Algorithmische Systeme bergen neue Korruptionsgefahren

Positionspapier von Transparency Deutschland

Juni 2020

Die zivilisatorischen und kulturellen Veränderungen, angetrieben durch die Entwicklung der datengeprägten Informationstechnologie nach der Jahrtausendwende, haben zu neuen Formen des Machtmissbrauchs geführt. Digitalisierung hat neue Möglichkeiten geschaffen, das Verhalten von Personen besser als je zuvor zum eigenen Vorteil zu erforschen und wirtschaftlich zu nutzen. Global operierende Digitalkonzerne haben sich unter der Philosophie des Radikallibertarismus mit den Stichworten absolute Freiheit, Abwesenheit staatlicher Regulierung und Marktradikalismus entwickelt. Mit immer neuen Geschäftsmodellen und Anwendungsbereichen, besonders durch die Nutzung von Netzwerkeffekten und Skalierungserträgen, wird versucht, Marktmacht auszudehnen. Die Globalisierung ermöglicht es, Staaten gegeneinander auszuspielen. Gesetzeslücken werden rigoros zum eigenen Vorteil genutzt.

In einer Art Wettlauf mit Konzernen und Start-ups und deren Innovationen versuchen Staaten die Grundrechte ihrer Bürgerinnen und Bürger, Kernelemente der staatlichen Verfasstheit sowie Aspekte des Gemeinwohls durchzusetzen.

Ins Auge zu nehmen sind zuerst die Daten selbst und wie sie erhoben werden. Daten, definiert als Informationen über Sachverhalte und Vorgänge, werden häufig ohne Wissen oder aktives Zutun der Betroffenen selbst generiert oder von Sensoren erfasst und in Form von Zeichen und Symbolen gespeichert. Algorithmen mit ihren programmierten Verarbeitungsvorschriften für Daten liefern schließlich Ergebnisse. So erfassen Computer unter anderem die Art, wie wir Informationen gewinnen und weitergeben, welche Nachrichten wir lesen oder hören, welche Videos wir sehen, mit wem wir wie lange Kontakt haben, was wir online kaufen, von wem wir uns beraten lassen und vieles mehr. Smartphones übermitteln Daten darüber, wie und wo wir uns bewegen, wo wir uns wie lange aufhalten, wer unsere Freunde und Freundinnen sind. Smarte Geräte wie Autos liefern Daten über unser Verhalten im Verkehr, smarte Uhren geben Auskunft über unsere Gesundheit, smarte Haushaltsgeräte liefern Daten über unsere Wohnung, in welcher Umgebung wir leben, wie wohlhabend wir sind.

All diese Einzeldaten werden oder können dazu genutzt werden, über Algorithmen unser Verhalten zu analysieren, Persönlichkeitsprofile zu erstellen, die dann für personalisierte Werbung, aber auch für personalisierte Preise oder für die Einschätzung unserer Kaufkraft genutzt werden können. Diese Analysen eignen sich unter anderem für Risikoabschätzungen durch Versicherungen und Finanzdienstleister, sie geben Auskunft über den jeweiligen Lebensstil und werden letztlich dazu verwendet aus den Verbraucherinnen und Verbrauchern, Nutzerinnen und Nutzern, maximalen Profit für das jeweilige Unternehmen zu erzielen. Maßgebliche Indikatoren von Marktmacht sind nicht mehr nur Größen wie Gewinn oder Kundenstamm, sondern insbesondere auch der Umfang des kontrollierten Datenpools.

Digitale Plattformen sind entstanden, die Angebot und Nachfrage in den verschiedenen Sektoren der Wirtschaft moderieren. Soziale Netzwerke bieten kostenlose Dienstleistungen gegen persönliche Daten, um diese dann an Unternehmen für Werbezwecke weiterzuverkaufen.

