

ENGLISH ARTICLE BELOW

Wer steuert in Zukunft unsere Entscheidungen? Wir, Artificial Intelligence – oder deren EigentümerInnen?

Florian Gasser, Institut für Systemisches Management & Public Governance, Universität St. Gallen
Mauro Gotsch, Institut für Marketing und Customer Insight, Universität St. Gallen

Abstract

Dieser Beitrag befasst sich mit den aktuellen gesellschaftlichen Herausforderungen von aufstrebenden datengetriebenen Technologien wie Artificial Intelligence (AI) (durch z.B. ChatGPT) als auch mit personalisierten Werbestrategien. Es zeigt sich bis dato, dass die Regularien in vielen diesen schnellweiterentwickelnden Bereichen hinterherhinken. Dieses Manko führt zu einem Machtgefälle zwischen international operierenden Konzernen und Bezugsgruppen, deren Datenschutzrecht durch die Nutzung von diesen neuen Technologien erodiert werden. Die Autoren schlagen vor, dass a) das Bewusstsein der Implikationen der Datenverwendung in neuen Technologien wie AI als auch für Werbezwecke bei der Bevölkerung erhöht werden sollte, b) dass das generelle Consent Management überarbeitet werden und sich eng an das DSGVO-Prinzip von «privacy by design» orientieren sollten und c) die Wissenschaft und die Gesellschaft sich noch stärker mit der Ausgestaltung der gesellschaftsorientierten Rahmenbedingungen auseinandersetzen sollte, um eine nachhaltige Nutzung neuer Technologien zu fördern.

Keywords: Privacy by Design; Consent Management; Datenschutz, Artificial Intelligence

Jede Generation hat seine Herausforderungen. Dies wussten bereits unsere Grossväter, die den zweiten Weltkrieg miterlebt, oder den Aufbau der Gesellschaft nach diesem zum Ziel hatten. Die Herausforderungen heute sind von ganz anderer Natur; Sie bestehen vor allem aus 0en und 1en und umfassen im 21. Jahrhundert so ziemlich jeden Lebensbereich. Ob man sich online verabredet, seine Finanzen verwaltet, seinen nächsten Lieblingsausflug nach Südtirol plant, einen kurzen Essay unterstützt durch *ChatGPT* verfasst, ein Stand-up-Paddle-Board für den nächsten Urlaub bestellt oder den Instagram-Kanal nach Omas Nähtipps durchforstet. All dies ist heute digital möglich, und noch nie war es so bequem. Doch mit welchen versteckten Herausforderungen kommt diese Bequemlichkeit?

In der kurzen Geschichte der Menschheit gab es noch nie einen so skalierbaren, dynamischen und immanenten Wandel: die digitale Transformation. Der allgegenwärtige Zugang zu Rechenkraft und Daten hatte einen vergleichbaren Einfluss auf die Weltwirtschaft wie Fords Massenproduktion in 1913. Der Unterschied ist die Zeitspanne. Die Tech-Giganten aus dem Silicon Valley errichteten innerhalb von knapp 25 Jahren ein Ökosystem, welches die Wertschöpfung der alten Wirtschaftsmächte Öl, Stahl und Bankwesen bereits heute um ein Vielfaches übertroffen hat.ⁱ

Die dominante Logik der Wirtschaft von standardisierter Massenproduktion zu kleinen Stückzahlen wird in diesem neuen Paradigma abgelöst durch einen neuen digitalen Tellerwäschertraum: Jeder Person ist es möglich, ein Startup zu gründen, das in kurzer Zeit die Aufmerksamkeit und Skalierung eines «analogen» Unternehmens übertreffen kann. Die Jagd nach diesen treffend benannten "Einhörnern" ist zu einem Generationstraum geworden - raus mit dem Alten, rein mit dem Neuen. Im Einklang mit diesem Verständnis wurden die Gatekeeper der Medienhäuser ersetzt durch die Tech-Giganten aus dem Silicon Valley. Jeder kann seine Meinung mit anderen teilen und zu jeder Tageszeit nahezu unbegrenzt Informationen online abrufen. Meinungsführer wurden zu Social Media-Influencer und Banken wurden zu Venture Capitalists und Business Angels. So lässt sich kurzerhand das goldene Zeitalter der Digitalisierung beschreiben, welches jedoch nicht nur mit positiven Auswirkungen für die Gesellschaft einhergeht.

