniesser dieser digitalen Revolution könnten Unternehmen und Aktionäre sein, die von einer erhöhten Produktivität profitieren werden. Die Gewinne für die Aktionäre könnten jedoch kurzfristig sein, wenn die Transformation nicht verantwortungsvoll vollzogen wird. Insbesondere das schweizerische Vorsorgesystem könnte darunter leiden, wenn die Zahl der Erwerbstätigen drastisch sinkt oder wenn die Entwicklung der Dienstleistungswirtschaft *(«gig economy»)* die Angestellten zu selbstständigen Unternehmern macht («Uberisierung»).

Um eine gerechte Transformation zu gewährleisten, ist es unerlässlich, eine Unternehmenspolitik einzuführen, welche die Verantwortung der Unternehmen für Arbeitsplatzverluste und -verlagerungen garantiert und wahrnimmt, zum Beispiel durch Umschulungsprogramme, Weiterbildung und Möglichkeiten des Arbeitsplatzwechsels. In dieser Hinsicht ermöglicht ein Technologie-Monitoring, technische Entwicklungen und die entsprechenden Qualifikationsanforderungen zu antizipieren. Auf diese Weise könnte eine verantwortungsvolle Umstellung bei den Kompetenzen der Mitarbeiter gewährleistet sein werden.

Zusammen mit der generellen Umstellung auf eine digitale Wirtschaft werden die Systeme für künstliche Intelligenz erfordern, dass die Angestellten auf allen Ebenen und in allen Berufen Zugang zu sozialer Sicherheit und lebenslanger Weiterbildung haben, um beschäftigungsfähig zu bleiben. Es liegt in der Verantwortung von Staaten und Unternehmen, Lösungen zu finden, die sicherstellen, dass alle Erwerbstätigen in allen Arbeitsformen das Recht und den Zugang zu beidem haben.

In einer Welt, in der die Präkarisierung und Individualisierung der Arbeit zunimmt, müssen zudem alle Beschäftigten unabhängig von ihrer Tätigkeit gleiche und solide soziale und grundlegende Rechte haben. Bei allen Systemen für künstliche Intelligenz sind Kontroll- und Ausgleichsmöglichkeiten vorzusehen, damit sichergestellt ist, dass ihr Einsatz und ihre zunehmende Verbreitung den Regelungen des Arbeitsrechts genügen, wie sie in den Menschenrechtsbestimmungen, den Übereinkommen der Internationalen Arbeitsorganisation (IAO) und den Gesamtarbeitsverträgen definiert sind.

2.7 Umweltauswirkungen

Die gegenwärtige digitale Revolution bringt auch wichtige ökologische Herausforderungen mit sich, dies zu einer Zeit, in der unsere Gesellschaft ihre Treibhausgasemissionen drastisch reduzieren muss, um die globale Erwärmung zu begrenzen. Die digitale Revolution hat jedoch ein

[5] https://futureoflife.org/open-letter-autonomous-weapons/

exponentielles Wachstum des CO_2-Fussabdrucks und eine starke Zunahme der Umweltauswirkungen zur Folge.

Gemäss einer Studie von GreenIT.fr[6] bestand die digitale Welt im Jahr 2019 aus 34 Milliarden Geräten (Smartphones, TV- und Computerbildschirme sowie vernetzte Objekte, usw.). Berücksichtigt man den gesamten Lebenszyklus der Informatikausrüstung, ist der Beitrag ihres digitalen Fussabdrucks zu jenem der Menschheit insgesamt keineswegs vernachlässigbar. Laut GreenIT.fr haben diese 34 Milliarden IT-Ausrüstungen, die verschiedenen Netzwerke (11 Milliarden DSL/Glasfaser-Boxen, 10 Millionen 2G- bis 5G-Relaisantennen und rund 200 Millionen weitere aktive WAN-Netzwerkausrüstungen) sowie die mehreren tausend Rechenzentren (mit mehr als 67 Millionen gehosteten Servern) im Jahr 2019 wie folgt zum ökologischen Fussabdruck der Menschheit beigetragen:

- 4,2% des Primärenergieverbrauchs (6800 TWh),
- 3,8% der Treibhausgasemissionen (1400 Millionen Tonnen THG).