Je mehr Daten über Plattformen oder im Bereich „Internet der Dinge“ über Personen auf dem Wege des Trackings gesammelt werden können, desto genauer und zuverlässiger sind die Prog-

Transparency International Deutschland e.V.
Tel. +49 30 549898-0 | Fax +49 30 549898-22
E-Mail: office@transparency.de
Webseite: www.transparency.de

Vorsitzender: Hartmut Bäumer
Stellvertretend: Carel Carlowitz Mohn,
Helena Peltonen-Gassmann
Geschäftsführerin: Dr. Anna-Maija Mertens

Jetzt spenden!
IBAN: DE07 4306 0967 1146 0037 00
BIC: GENODEM1GLS
Vereinsregister Berlin: 16181

nosen über zukünftiges Verhalten. Mit den Erkenntnissen, die aus dem Profiling gewonnen werden, wächst die Gefahr des Manipuliertwerdens und der Fremdbestimmung. Digitalisierung ermöglicht durch die intransparente und schwer kontrollierbare Sammlung und Nutzung personenbezogener Daten systemische Korruption.

Um sie abzuwehren sind gesetzliche Regelungen und staatliche Kontrollen erforderlich. Für diese gilt die durch das Grundgesetz festgelegte Werteordnung. Ferner muss es öffentliche Institutionen geben, welche die gesetzliche Umsetzung begleiten, lenken und kontrollieren. Und es muss vor allem Transparenz geben, durch welche die Einsicht in die verschiedenen Formen der Digitalisierung sichergestellt wird. Diese Einsicht ist eine Voraussetzung für Kontrolle und die Abwehr von Machtmissbrauch.

Bei der Anwendung von künstlicher Intelligenz, wie sie in der Praxis als „Machine Learning“ zum Einsatz kommt, ergeben sich für die Anforderungen an Transparenz besondere Schwierigkeiten. Die algorithmischen Systeme des Machine Learning arbeiten mit einer Blackbox. Dabei wird das Ziel von Menschen vorgegeben, das System lernt durch die eingefütterten Daten aus der Vergangenheit. Es erkennt so Muster und errechnet daraus neue Erkenntnisse oder Wahrscheinlichkeiten für die Zukunft, die sein Eigentümer interpretiert. Die Auswahl der Trainingsdaten hat dabei erheblichen Einfluss auf die Ergebnisse künftiger Berechnungen und bietet großen Spielraum für beabsichtigte oder unbeabsichtigte Manipulation des eigentlich angestrebten Ziels. Der Zusammenhang zwischen Zielsetzung, Trainingsdaten, Schlussfolgerungen und daraus abgeleiteten Maßnahmen bleibt dabei undurchsichtig. Nur durch die gezielt veränderte Eingabe von Datensätzen lässt sich in Analogie die Entscheidungsfindung sichtbar und nachvollziehbar machen.

Mit diesem Positionspapier will Transparency Deutschland das Handlungsspektrum für seine Begleitung des Prozesses der notwendigen Regulierung abstecken. Im Lichte neuer Erkenntnisse über Chancen und Gefahren soll das Positionspapier aktualisiert und fortgeschrieben werden. Die spezifischen Erfordernisse in einzelnen Sektoren wie dem Medienbereich, dem Gesundheits-, Energie-, Verkehrsbereich, der öffentlichen Verwaltung und der demokratischen Willensbildung, werden in eigenen Positionspapieren behandelt.

1. Grundsätze für die Sammlung von personenbezogenen Daten

1.1 Freiwillige Einwilligung in die Nutzung personenbezogener Daten

Die Einwilligung in die Nutzung personenbezogener Daten ist nur wirksam, wenn sie freiwillig erfolgt. Freiwillig kann diese Einwilligung aber nur sein, wenn sie ohne Zwang abgegeben wird. Begünstigt wird dies, wenn es Alternativen zur Auswahl gibt. Die Einwilligung muss widerrufen werden können und muss zu einer vollständigen Löschung der betreffenden Daten beim Dienstleister führen.