Die Implikation dieses neuen Marktökosystems ist deutlich: Produktivität ist getrieben durch Innovation und Zugang zu dem neuen Öl: Daten. Weltweit investieren Tech-Firmen Unsummen in Forschungs- und Entwicklungsprojekte für Produkte, welche neue Aspekte unseres Lebens digitalisieren. Die daraus entstehenden Produkte machen unser Leben wesentlich leichter: künstliche Intelligenzen und Big Data-getriebene Datenverarbeitungsprozesse erlauben uns effiziente Navigation, effizienteres Einkaufen und sogar verbesserte Gesundheit. Aus Unternehmenssicht bietet jede digitale Dienstleistung allerdings auch die Möglichkeit, neue Datenlieferketten zu erschliessen. Google Maps kennt unser Bewegungs- und Einkaufsverhalten. Amazons Alexa weiss wie wir sprechen und was uns interessiert. Facebook kennen unsere politische Einstellung und sexuelle Orientierung.ⁱⁱ Diese Daten werden wiederum verwendet, um neue künstliche Intelligenzen zu trainieren und menschliches Verhalten vorherzusagen.

Was auf den ersten Blick aussieht wie ein normaler Marktaustausch – Daten gegen Dienstleistung – beruht auf einem äusserst einseitigen Machtverhältnis. Grosse Konzerne und

Staatsapparate bestimmen die Bedingungen dieses Austausches praktisch unilateral, was längerfristig zu einer für Konsumenten gefährliche Entwicklung führt. Darin folgt die Verarbeitung und Erhebung von Daten noch immer einer Internetlogik aus den 90er Jahren. Unlesbare Datenschutzvereinbarungen werden Konsumenten beim Kauf von digitalen Services aufgedrückt, was als Zustimmung für die Nutzung sämtlicher durch die Person in dem Service produzierten Daten verstanden wird. Es geht dabei vor allem um das Abgreifen von Verhaltensdaten, welche nur indirekt etwas mit genutzten Service zu tun haben. Google Maps merkt sich nicht nur die gesuchten Routen des Nutzers, sondern auch wo diese Person einkehrt. Virtual Private Network Apps verschleiern zwar die Internetaktivitäten seiner Nutzer gegenüber Webseitenbetreibern, speichern diese Daten aber häufig für die eigene Nutzung.ⁱⁱⁱ

Das an sich ist schon problematisch - doch davon ausgehend, dass wir als Menschheit diese Als nutzen wollen, um die Welt um uns herum zu verändern (beispielsweise durch Vorhersagealgorithmen für Rückfälligkeitsraten in Verbrechen^{iv}, Sozialkreditsysteme zur Verhaltenslenkung^v, oder Genommodelle zur Berechnung von Krankheitswahrscheinlichkeit in Föten^{vi}) laufen wir in eine immanente Gefahr, dass wir neue Machtstrukturen erschaffen, die auf der zustimmungsfreien Ausbeutung von persönlichen Daten beruhen. Diese Strukturen können dann dazu verwendet werden, um unser Verhalten zu lenken um neue Daten zu generieren. Sind solche Strukturen erst einmal etabliert, wird es schwer, sie wieder niederzureissen.

Um die Auswirkungen zu verdeutlichen, wollen wir ein fiktionales aber heute bereits mögliches Beispiel durchspielen: Eine Fast-Food-Kette versucht sich in einer Kleinstadt zu etablieren. Dazu verteilen sie Flyer für die Restaurant-App mit exklusiven Gutscheinen in ihrem Stadtviertel. Weil es im Verhältnis zu anderen ausgewogeneren Alternativen günstig ist, entscheidet sich ein Kunde zu dem Restaurant zu gehen und bezahlt dort seinen Konsum mit einem Promotionscode und am besten noch in der Unternehmens-App. Dieses Entscheidungsverhalten wird zusammen mit einem Targeting Algorithmus verarbeitet. Das Restaurant lernt dadurch kontinuierlich dazu, wie sie jene Person am besten dazu ermutigen kann, in Zukunft wieder dieselbe Entscheidung zu treffen. Um dies zu erreichen, wird die digitale Umwelt des Kunden so verändert, dass die Wahrscheinlichkeit steigt, ihn wieder in das Restaurant oder in andere Filialen zu locken. Konkret sieht das so aus, dass der Kunde bei seinem alltäglichen Internetkonsum, sei es das Youtube Video zu Omas Strickkurs, oder bei dem Teilen von Urlaubsbildern auf Instagram, immer wieder Werbung des Restaurants sieht und Gutscheine zugespielt bekommt. Auf Basis seiner Suchhistorie