Die Coronavirus-Krise, die dazu führte, dass mehr als 3 Milliarden Menschen zu Hause bleiben und IT-Dienstleistungen in Anspruch nehmen, hat diesen Trend mit einer noch rasanteren Zunahme der Datenströme weiter verstärkt.

Angesichts der ungebremsten Zunahme der Nutzung von vernetzten Objekten, Computernetzwerken und einer datenzentrierten Wirtschaft wird der digitale Fussabdruck in den kommenden Jahren weiterhin exponentiell wachsen. Es besteht Handlungsbedarf für Unternehmen, Verbraucher und Regierungen.

[6] https://www.greenit.fr/wp-content/uploads/2019/10/2019-10-GREENIT-etude_EENM-rapport-accessible.VF_.pdf

3 Erwartungen von Ethos

Ethos erwartet von den Unternehmen, an denen sie als Aktionärin beteiligt ist oder gegenüber denen sie als Vertreterin anderer institutioneller Anleger auftritt, dass sie die Anwendung der folgenden Grundsätze gewährleisten.

Die Grundsätze von Ethos für die digitale Verantwortung

1. Implementierung eines Kodex für digitale Verantwortung
2. Sicherstellung der Transparenz gegenüber den Anspruchsgruppen bezüglich der digitalen Praktiken und des digitalen Fussabdrucks
3. Einhaltung der höchsten Standards der Datenverarbeitung und des Datenschutzes
4. Implementierung ethischer Grundsätze bei der Nutzung der künstlichen Intelligenz (KI)
5. Ausschluss sensibler Aktivitäten im Zusammenhang mit der Digitalisierung
6. Gewährleistung einer gerechten und verantwortungsvollen sozialen Transformation
7. Beitrag zur Reduzierung des ökologischen Fussabdrucks der digitalen Technologien

Grundsatz 1: Implementierung eines Kodex für digitale Verantwortung

Der Verwaltungsrat muss sicherstellen, dass das Unternehmen über einen Kodex für digitale Verantwortung verfügt, welcher die wichtigsten Fragen, mit denen das Unternehmen konfrontiert ist, abdeckt. Dabei muss er auch die Wesentlichkeit dieser Fragen in Bezug auf den Tätigkeitsbereich und die spezifischen Merkmale des Unternehmens gewichten. Der Verwaltungsrat ist dafür verantwortlich, dass alle digitalen Themen abgedeckt sind und jährlich überprüft wird, ob diese immer noch relevant sind. Der Kodex sollte mindestens die folgenden Punkte abdecken:

- **Governance:** Die Art und Weise, wie die digitalen Herausforderungen des Unternehmens behandelt werden, sollte im Kodex festgelegt werden. Der Verwaltungsrat muss sich regelmässig mit dem Thema befassen und sicherstellen, dass seine Mitglieder die Chancen, Risiken und Herausforderungen der Digitalisierung verstehen. Die Geschäftsleitung sollte einen für den Bereich Digitalisierung zuständigen «Chief Digital Officer» ernennen und für die Umsetzung des Kodex und seine Einhaltung verantwortlich sein.
- **Technologie-Monitoring:** Im Kodex sollte erwähnt sein, wie der Verwaltungsrat und die Geschäftsleitung des Unternehmens die für seine Aktivitäten relevanten technologischen Entwicklungen beobachten. Dies setzt eine ständige Überwachung und eine Berücksichtigung der Entwicklungen bei der Definition der Strategie und der Risiken des Unternehmens voraus.
- **Cybersicherheit:** Der Kodex sollte einen Abschnitt darüber enthalten, wie das Unternehmen mit diesem Risiko umgeht. Die Cybersicherheitsstrategie sollte vom Prüfungsausschuss überprüft werden, und die Geschäftsleitung sollte einen «Chief Security Officer» ernennen. Angesichts der Sensibilität des Themas liegt es auf der Hand, dass die Einzelheiten der Sicherheitspolitik vertraulich bleiben müssen. Wichtig ist jedoch die Bestätigung des Unternehmens, dass regelmässige Sicherheitsaudits durchgeführt werden und dass das Bewusstsein bei allen Systembenutzern geschärft wird.
- **Privatsphäre und Datenschutz:** Unternehmen sollten in ihrem Kodex bestätigen, dass sie sich verpflichten, den Datenschutz und die Privatsphäre ihrer Anspruchsgruppen zu respektieren (siehe Grundsatz 3 unten).
- **Ethische Regeln für den Einsatz künstlicher Intelligenz (KI):** Der Kodex sollte einen detaillierten Abschnitt oder Verweis auf spezifischere Grundsätze zu den Regeln für den Einsatz von KI enthalten (siehe Grundsatz 4 unten).
- **Soziale Verantwortung für den digitalen Wandel:** Die Auswirkungen des digitalen Wandels auf die Mitarbeiter des Unternehmens sollten ebenfalls Teil des Kodex sein (siehe Grundsatz 6 unten).