1.2. Datensparsamkeit

Das Bestreben möglichst viele Daten zu sammeln, zu verarbeiten und zu speichern, ist der Digitalisierung immanent. Je mehr Daten verarbeitet werden, umso größer ist die Genauigkeit der Aussagen und damit auch der wirtschaftliche Wert. Das Prinzip der Datensparsamkeit, das im Datenschutzrecht fest verankert ist, verhilft dem Grundrecht auf informationelle Selbstbestimmung zur Durchsetzung. Es schafft ein Gegengewicht zum angestrebten geschäftlichen Nutzen, der mit der Masse der Daten zunimmt.

1.3. Zweck der Datenerhebung

Das Ziel der Datensparsamkeit wird gestützt durch den Grundsatz, dass eine Datenverarbeitung nur zu einem besonderen Zweck erfolgen darf. Die Art des Zwecks ist anzugeben, z.B. Verarbeiten der Daten mit welchem Ziel, oder das Handeln mit Daten. Die differenzierte Einwilligung zur Datenverarbeitung im Hinblick auf einzelne Zwecke ist erforderlich. Eine Weiterverwendung zu anderen Zwecken bedarf einer erneuten Einwilligung.

1.4. Datenschutz als Grundeinstellung („Privacy-by-Default“, Art. 25 DSGVO)

Zur Beachtung der Vorgaben der Datenschutzgrundverordnung muss die Grundeinstellung bei der Nutzung von Plattformen oder technischen Geräten stets die datenschutzfreundlichste Einstellung sein. Die Konsequenz der Wahl anderer Einstellungen muss verständlich dargelegt werden.

1.5. Tracking

Tracking findet in den verschiedensten Formen statt. Die Aktionen der Nutzerinnen und Nutzer im Internet werden festgehalten. Es wird aufgezeichnet von welchen Endgeräten (Computer und Smartphones) welche Webseiten aufgerufen werden, wie die Bewegungen auf den Seiten sind, zu welchen Zeiten und mit welcher Verweildauer, in welcher Reihenfolge etc. Geodaten werden mit GPS oder Galileo ermittelt. Einwahlorte (WLAN) werden erfasst, auch ohne das Wissen von Handynutzerinnen und -nutzern. Daten, erzeugt durch unser Verhalten in Kombination mit Geräten, werden verarbeitet und gespeichert.

- Tracking erfordert eine voraussetzungslose Einwilligung.
- Widerspruch zur Einwilligung muss möglich sein.
- Verbot von Tracking-Walls (take it or leave it).
- Abgestufte Zustimmung muss möglich sein. Zum Beispiel:
    - Technisch erforderliche Cookies erlauben
    - Tracking nur bei Nutzung der App
    - Analyse des Verhaltens auf der Website erlauben
    - Verarbeitung der Daten zu Werbezwecken erlauben
    - Verkaufen und Handeln erlauben.
- Offline Tracking nur mit ausdrücklicher Einwilligung

1.6. Personenbezogene Daten aus dem Internet der Dinge

Verhaltensgenerierte Daten mit Personenbezug dürfen nur, wenn sie für den Zweck der Nutzung des Gerätes erforderlich sind, erfasst, verarbeitet und gespeichert werden. Dazu bedarf es der Einwilligung durch Nutzerinnen und Nutzer.

Daten, die während der Nutzung vorübergehend gespeichert werden (z.B. Navigation), müssen nach Ende der Nutzung gelöscht werden.

Die Speicherung personenbezogener Daten der Nutzerinnen und Nutzer ist grundsätzlich unzulässig.

2. Verarbeitung von Daten

2.1. Sicherheit und Robustheit

Die Sicherheitsvorschriften für Produkte müssen auch für Dienstleistungen gelten, die auf Technologien basieren, die algorithmische Systeme nutzen. Die Sicherheit der Produkte und Dienstleistungen ist auf dem Stand der Technik zu halten. Dies gilt für den gesamten Lebenszyklus eines Produktes und für Dienstleistungen (Qualitätssicherung). Algorithmische Systeme mit hohem Risiko sind alle zwei Jahre durch die zuständige Prüfinstitution zu überprüfen.