ist es möglich die Gefühlslage oder relevante Suchwörter in Bezug auf Essen für die jeweilige Person zu identifizieren – und darauf zu reagieren. Pushnachrichten mit weiteren Essensrabatten werden ausgespielt, wenn die Person am ehesten darauf reagiert: im Pendlerverkehr, nach einem langen Arbeitstag, etc. Das jeweilige Verhalten wird nicht nur gesteuert, sondern die Daten des einen Kunden verbessern Tag für Tag wiederum diese Steuerung für die gesamte Kundschaft. Ins Extreme geführt bedeutet dies, dass alltägliche Entscheidungen vorweggenommen werden - bevor Sie selbst bewusst getroffen wurden. Eine perfekte Vorhersage eines Verhaltens, dass durch die Vorhersage ausgelöst wurde.

Das Problematischste dabei ist nicht unbedingt die Steuerung an sich, sondern dass der einzige Impuls den der Kunde im Beispiel für die Steuerung gegeben hat, ein schneller Klick auf "akzeptieren" in der Fastfood App war, welche dieser entweder a) nicht gelesen hat, oder b) auch beim Lesen nicht verstanden hat, da die zentralen Informationen sich in einem Meer von AGBs nahtlos einbetten^{vii}.

Häufig führen diese im ersten Anschein unschuldigen Klicks dazu, die Zahlungsbereitschaft spezifischer Kundengruppen zu erfassen und diese durch verschachtelte Cookie-Bedingungen intransparent zu halten^{viii}. Die Gesetzeslage der EU hat mit der DSGVO zwar einen klaren Gegenimpuls gegeben – doch die EU berichtet auch, dass 97% der grössten Online Shops in Europa^{ix} absichtlich diese Intransparenz durch das Design ihrer Website fördern. Das Gleiche gilt für die Empfehlung von Produkten und Dienstleistungen auf der Grundlage eines gemeinsamen Standorts, Werbeschaltung von Marken, die in der Nähe eines audioaufnahmefähigen Geräts ausgesprochen werden, oder die Anzeige der am besten geeigneten Produkte und Dienstleistungen als Werbebotschaft unter den gesuchten Inhalten. Die Umgehung dieser Geschäftspraktiken führt in der Regel zu einem undurchsichtigen «*Cookie-Bypass-Tango*», den viele User irgendwann aufgeben^x.

Diese neue digitale Geschäftslogik ist jene, worauf heute die meisten Werbetreiber ihre Funktionalität ausrichten^{xi}. Wenn diese Logik aber nicht mehr nur für das reine Profitstreben Verwendung findet, sondern auch auf entscheidende Lebensbereiche, wie Politik, Gesundheit und eigene Finanzen überschwappt, kann dies nicht nur zu einem Problem, sondern zu weiteren gesellschaftlichen Krisen führen.

Um dies zu verhindern, muss das «*Consent Management*» schon heute – am besten schon gestern – auf die technischen Möglichkeiten unserer Zeit angepasst werden. Es ist Tatsache, dass das starre Rechtssystem bei schnellen technologischen Entwicklungen hinterherhinkt^{xii}. Um den Prozess der notwendigen rechtlichen Rahmenbedingungen

frühzeitig zu fixieren bzw. die Gefahr einer erst zu spät entdeckten AI-Steuerungsstruktur zu umgehen, muss jetzt reagiert werden. Ist eine AI-Steuerungsstruktur erst einmal umgesetzt und implementiert, ist sie schwer noch in den Griff zu bekommen, ohne mit ihr verbundene Dienstleistungen im Ökosystem ebenfalls zu zerstören^{xiii}.