- **Prinzip der Reduzierung des digitalen ökologischen Fussabdrucks:** Unternehmen sollten in ihrem Kodex für digitale Verantwortung festlegen, wie die Umweltauswirkungen von digitalen Produkten und Dienstleistungen sowie von Daten und Netzwerken des Unternehmens minimiert werden (siehe Grundsatz 7 unten).

Grundsatz 2: Sicherstellung der Transparenz gegenüber den Anspruchsgruppen

Die Umsetzung des Kodex für digitale Verantwortung sollte von den Anspruchsgruppen des Unternehmens (Kunden, Lieferanten, Aktionäre, Gesellschaft usw.) überprüfbar sein. Dies erfordert eine vollständige Transparenz, die auf der Website und im Jahresbericht leicht zugänglich und verständlich ist, insbesondere bei den folgenden Punkten:

– Der Kodex für digitale Verantwortung sollte im Internet, in den Sprachen der Länder, in denen das Unternehmen tätig ist, **verfügbar sein**.

– Die Benutzer **sollten wissen, welche Daten gesammelt werden**, und sie sollten darauf zugreifen können. Auch die Speicherorte der Daten sollten mitgeteilt werden, ebenso wie die Art und Weise, in der private Daten verschlüsselt werden.

– Die Vertraulichkeitsregeln bezüglich Daten sollten für die **Benutzer verständlich und leicht** zugänglich sein.

– **Der Einsatz von künstlicher Intelligenz** in den Entscheidungsprozessen sollte klar kommuniziert werden.

– Ein die Datensicherheit gefährdender Angriff sollte **unverzüglich gemeldet werden**. Benutzer, deren Daten kompromittiert wurden, sind ebenfalls zu informieren.

Grundsatz 3: Einhaltung der höchsten Standards der Datenverarbeitung und des Datenschutzes

Unternehmen sollten in diesem Bereich die höchsten Standards anwenden, um rechtliche und finanzielle Risiken zu minimieren. Dabei sollten sie vor allem die folgenden Punkte beachten:

– Die Produkte und Dienstleistungen von Unternehmen sollten so konzipiert sein, dass sie die Privatsphäre der Benutzer jederzeit respektieren («**privacy by design**») und stets einen Standardmodus anbieten können, der diese Privatsphäre achtet («**privacy by default**»).

– Personen, deren Daten gesammelt werden, sollten vor jeder Verwendung ihrer Daten ausdrücklich ihre freie und informierte Zustimmung geben («**opt in**»).

– Unternehmen dürfen die privaten Daten nicht zur Überwachung des Verhaltens verwenden.

– Ohne einen bestimmten Grund (Zweck) dürfen keine Daten gesammelt und gespeichert werden.