2.2. Daten aus dem Internet der Dinge

Verhaltensgenerierte Daten dürfen nur für den durch das Gerät vorgegebenen Zweck genutzt werden. Daten, die durch ein Gerät generiert werden und einen Personenbezug beinhalten, dürfen nur gespeichert und weiterverarbeitet werden, wenn der Personenbezug anonymisiert wird. Die Weiterverarbeitung personenbezogener Daten zu anderen Zwecken als jenen, die sich aus der Nutzung der Geräte ergeben, sind grundsätzlich unzulässig.

2.3. Nicht-Diskriminierung und Fairness

Diskriminierung wird als die Benachteiligung von Gruppen oder Personen verstanden, z.B. auf Grund ihrer Herkunft, ihres Geschlechts, ihrer Religionszugehörigkeit oder ihrer sozialen Stellung. Fairness steht gemeinhin für gerechtes, anständiges und ehrliches Handeln.

Die Grundsätze der Nicht-Diskriminierung und Fairness sind einzuhalten, besonders um das durch das Grundgesetz garantierte Grundrecht auf Gleichbehandlung umzusetzen. Die Verwendung anderweitig beschaffter Daten von Dritten ist unzulässig, sofern keine Nachvollziehbarkeit und Transparenz vorliegt.

Bei standardisierten Endverbraucherprodukten und -dienstleistungen sind individualisierte Preise verboten.

2.4. Profiling

Das Erstellen des Gesamtbildes einer Persönlichkeit darf ausschließlich streng zweckgebunden erfolgen und ist nur zulässig mit Einwilligung der Nutzerin oder des Nutzers.

2.5. Scoring

Das menschliche Verhalten wird beim Scoring auf einen Wert reduziert, z.B. wird das Verhalten in Beziehung zu einer vertraglichen Verpflichtung gesetzt. Scoring trägt das Potential zu Diskriminierung bzw. Benachteiligung in sich. Wird bei der Nutzung von angebotenen Dienstleistungen ein Scoring vorgenommen, so ist die Nutzerin oder der Nutzer darüber zu informieren. Auf Verlangen der Nutzerin oder des Nutzers ist das Zustandekommen des sie betreffenden Scores offenzulegen und zu erläutern. Beim Gesetzgeber ist darauf hinzuwirken, dass das Zustandekommen des Scores, seine Offenlegung und Erläuterung, nicht mit dem Hinweis auf Betriebs- und Geschäftsgeheimnisse verweigert werden darf.

3. Institutionen

Ein auf sozialer Marktwirtschaft basierendes Wirtschaftssystem braucht vertrauenswürdige, unabhängige und parlamentarisch kontrollierte Institutionen, um die Umsetzung von Rechtsvorschriften bei den eingesetzten Softwaresystemen zu überprüfen und durchzusetzen. Das müssen für die verschiedenen Sektoren (Gesundheit, Verkehr, Energie, Finanzen, Justiz, Handel und Verbraucher) gesetzlich verankerte Institutionen sein. Sie dürfen nicht im Wettbewerb zu einander stehen. Sie müssen unabhängig sein und der parlamentarischen Kontrolle unterstehen. Für sie muss ein gesetzlich verankertes Auskunftsrecht und eine Berichtspflicht verfügt werden. Sie sind ausreichend mit qualifizierten Ressourcen (Personal, Finanzen, Technik) auszustatten.

3.1. Qualitätsüberwachung

Die gesetzlichen Prüfinstitutionen haben die Aufgabe der Qualitätsüberwachung, Kontrolle und Einhaltung der gesetzlichen Vorgaben. Dazu gehören u.a. Updates über den gesamten Lebenszyklus eines eingesetzten algorithmischen Systems und die Gewährleistung der Cybersicherheit nach dem Stand der Technik.