Wie gross die Macht von einzelnen Konzernen bereits ist, zeigt sich bei Google und Meta, welche aufgrund ihrer Grösse und finanziellen Möglichkeiten die Politik und die Gesetzgebung in vielen Ländern schon im Vorfeld beeinflussen können und massgeblich an der Meinungsbildung der Bevölkerung beteiligt ist^{xiv}. Erst im Oktober 2022 haben mehrere Mitglieder des EU-Parlaments eine Lobbying-Beschwerde gegen Meta, Google und Amazon eingereicht, da diese äusserst offensiv im Vorfeld über eine externe Lobbygruppe ohne Offenlegung für die Abstimmung über den «*Digital Markets Act*» lobbyiert haben.^{xv} Auch zahlreiche weitere Berichte zeigen auf, in welcher Art und Weise über bald ein Jahrzehnt grosse US-Tech-Firmen ihre Interessen über Beeinflussungsstrategien auf politischer Ebene verfolgen.^{xvi} Wie Zuboff, Autorin von «*Age of Surveillance Capitalism*» beschreibt *“It is possible to have surveillance capitalism, and it is possible to have a democracy. It is not possible to have both”*^{xvii}. Daher ist es wichtig, so bald wie möglich Leitlinien festzulegen, um das *Consent Management* wieder unter demokratische Kontrolle zu bringen.

Ein Reagieren auf neue technologische Vorstösse und ein Vertrauen auf die Selbstregulierung aller involvierter Parteien allein kann das Aufkommen von problematischen Datenverarbeitungspraktiken nicht verhindern^{xviii}. Um Herr und Frau der Lage zu werden, ist die Kooperation aller Stakeholder in einem Datenökosystem unabdingbar.

Hier kann die Wissenschaft einen wesentlichen Beitrag leisten, um Kontrollmechanismen zu installieren bzw. vor etwaigen negativen Auswirkungen für die Allgemeinheit zu informieren. Eine zentrale Rolle spielt hier auch die Wissenschaftskommunikation. In der Vergangenheit konnten komplexe Sachverhalte häufig nicht in einfach verständliche Nachrichten übersetzt werden, sodass wesentliche wissenschaftliche Erkenntnisse für Teile der Gesellschaft nicht greifbar gemacht werden konnten. So sollten WissenschaftlerInnen unterstützt werden, Themen wie Privacy und AI faktenorientiert und einfach verständlich aufzuarbeiten und der Allgemeinheit zur Verfügung zu stellen.

Die Politik und Bildungsinstitutionen müssen zusätzlich dafür sorgen, dass die bevölkerungsweite notwendige Aufmerksamkeit geschaffen wird, welchen Einfluss Datenverarbeitung und AI-getriebene Vorhersagemodelle auf unser tägliches Leben bereits haben und in Zukunft noch haben könnten. Die Kundschaft von datenintensiven Dienstleistungen

muss verstehen, dass ihre Interaktion mit dem Dienst Daten generiert, welche weitaus mehr Rückschlüsse auf ihr Leben zulässt, als ihnen vielleicht angenehm ist. Darüber hinaus sind Entwickler und Innovatoren gefragt, ihre Arbeitgebenden mit ethischen Fragestellungen zu konfrontieren und auch bei sinnreichen Regulierungsmassnahmen mitzuarbeiten. Nur durch die Integration der Kundschaft in die Datenwertschöpfung können Geschäftsmodelle in diesen zukunftsorientierten Branchen nachhaltig bestehen. Datenschutz muss dabei als zentraler Designaspekt verstanden werden, nicht als Einschränkung.

Zukunftsgerichteter Umgang mit persönlichen Daten darf diese nicht als zu erobernde Ressource verstehen, sondern als beschütztes Eigentum jeder Person. Das Credo der DSGVO – «*privacy by design*» - ist eine solide Basis für zukünftige Bemühungen. Doch auch diese Basis muss aufgrund der sich kontinuierlich weiterentwickelnden technologischen Möglichkeiten immerzu adaptiert werden.