– Unternehmen sollten den Grundsatz der strikt minimalen Datenerhebung und des minimalen Datenbesitzes (Verhältnismässigkeit) einhalten. Sie sollten Technologien einführen, die es ihnen ermöglichen, die Einhaltung dieses Grundsatzes (Privacy Enhancing Technologies oder PETs) bei ihren Online-Diensten und Websites zu gewährleisten.

Grundsatz 4: Implementierung ethischer Grundsätze bei der Nutzung der künstlichen Intelligenz (KI)

Voraussetzung für die Nutzung künstlicher Intelligenz ist das Erstellen eines Ethik-Kodex, der sich mit den folgenden Grundsätzen befassen sollte:

– Unternehmen, die Systeme der künstlichen Intelligenz entwickeln, sollten sicherstellen, dass man diese mit dem Ziel entwickelt, die Gesellschaft und die Umwelt positiv zu beeinflussen.

– Autonom arbeitende Technologien können je nach Qualität der Programmierung und der Daten, welche die Algorithmen speisen, bestimmte Vorurteile widerspiegeln und verstärken. **Unternehmen müssen die Gleichbehandlung und Nichtdiskriminierung** durch die von ihnen entwickelte und genutzte künstliche Intelligenz sicherstellen. Letztere sollte sich nicht ungerecht auswirken, insbesondere nicht in Bezug auf sensible Merkmale wie ethnische Zugehörigkeit, Geschlecht, Nationalität, Einkommen, sexuelle Orientierung, Fähigkeiten und die politische oder religiöse Orientierung («unvoreingenommene KI»).

– Unternehmen müssen jederzeit **erklären können, wie ihre Systeme der künstlichen Intelligenz funktionieren**, und den Entscheidungsprozess nachvollziehen können (erklärbare KI).

– Die Verwendung einer Entscheidung der künstlichen Intelligenz durch das Unternehmen sollte **der Zustimmung durch einen Mensche**n und einem Einspruchsrecht unterstellt sein («human in the loop»).

– Unternehmen sollten sicherstellen, dass es jederzeit möglich ist, in den Programmen einen **manuellen Modus** zu wählen, und dass dieser Modus gegenüber dem autonomen Modus Vorrang hat.

– Sie sollten die Leistung und Qualität ihrer Systeme für künstliche Intelligenz **regelmässig überprüfen**.

– Ausserdem sollten sie sicherstellen, dass die Entwicklung der künstlichen Intelligenz verantwortungsvoll, sicher und nützlich ist, dass die **Maschinen nur den Status von Werkzeugen** haben und der Mensch die Kontrolle und Verantwortung behält.

Grundsatz 5: Ausschluss sensibler Aktivitäten im Zusammenhang mit der Digitalisierung

Die Unternehmen müssen definieren, welche Aktivitäten im Zusammenhang mit der künstlichen Intelligenz verboten werden sollen. Ethos ist der Ansicht, dass die Risikomanagementsysteme der Unternehmen berücksichtigen müssen, dass solche Güter, Dienstleistungen oder Programme insbesondere nicht zur Entwicklung oder zur Nutzung der folgenden Aktivitäten beitragen dürfen:

– Personen-Überwachungssysteme, die Grundrechte verletzen,

– Systeme zur Begrenzung oder Verringerung der Meinungsfreiheit,

– Systeme, die konzipiert wurden, um Abhängigkeiten zu erzeugen,

– autonome Waffen,

– Systeme, die dazu beitragen, einen Markt zu manipulieren oder das Verhalten eines Marktes oder einer Bevölkerung auf versteckte Weise zu beeinflussen,

– Systeme, die sensible, rassistische, sexistische oder illegale Inhalte verbreiten oder die den Zugang zu Inhalten und Aktivitäten ermöglichen, die für Minderjährige ungeeignet sind.

Grundsatz 6: Gewährleistung einer gerechten und verantwortungsvollen sozialen Transformation

Um eine gerechte Transformation zu gewährleisten, ist es unerlässlich, eine Personalpolitik einzuführen, welche die Verantwortung der Unternehmen für Verlagerungen oder den Abbau von Arbeitsplätzen sicherstellt.