3.2. Zulassung und Datenfolgeabschätzung

Algorithmische Systeme, die personenbezogene Daten in Risikobereichen verarbeiten, bedürfen der Zulassung durch die gesetzliche Prüfinstitution. Zu prüfen sind insbesondere Sicherheit, die Einhaltung gesetzlicher Vorschriften und Transparenz durch das Datensicherheitsblatt (siehe Anlage).

Algorithmische Systeme mit hohem Risiko (ab Stufe 3; siehe 4.2 Kritikalität) müssen alle zwei Jahre überprüft werden.

Für ihre Implementierung ist eine Datenfolgeabschätzung (DFAS) gemäß Art. 35 DSGVO vorzunehmen.

3.3. Gültigkeit der Regulierung für ausländische Anbieter

Die Regelungen müssen für alle Anbieter verpflichtend sein, die sich an den deutschen Markt richten, auch wenn der Firmensitz im Ausland ist. Der Anbieter ist verpflichtet eine Niederlassung in Deutschland zu unterhalten. Sie unterliegt der deutschen Gerichtsbarkeit.

4. Transparenz

4.1. Nachvollziehbarkeit

Die von algorithmischen Systemen errechneten Ergebnisse müssen für Nutzer und Nutzerinnen nachvollziehbar und justiziabel sein.

Bei selbstlernenden, algorithmischen Systemen muss das System so trainiert werden, dass die Zielvorstellungen im Ergebnis erreicht werden. Die Trainingsdaten müssen dokumentiert und in einer datenschutzgerechten Form gespeichert werden, damit sie zu Zwecken der Simulation eingesetzt werden können. Denn nur so sind einzelne Ergebnisse nachvollziehbar. Der materielle Aufwand ist dabei so groß, dass die Dokumentation und Speicherung von Trainingsdaten beim jetzigen Entwicklungsstand nur bei Entscheidungen mit hohem Risiko gerechtfertigt erscheint (vgl. Kritikalität).

4.2. Kritikalität

Um die Nachvollziehbarkeit von auf Algorithmen basierten Entscheidungen zu gewährleisten und praktikabel zu machen, schlägt die Datenethikkommission (DEK) der Bundesregierung eine Einteilung der Algorithmen nach dem Schädlichkeitspotential des Algorithmus für Menschen vor (siehe auch Weißbuch der EU-Kommission zur künstlichen Intelligenz, S. 12). Die DEK empfiehlt eine 5-stufige Einteilung. Persönliche Auskunftspflichten sind besonders in den Risikosektoren Gesundheit, Verkehr, Versicherungen, Personalentscheidungen, Justiz, Banken, Finanzen und öffentliche Verwaltung einzurichten. Das sektorale Gefährdungspotential ist mit dem persönlichen Risiko im Hinblick auf Verletzungs- oder Lebensgefahr und materielle oder immaterielle Schäden abzugleichen. Transparency Deutschland unterstützt diesen Vorschlag mit der Maßgabe, dass wirtschaftliche Interessen bei den notwendigen Abwägungen nachrangig zu behandeln sind.

4.3. Kennzeichnungspflicht

Algorithmische Systeme sind zu kennzeichnen, wenn sie personenbezogene Daten verarbeiten. Es ist für den menschlichen Kommunikationspartner transparent zu machen, wenn mit einem KI-System kommuniziert wird.

4.4. Auskunftspflichten

Die Pflicht zur Auskunft besteht gegenüber den Nutzerinnen und Nutzern bei Entscheidungen mit Schädigungspotential (siehe Kritikalität, dazu gehören z.B. Auskünfte über die Kreditwürdigkeit), die von algorithmischen Systemen oder von Personen mit Unterstützung von algorithmischen Systemen getroffen wurden. Die Entscheidung muss nachvollziehbar sein durch Offenlegung der Entscheidungskriterien. Sie muss korrigierbar und justiziabel sein und sie muss durch Personen kommuniziert werden. Diese Auskunftspflichten gegenüber Nutzerinnen und Nutzern gehen den Betriebs- und Geschäftsgeheimnissen vor.