Wir brauchen einen gesunden wissenschaftlichen Dialog, welcher unser Wissen über Zustimmungsmanagement und Datenschutzbedürfnisse von Konsumenten weiter vertiefen kann. Wir müssen verstehen, dass viele aktuelle digitale Geschäftsmodelle das effektive Datenschutzselbstmanagement von Konsumenten verunmöglicht – oder eben jenen Zustand sogar dezidiert ausnützt, um das eigene Gewinnstreben zu maximieren. Wir brauchen neue Technologien, welche den Big Data Verbrennungsmotor des Internets durch eine «emissionsfreie» Alternative ersetzen kann. Wir brauchen gesetzliche Vorstösse, welche sich auf die Konsequenzen von Datenverarbeitungen konzentrieren anstatt nur auf die Datenerhebung. Wir brauchen Regularien, die nicht nur reagieren, sondern proaktiv die Zukunft mitgestalten, Rechtssicherheit liefern und gleichzeitig von Anfang an Missbrauch bestmöglich unterbinden.

Kurzum, wir brauchen Lösungen für die rechtlichen, technischen, ethischen und psychologischen Probleme der aktuellen Datenverarbeitungslogik, wenn wir deren Früchte auch in der Zukunft geniessen möchten, ohne irgendwann zu bemerken, dass unsere Entscheidungen nicht mehr unsere eigenen sind.

Literaturverzeichnis

- ⁱ American Business History Center (2022). Most Valuable Companies: The Last 25 Years, online: <https://americanbusinesshistory.org/most-valuable-companies-the-last-25-years/>
- ⁱⁱ Chen, D., Fraiberger, S. P., Moakler, R., & Provost, F. (2017). Enhancing transparency and control when drawing data-driven inferences about individuals. *Big data*, 5(3), 197-212.
- ⁱⁱⁱ How to Geek (2019). Do not use Facebooks Onavo VPN: It's Designed to Spy On You, online: <https://www.howtogeek.com/342731/dont-use-facebooks-onavo-vpn-its-designed-to-spy-on-you/>
- ^{iv} Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science advances*, 4(1), eaao5580.
- ^v Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, 49(2), 187-212.
- ^{vi} Nature (2022). The controversial embryo tests that promise a better baby, online: <https://www.nature.com/articles/d41586-022-02961-9>
- ^{vii} Slepchuk, A. N., & Milne, G. R. (2020). Informing the design of better privacy policies. *Current Opinion in Psychology*, 31, 89-93.
- ^{viii} Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1-13).
- ^{ix} European Commission (2022). Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation: final report, Publications Office of the European Union, online: <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418>
- ^x Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.*, 126, 1880.
- ^{xi} Zuboff, S. (2019, January). Surveillance capitalism and the challenge of collective action. In *New labor forum* (Vol. 28, No. 1, pp. 10-29). Sage CA: Los Angeles, CA: SAGE Publications.
- ^{xii} Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash. L. Rev.*, 89, 1-51.
- ^{xiii} Vgl. z.B. Gizmodo (2019). Life Without the Tech Giants, online: <https://gizmodo.com/life-without-the-tech-giants-1830258056>
- ^{xiv} CNBC (2018). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal, online: <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>
- ^{xv} Bloomberg (2022). US Tech Firms Hid Lobbying Efforts, European Parliament Says, online: <https://www.bloomberg.com/news/articles/2022-10-14/big-tech-firms-hid-lobbying-efforts-european-parliament-says>
- ^{xvi} The Guardian (2022). I saw first-hand how US tech giants seduced the EU – and undermined democracy, online: <https://www.theguardian.com/commentisfree/2022/jun/28/i-saw-first-hand-tech-giants-seduced-eu-google-meta>
- ^{xvii} Zuboff, S. (2022). Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. *Organization Theory*, 3(3), 5.
- ^{xviii} Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash. L. Rev.*, 89, 1-51.

Who will control our decisions in the future? Us, Artificial Intelligence - or their owners?

