Themendossier

Social Bots

Hier finden Sie einen Video-Impuls zu Social Bots von Lena Clever (Westfälische Wilhelms-Universität Münster)
[link führt zu dem Video auf der Plattform YouTube]

Was sind Social Bots?

Bots (vom englischen „robot“) sind Computerprogramme, die automatisiert Aufgaben im Internet erfüllen. Sie werden je nach Einsatzbereich und Funktionsweise in verschiedene Typen eingeteilt. Diese sind unterschiedlich komplex: So gibt es sehr simple Programme, jedoch auch technisch stark ausgefeilte Bots. Als grundlegende Typen von Bots gelten der Webcrawler und Chatbots. Webcrawler agieren im Hintergrund und dienen der Analyse. Chatbots arbeiten reaktiv und werden daraufhin programmiert, selbstständig Chat-Unterhaltungen zu führen und Kundenanfragen zu bearbeiten. Chatbots werden in der Regel als Serviceleistung angeboten und können oft als Maschinen identifiziert werden. Bei sogenannten Social Bots ist hingegen nicht erkennbar, dass nicht mit echten Menschen interagiert wird (vgl. Ionos). Social Bots kombinieren die Technologie von Webcrawlern und Chatbots und agieren in Sozialen Netzwerken wie Twitter oder Facebook. Dort imitieren sie mit gefälschten oder gehackten Accounts echte Nutzer*innen und sollen so andere Nutzer*innen täuschen und manipulieren. Ziel der Entwickler*innen dieser Bots ist es, öffentliche Diskussionen zu manipulieren, zu blockieren oder in eine bestimmte Richtung zu lenken. Zu diesem Zweck analysieren Social Bots Inhalte in Sozialen Medien und werden automatisch aktiv, wenn sie zuvor festgelegte Themen oder Aktivitäten registrieren. Sie können dann bestimmte Inhalte liken, retweeten oder selbst Kommentare erstellen und so die Relevanz von Themen sowie Meinungen verzerren. (vgl. Bendel 2021).

Wo begegnen uns Social Bots?

Prinzipiell kann jede Person, die in sozialen Netzwerken aktiv ist, mit Social Bots in Berührung kommen. Ist der Mensch hinter einem Nutzerprofil nicht aus einem analogen Kontext bekannt, ist eine Fälschung des Accounts nicht ausgeschlossen. Social Bots teilen nicht nur Inhalte, sie versenden auch Freundschaftsanfragen. Sie versuchen so Daten der kontaktierten Personen zu sammeln. Zum eigenen Schutz ist es sinnvoll, sich Profile genau anzusehen und zu beurteilen, wie glaubhaft diese wirken. Eine Möglichkeit Fake-Profile zu entlarven ist es, ihnen kontextabhängige Fragen zu stellen. Diese können von Bots oft nicht beantwortet werden. (vgl. Mohabbat Kar & Gumz 2017). Plattformen versuchen sich vor Bots unter anderem mittels sogenannter Captchas zu schützen. Die Kurztests, bei denen beispielsweise bestimmte Bilder ausgewählt werden sollen, müssen inzwischen auf vielen Webseiten von Nutzer*innen bestanden werden. Die Tests können einfache Bots entlarven, da diese kein Abstraktionsvermögen besitzen. Je komplexer der Roboter technisch umgesetzt wurde, desto schwerer ist es jedoch, ihn zu identifizieren. Der technologische Fortschritt und die Weiterentwicklung künstlicher Intelligenzen machen die Entlarvung von Social Bots noch schwieriger (vgl. Ionos).