– Die Unternehmen sollten Programme für die persönliche Förderung und Umschulung vorsehen, indem sie Weiterbildungen sowie Möglichkeiten für den Stellenwechsel anbieten.

– Sie sollten Systeme für künstliche Intelligenz bereitstellen, die den Menschen dienen und den Arbeitsplatzabbau durch eine gerechte Verteilung der Produktivitätsgewinne begrenzen.

– Werden in der Personalverwaltung Mitarbeiterdaten oder Systeme für künstliche Intelligenz verwendet, sollten die Mitarbeitenden informiert werden und das Recht haben, Transparenz über die Entscheidungen und Ergebnisse von solchen Systemen und die ihnen zugrundeliegenden Algorithmen zu verlangen. 7

– Ungeachtet der Entwicklung neuer Geschäftsmodelle durch die digitale Transformation und künstliche Intelligenz sollte es Unternehmen nicht gestattet sein, sich ihren Verpflichtungen gegenüber den Mitarbeitenden zu entziehen sowie Gesamtarbeitsverträge oder Sozialversicherungssysteme zu umgehen.

– Unternehmen sollten die Entwicklung der Technologien beobachten, um ihren Bedarf

[7] Top 10 principles for Ethical artificial intelligence, UNI Global Union, Prinzip 1

an Kompetenzen zu planen und Umschulungen sowie der Weitergabe interner Expertise den Vorrang einzuräumen.

– Die Unternehmen sollten einen Teil ihres Nachhaltigkeitsberichts der Erläuterung ihrer Bemühungen für den Erhalt der Arbeitsplätze Beschäftigung widmen (Anzahl der Umschulungen, Anzahl der Weiterbildungsstunden, Anzahl der durch Systeme abgebauten oder ersetzten Arbeitsplätze, Massnahmen zur Umverteilung der Produktivitätsgewinne).

Grundsatz 7: Beitrag zur Reduzierung des ökologischen Fussabdrucks der digitalen Technologien

Die digitale Revolution hat erhebliche Auswirkungen auf die Umwelt, vor allem wenn man den Fussabdruck der vernetzten Produkte über ihren gesamten Lebenszyklus und die explosionsartige Zunahme der gespeicherten und konsumierten Datenmengen betrachtet. Der grossangelegte Einsatz komplexer Algorithmen impliziert auch eine ständig steigende Rechenleistung und damit einen exponentiellen Energieverbrauch. Alle Unternehmen können Massnahmen ergreifen, um den ökologischen Fussabdruck ihrer digitalen Lösungen zu verringern. Insbesondere können sie:

– die Lebensdauer der Geräte verlängern und die gesetzliche Gewährleistungsfrist erhöhen,

– den Bedarf an digitalen Dienstleistungen durch ihr Öko-Design reduzieren,

– die Wiederverwendung und das Recycling von digitalen Produkten fördern,

– Kunden darüber aufklären, wie sie den ökologischen Fussabdruck vernetzter Produkte minimieren können.

– im Nachhaltigkeitsbericht relevante Daten veröffentlichen, etwa über das Recycling, die durchschnittliche Lebensdauer der vernetzten Produkte, den Energieverbrauch von IT-Systemen, die gespeicherten Datenmengen oder andere relevante Umweltindikatoren, um Vergleiche und Entwicklungen auf Dauer zu ermöglichen.

– die Umweltauswirkungen bei der Entscheidung, ob IT-Dienstleistungen internalisiert oder ausgelagert werden sollen, regelmässig beurteilen und berücksichtigen.

Ethos
Place de Pont-Rouge 1
Postfach 1051
1211 Genf 26
Schweiz

T + 41 (0)22 716 15 55
F + 41 (0)22 716 15 56

Büro Zürich
Bellerivestrasse 3
8008 Zürich
Schweiz

T + 41 (0)44 421 41 11
F + 41 (0)44 421 41 12

info@ethosfund.ch
www.ethosfund.ch