Florian Gasser, Institute for Systemic Management & Public Governance, University of St. Gallen
Mauro Gotsch, Institute for Marketing and Customer Insight, University of St. Gallen

Abstract

This paper addresses the current societal challenges of emerging data-driven technologies such as the rise of artificial intelligence (AI) (with tools like ChatGPT) as well as personalized advertising strategies. The vivid discussions on data ownership and privacy surrounding these technologies makes it apparent that governmental regulation is not keeping up with technological progress. This shortcoming leads to a skewed balance of power between internationally operating corporations and consumers threatened in their privacy through explosive data capture. The authors suggest that a) awareness of the implications of data processing in AI-driven (marketing) applications should be raised amongst the population, b) consent management should be revised and closely aligned with GDPR-oriented rules of privacy by design, and c) academia and policy makers should engage even more with the design of privacy-oriented legal frameworks to promote a sustainable and mutually beneficial data ecosystem.

Keywords: Privacy by Design; Consent Management; Data Protection, Artificial Intelligence

Every generation has its challenges. This was already known to our grandfathers who lived through the Second World War, or whose goal was to rebuild society after it. Today's challenges are of a different nature; they consist mainly of 1s and 0s, and encompass pretty much every area of life. Whether you are dating online, managing your finances, planning your next holiday in South Tyrol, "writing" a short essay assisted by *ChatGPT*, ordering a stand-up paddle board for your next vacation, or scouring the Instagram channel for grandma's sewing tips. All of this is possible digitally, and it has never been so convenient. It begs the question; how are and will we be paying for this newfound convenience?

In humankind's short history, there has never been such a scalable, dynamic, and imminent economic change as the digital transformation. Ubiquitous access to computing power and data has had an impact on the global economy comparable to Ford's technique of mass production in 1913. However, there is a significant difference in the time span of popularization between both milestones. Within barely 25 years, the tech giants from

Silicon Valley built an ecosystem that today has already surpassed the combined value creation of the old economic powers of oil, steel, and banking many times overⁱ.

The dominant logic inherent to the economy of standardized mass production is replaced in this new paradigm with a novel digital dishwasher's dream: any person could found a start-up that could surpass the capitalization and scale of an "analog" company in just a few years. Chasing these fittingly named "Unicorns" has become a generational dream – out with the old, in with the new. In line with this thinking, the tech giants from Silicon Valley have replaced the gatekeepers of the media houses with publicly accessible media platforms dwarfing all alternatives in reach. Everyone can share their opinion with anyone and access almost unlimited information at any time of the day. Opinion leaders have become social media influencers and banks are competing with venture capitalists and business angels. This is how the golden age of digitalization is often described in a nutshell, glancing over the societal disruption caused by it.

The implication of this new market ecosystem narrative is clear: productivity is driven by innovation and access to the new oil: data. Tech companies worldwide are investing vast sums in research and development projects for products that digitize new aspects of our lives. The resulting products undoubtedly make our lives easier: artificial intelligences and Big Data-driven data processing allow us to navigate effectively, shop more efficiently and even optimize our health. Yet, from a business perspective, every digital service also offers the opportunity to tap into new supply chain of behavioural data. Google Maps knows our movement and shopping preferences. Amazon's Alexa knows how we speak and what interests us. Facebook knows our political views and sexual orientationⁱⁱ. This personal data is in turn used to train new AIs and predict human behaviour.

What at first glance looks like a regular market exchange - data for services - is based on a highly one-sided power relationship. Large corporations and state apparatuses determine the conditions of this exchange practically unilaterally, which in the long run leads to a dangerous erosion of consumers' rights. In this, the processing and capture of data still follow an internet logic from the 1990s. Illegible data protection agreements are imposed on consumers when they buy digital services which in turn are used as proof of consent for the processing of all possible data produced in the interaction. Such exchanges often go beyond simple usage data capture for the service in question. Often, behavioural or personal data with little to no relation to the service in question is captured for future use. For example, Google Maps not only remembers the user's searched routes, but also where this

person stops. Virtual private network apps conceal their users' internet activities from website operators but could store this data for their own useⁱⁱⁱ.