4.5. Betriebs- und Geschäftsgeheimnisse

Stehen dem Auskunftsverlangen der Nutzer und Nutzerinnen in den Risikosektoren nach vollständiger Offenlegung Betriebs- und Geschäftsgeheimnisse entgegen, ist der sektorale staatliche Treuhänder (siehe Institutionen) einzuschalten. Zur Offenlegung gegenüber den Treuhändern sind die Betreiber der algorithmischen Systeme verpflichtet. Der Treuhänder vertritt die Interessen der Nutzerinnen und Nutzer. Der Treuhänder informiert Nutzerinnen und Nutzer, ohne Betriebs- und Geschäftsgeheimnisse preiszugeben.

4.6. Schutzinformationen

Da Algorithmen mit Daten arbeiten, sind Informationen über die Daten und die Art der Datengewinnung, des Datenschutzes und Basisinformationen über den Algorithmus erforderlich.

Zu den vorgeschriebenen Informationen über den Datenschutz bei Webseiten oder Apps muss das Datensicherheitsblatt aufgeführt werden. Bei Cookies sind die Alternativen – wie ablehnen, technisch notwendig, Analyse des Verhaltens auf der Website, Datennutzung zu Werbezwecken, Handel und Verkauf von personenbezogenen Daten – aufzuführen. Ferner ist ein Button „Basisinformation“ vorzusehen. Mit ihm wird das jeweilige Datensicherheitsblatt aufgerufen.

4.7. Datensicherheitsblatt

Das Datensicherheitsblatt informiert in knapper, übersichtlicher, tabellarischer Form über die Eckdaten eines Algorithmus (siehe Anlage).

5. Wettbewerb

Im Internet werden besonders in den sozialen Netzwerken „kostenlose“ Dienstleistungen angeboten, wenn im Gegenzug persönliche Daten (dazu zählen auch verhaltensgenerierte Daten) gesammelt, aufgezeichnet, verarbeitet, gespeichert und für verschiedenste Geschäftszwecke genutzt werden dürfen.

Die Datenschutzgrundverordnung (DSGVO) verlangt, dass die Einwilligung zur Datennutzung freiwillig geschehen muss. Die freiwillige Nutzung setzt adäquate Wahlmöglichkeiten voraus. Dem stehen Monopole und Oligopole besonders in digitalen Märkten entgegen. Den Kartellbehörden obliegt es, die Voraussetzungen für den Wettbewerb auch auf digitalen Märkten durchzusetzen und zu sichern. Wettbewerb ist erforderlich, damit die Schutzrechte der DSGVO in der Praxis durchsetzbar sind und Missbrauch eingedämmt werden kann. Um den Wettbewerb auf digitalen Märkten vor Missbrauch von Marktmacht zu schützen, muss das Gesetz gegen Wettbewerbsbeschränkungen novelliert werden. Dabei sind besonders die Schlüsselmerkmale – extreme Skalenerträge, Netzwerkeffekte und die besondere Rolle von Daten – zu berücksichtigen. Transparency Deutschland unterstützt den Vorschlag der Bundesregierung.

5.1. Preisabsprachen

Von Algorithmen automatisiert gesteuerte Preisangleichungen sind wie analoge Preisabsprachen zu behandeln. Sie entsprechen einem Monopolverhalten und setzen die Vielfalt von Märkten außer Kraft.

5.2. Intermediationsmacht

Bei der Bewertung der Marktmacht sind auch Einflussnahmen der Plattformen durch Listing und Ranking zu bewerten.

5.3. Selbstbevorzugung

Verboten ist die Selbstbevorzugung durch vorteilhaftes Listing eigener Produkte der Plattformbetreiber.