This in itself is problematic - but assuming that we want to use AI to change the world around us (for example, through predictive algorithms for recidivism rates in criminals^{iv}, social credit systems to guide behaviour^v, or genomic models to calculate disease likelihood in fetuses^{vi}) we run an inherent risk of creating new power structures based on the consent-free exploitation of personal data. These structures can then be used to guide our behaviour to generate new data. Once such structures are established, it will become increasingly difficult to tear them down again.

To illustrate this effect, let's go through a fictional but theoretically possible example: A fast food chain is trying to establish itself in a small town. To do so, they distribute flyers for the restaurant app with exclusive vouchers in their neighbourhood. The offer draws in a customer who utilizes the promotional code and, best of all, pays with the company app. A link between the flyer, the person and their consumption choice has been established. This decision-making behaviour is observed across all customers and fed to a targeting algorithm. The restaurant then continuously learns how to best encourage that person to make the same decision again. To achieve this, the customer's digital environment is modified to increase the likelihood of attracting them back to the restaurant. In concrete terms, this means that the customer is repeatedly confronted with advertisements from the restaurant and is sent vouchers during their everyday internet consumption, be it the YouTube video of grandma's knitting class or sharing holiday pictures on Instagram. Based on their search history, it is possible to identify - and respond to - the emotional state or relevant search terms related to food for that person. Push messages with further food discounts are played when the person is most likely to react to them: in commuter traffic, after a long day at work, etc. The respective behaviour is not only measured but also influenced. Taken to the extreme, this means that everyday decisions are anticipated before they are made consciously. A perfect prediction of a behaviour that was triggered by said prediction.

Troubling is not necessarily the control itself, but that the only impulse the customer gave for the control in the example was a quick click on "accept" in the fast-food app, which the customer either a) did not read, or b) did not understand even when reading, as all crucial information is seamlessly embedded in a sea of general terms and conditions^{vii}.

The entire purpose of these innocent seeming clicks is to capture the willingness to pay of ever smaller customer groups while keeping them in the dark through nested cookie

conditions^{viii}. While the EU's legislation has provided a clear counter-impulse with the GDPR – the EU also reports that 97% of the largest online shops in Europe^{ix} intentionally promote this intransparency through the design of their website. The same is true for products recommendations and services based on a shared location, advertising brands spoken near an audio-recording device, or displaying the most appropriate products and services as an advertising message under searched content. *Bypassing* these business practices usually leads to an opaque “*cookie bypass tango*” that many users eventually abandon^x.

This new digital business logic is what most advertisers are basing their functionality on today^{xi}. However, if this logic is no longer only used for the pure pursuit of profit, but also spills over into crucial areas of life such as politics, health, and one's finances, a personal problem might grow into a societal crisis.

To prevent this, “*Consent Management*” must be adapted to the technical possibilities of today. It is apparent that the rigid legal system lags behind the rapid technological development deliberately exploiting their slowness^{xii}. As such, legislation on theoretical future use cases of big data algorithms need to be made today, to avoid the danger of an unwanted AI control structure that is only discovered too late. Once an such a control structure has been implemented, it is not easy to get a grip on it without also destroying related services in the ecosystem^{xiii}.

The extent of the power of individual corporations is already evident in the case of Google and Meta, which, due to their size and financial possibilities, can influence politics and legislation in many countries in advance and are actively involved in shaping the opinions of the population^{xiv}. As recently as October 2022, several members of the EU Parliament filed a lobbying complaint against Meta, Google, and Amazon for lobbying extremely aggressively in advance via an external lobby group without disclosure for the vote on the “*Digital Markets Act*”^{xv}. Numerous other reports also show how, over the course of almost a decade, large US tech companies have pursued their interests through influence strategies at the political level.^{xvi} As Zuboff, author of the “*Age of Surveillance Capitalism*”, mentioned “*It is possible to have surveillance capitalism, and it is possible to have a democracy. It is not possible to have both*”^{xvii}. Hence, it is important to set guidelines as soon as possible to bring consent-management back under democratic control.

Relying on the self-regulation of all parties involved alone cannot prevent the emergence of problematic data processing practices^{xviii}. The cooperation of all stakeholders within a data ecosystem is necessary.

Here, academia can contribute to installing control mechanisms or providing information about possible adverse effects to the general public. Science communication also plays a central role here. In the past, complex issues often could not be translated into easily understandable messages, so that essential scientific findings could not be made tangible for parts of society. Thus, scientists should be supported in processing topics such as privacy and AI in a fact-oriented and easily understandable way and making them available to the general public.

Policymakers and educational institutions must ensure that a population-wide awareness of the impact that data processing and AI-driven predictive models already have and could have in the future on our daily lives is created. Customers of data-intensive services need to understand that their interaction with this service generates data that can be used to draw far more conclusions about their lives than they might be comfortable with. Furthermore, developers and innovators are asked to confront their employers with ethical issues and cooperate in meaningful regulatory measures. Only by including customers into data value creation can business models in these future-oriented industries survive in the long term. Finally, data protection must be understood as a central design aspect, not a restriction.

Future-oriented handling of personal data must not be understood as a resource to be exploited but as a personal property to be protected. The credo of the GDPR - "*privacy by design*" - is a solid basis for future efforts. However, even this basis must be constantly adapted due to keep up with continuously evolving technological possibilities.

We need a healthy scientific dialogue to further deepen our knowledge of consumer consent management and privacy needs. We need to understand that many current digital business models make effective consumer privacy self-management impossible - or even exploit this state of affairs to maximise their profit motives. We need new technologies that can replace the Big Data combustion engine of the internet with an "emission-free" alternative. We need legislation that focuses on the consequences of data processing rather than just on data collection. We need regulations that not only react, but proactively help to shape the future, provide legal certainty, and simultaneously prevent abuse as best as possible right from the start.

In short, we need solutions to the legal, technical, ethical, and psychological problems of current data processing logic if we want to enjoy its fruits in the future without realising at some point that our decisions are no longer our own.

Bibliography

- ⁱ American Business History Center (2022). Most Valuable Companies: The Last 25 Years, online: <https://americanbusinesshistory.org/most-valuable-companies-the-last-25-years/>
- ⁱⁱ Chen, D., Fraiberger, S. P., Moakler, R., & Provost, F. (2017). Enhancing transparency and control when drawing data-driven inferences about individuals. *Big data*, 5(3), 197-212.
- ⁱⁱⁱ How to Geek (2019). Do not use Facebook's Onavo VPN: It's Designed to Spy On You, online: <https://www.howtogeek.com/342731/dont-use-facebooks-onavo-vpn-its-designed-to-spy-on-you/>
- ^{iv} Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science advances*, 4(1), eaao5580.
- ^v Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, 49(2), 187-212.
- ^{vi} Nature (2022). The controversial embryo tests that promise a better baby, online: <https://www.nature.com/articles/d41586-022-02961-9>
- ^{vii} Slepchuk, A. N., & Milne, G. R. (2020). Informing the design of better privacy policies. *Current Opinion in Psychology*, 31, 89-93.
- ^{viii} Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (pp. 1-13).
- ^{ix} European Commission (2022). Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation: final report, Publications Office of the European Union, online: <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418>
- ^x Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.*, 126, 1880.
- ^{xi} Zuboff, S. (2019, January). Surveillance capitalism and the challenge of collective action. In *New labor forum* (Vol. 28, No. 1, pp. 10-29). Sage CA: Los Angeles, CA: SAGE Publications.
- ^{xii} Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash. L. Rev.*, 89, 1-51.
- ^{xiii} See e.g. Gizmodo (2019). Life Without the Tech Giants, online: <https://gizmodo.com/life-without-the-tech-giants-1830258056>
- ^{xiv} CNBC (2018). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal, online: <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>
- ^{xv} Bloomberg (2022). US Tech Firms Hid Lobbying Efforts, European Parliament Says, online: <https://www.bloomberg.com/news/articles/2022-10-14/big-tech-firms-hid-lobbying-efforts-european-parliament-says>
- ^{xvi} The Guardian (2022). I saw first-hand how US tech giants seduced the EU - and undermined democracy, online: <https://www.theguardian.com/commentisfree/2022/jun/28/i-saw-first-hand-tech-giants-seduced-eu-google-meta>
- ^{xvii} Zuboff, S. (2022). Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization. *Organization Theory*, 3(3), 5.
- ^{xviii} Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash. L. Rev.*, 89, 1-51.