5.4. Portabilität und Interoperabilität

Transparency Deutschland tritt für eine Verpflichtung zu Portabilität bei Plattformdiensten (z.B. bei Banken) und für Interoperabilität (z.B. bei Email-Diensten) ein, um Monopolstrukturen und Lock-in-Effekte aufzubrechen und um die Voraussetzungen zur Freiwilligkeit bei der Zustimmung zur Nutzung der persönlichen Daten zu schaffen.

6. Algorithmische Systeme und öffentliche Hand

6.1. Open Source

Open-Source-Programme (wie Linux) oder -Protokolle (E-Mail oder Internetprotokolle wie http) sind quelloffen und können von jedem eingesehen, geprüft und genutzt werden. Quelloffene Software schafft Transparenz und Kontrolle. Sie schützt dadurch vor Missbrauch. Programme der öffentlichen Hand oder mit öffentlichen Geldern finanzierte Programme haben quelloffen zu sein.

6.2. Sicherheit durch dezentrale Speicherung von Daten.

Das Prinzip möglichst dezentraler Speicherung, besonders bei personenbezogenen Daten, ist einzuhalten. Durch die dezentrale Speicherung wird der missbräuchliche Zugriff auf Daten deutlich erschwert, vgl. die Debatte um die Corona-App der Bundesregierung.

6.3. Datenschutzfolgeabschätzung

Bei allen algorithmischen Systemen, die mit personenbezogenen Daten und in Bereichen mit hohem Risiko arbeiten, ist eine Datenschutzfolgeabschätzung nach DSGVO Art. 35 vorzunehmen.

_____

Verfasst von der Arbeitsgruppe Digitalisierung

Verabschiedet in der Vorstandssitzung am 19. Juni 2020

ANLAGE: Erläuterung zum Datensicherheitsblatt

Um mehr Sicherheit und Transparenz beim Einsatz von Algorithmen für Nutzerinnen und Nutzer zu schaffen, schlägt Transparency Deutschland ein Datensicherheitsblatt für Algorithmen vor. Als Beispiel dient das Informationssystem REACH der EU für chemische Stoffe, die für das Sicherheitsdatenblatt der chemischen Industrie verantwortlich zeichnet. Ziel dieses Systems ist die Gewährleistung der sicheren Verwendung dieser Stoffe. Das Informationssystem klärt auf über gefährliche Eigenschaften, Einstufung und Kennzeichnung, sowie über sichere Aufbewahrung. In Analogie zu chemischen Stoffen ist der Zweck eines Datensicherheitsblattes Basisinformationen über einen eingesetzten Algorithmus zu geben. Jede Nutzerin und jeder Nutzer sollte Informationen über den Zweck des Algorithmus und seine Kritikalität erhalten, wenn personenbezogene Daten verarbeitet werden, dazu gehören auch verhaltensgenerierte Daten, die sich Personen zuordnen lassen (zur Kritikalität siehe Positionspapier 4.2.).

Transparency International Deutschland e.V.
Tel. +49 30 549898-0 | Fax +49 30 549898-22
E-Mail: office@transparency.de
Webseite: www.transparency.de

ANLAGE: Datensicherheitsblatt für Algorithmen

	1.0	**Identifizierung der App**	**Beispiel 1**	**Beispiel 2**	**Beispiel 3**
	1.1	**Name der App**	**booking.com**	**garmin App**	**WhatsApp**
	1.2	Anbieter		Garmin (Sport / Fitness)	WhatsApp
	1.3	Versionsnummer			
	1.4	Sprach/Länderversion			
	1.5	Datum In-Verkehrbringung			
	1.6	Entwickler der APP			
	1.7	GAFAM (Google, Amazon, …) zugehörige? Welche?	???	???	Facebook
	2.0	**Zweck der App**			
Nutzen/Funktionalität?	2.1	Reisemöglichkeiten vorschlagen	schlägt Hotels & Mietwagen vor	Lauf/Radtouren aus Datensammlung	nein
	2.2	Reservieren & Ticket buchen	ja	nein	nein
	2.3	Angebot an Gütern anzeigen	nein	nein	nein
	2.4	Kauf von Gütern	nein	nein	nein
	2.5	Selbstdarstellung (Facebook, Instagramm, Twitter ...)	nein	durch seine eigenen Leistungen	ja
	2.6	Persönlicher Chat (WhatsApp u.ä)	nein	nein	ja
	3.0	**Stammdaten (soweit erforderlich)**			
Erklären, warum diese	3.1	Name, Vornahme	ja	ja	ja
Daten erforderlich sind	3.2	Zahlungsmittel	ja	in App Käufe	nein
	3.3	Email	ja	ja	ja
	3.4	Handynummer	ja	nein	ja
	3.5	Adresse	nein	nein	nein
	4.0	**Pers. Daten für die technische Funktion der App**			
Erklären, warum diese	4.1	Standort / Bewegungsdaten (GPS)	fragt nach	ja	nein
Daten erforderlich sind	4.2	Zeichnet persönliche Historie auf	ja	ja	ja
	4.3	Kontakte	nein	nein	ja
	4.4	Mikrophon	nein	nein	ja
	4.5	Kamera	nein	nein	ja
	4.6	Surfverhalten (Webseiten, Dauer)	???	nein	nein
	4.7	Statische Körperdaten (Größe, Gewicht, Geschlecht, Alter)	Alter, Geschlecht	Alter, Geschlecht, Größe, Gewicht	nein
	4.8	Dynamische Körperdaten (Puls, weitere …)	nein	Puls, Schrittfrequenz, Symmetrie	nein
	4.9	Zugehörigkeit (Rasse, Hautfarbe, Ethnie, Religion, Abstammung, …)	nein	nein	nein
	4.10	Meinungsaußerungen (Chat, …)	Bewertungen	nein	ja
	4.11	Lebensituationen (Facebook, Instagramm, ...)	nein	nein	ja
	5.0	**Prüfung der Algorithmen, Zertifizierung durch unabhängige staatlich überwachte Institutionen**			
Verifizierung ob Korrekt	5.1	Datensätze, die in die Entwicklung/in das KI Training der App eingegangen sind			
Kontrolle durch Menschen	5.2	Plausibilitätschecks, dass die Apps/KI auch die richtigen Ergebnisse liefert			
	5.3	Plausiblitätschecks, die Grenzbereiche von Korrelationen aufweisen (Berücksichtigung)?			
	5.4	Zertifizierung als Voraussetzung für die Nutzung der App mit persönlichen Daten			
	5.5	Festlegung von Wiederholungsprüfungen, auch zwecks Autorisierung von Weiterentwicklungen			
	6.0	**Datenverarbeitung durch den Anbieter**			
Anbieter erklärt	6.1	Personifizierte Werbung	???		nicht in der App
was mit den Daten	6.2	Mitteilungen schicken	fragt nach (habe ich verneint)		nein
und ihrer Auswertung	6.3	Datenverkauf an Dritte (z.B. Facebook and CA)	???	??? (Hoffentlich nicht)	???
geschieht, insbesondere	6.4	Datenservice für Dritte (z.B. Cambridge Analytica für US Wahlkampf)	???	???	???
Teilen mit Dritten	6.5	Erstellung von Profilen für Dritte (Banken, Versicherungen, Krankenkassen, …)	???	???	???
	6.6	Anonyme Nutzungsstatistiken	???	???	???
	6.0	**Datenspeicherung**			
wie sicher werden	6.1	Speicherort der Daten (Nation)	???	???	???
Daten übertragen,	6.2	Sicherheitsstandards bei Übermittlung (z.B. End-to-End Verschlüsselung)	???	???	???
gesichert, gelöscht	6.3	Löschungsprozess/datum der persönlichen Daten	???	???	???