Social Bots als Phänomen im digitalen Raum

Social Bots sind nicht per se schadhaft, die Art und Absichten, wie sie eingesetzt werden, hängt von den Intentionen der sie programmierenden Menschen ab.
Laut dem Imperva Bad Bot Report (2022) hatten sogenannte „Bad Bots“ im Jahr 2021 27,7 Prozent Anteil am gesamten Datenverkehr auf Webseiten. Bad Bots sind eine Form von Social Bots und führen automatisiert Aufgaben mit schadhaften Absichten durch. Die Übernahme von Accounts, also die digitale Version von Identitätsdiebstahl, ist dabei der häufigste von Bots ausgeführte Angriff. Besonders die Plattform Twitter ist betroffen: Schätzungen gehen davon aus, dass neun bis 15 Prozent der aktiven Twitter-Accounts von Bots operiert werden (Varol et al. 2017). Twitter ist wegen der Kürze der Tweets für den Einsatz von Bots besonders geeignet, da sie dort auch bei geringer technischer Komplexität kaum erkannt werden. Sie sind in der Regel daraufhin programmiert, Timelines und Posts nach bestimmten Wörtern und Hashtags zu durchsuchen und automatisiert auf diese zu reagieren. Dabei können verschiedene Reaktionsmuster beobachtet werden: Sogenannte „Überlaster“ posten in sehr hohem Umfang Kommentare, um andere Meinungen in den Hintergrund zu drängen. Sie sind besonders effektiv, wenn sie in einem Netzwerk aus Bots interagieren. Auch „Trendsetter“ agieren im Team und haben es zum Ziel, bestimmten Hashtags und entsprechenden thematischen Beiträgen eine hohe Reichweite zu verschaffen. „Auto-Trolle“ klinken sich in Diskussionen ein, um einzelne Nutzer*innen abzulenken und so das ursprüngliche Gespräch zu blockieren.

Wie fordern Social Bots unsere Demokratie heraus?

Unternehmen können Social Bots einsetzen, um die Popularität eines Produkts künstlich zu verstärken. Auf ähnliche Weise ist es auch politischen Akteur*innen möglich, eigene Kampagnen voranzutreiben. Durch massenweise Tweets und Kommentare kann die Sichtbarkeit bestimmter politischer Meinungen und Themen erhöht werden. Auch politische Gegner*innen können gezielt diskreditiert sowie Desinformationen verbreitet werden. Sowohl im Vorfeld des Brexit-Votums als auch der amerikanischen Präsidentschaftswahl sollen Social Bots zum Einsatz gekommen sein (Kollanyi et al. 2016). Sie bieten zudem Randgruppen aus dem links- und rechtsextremistischen Spektrum die Möglichkeit, ihre Inhalte einer breiteren Masse zugänglich zu machen und populärer wirken zu lassen. (vgl. Ionos). Gefährlich ist dies deswegen, da Menschen aus Sorge vor sozialem Ausschluss dazu tendieren, sich der Mehrheitsmeinung anzuschließen (vgl. Sorge 2022). Diese Sorge wird von einigen Studien relativiert, die herausfanden, dass menschliche Interaktionen mit von Bots generierten Inhalten vorwiegend in bereits radikalisierten Gruppen stattfanden. Doch selbst bei geringer Interaktion mit den Bots kann das häufige Teilen von Inhalten im Zusammenhang mit Algorithmus basierten Vorschlägen für andere Nutzer*innen dazu führen, dass diese Inhalte vermehrt Nutzer*innen empfohlen werden (Pescetelli et al. 2022). Eine wichtige Rolle nehmen dabei auch die Medien und Politik ein: Da diese zunehmend auf Social-Media-Analysen für ihre Recherchen zurückgreifen, reproduzieren sie unter Umständen die bereits verzerrte Öffentlichkeit (vgl. Gumz & Mohabbat Kar 2017). Wie stark der Einfluss von Social Bots tatsächlich ist, ist jedoch umstritten. Eine Forschung zu dem Thema ist schwierig, da es methodisch nicht leicht ist, Social Bots als solche zu identifizieren. Einige Kritiker stellen deswegen das tatsächliche Ausmaß von Social Bot Accounts in Frage (vgl. Gallwitz & Kreil 2020).

Wie lassen sich Social Bots in den Lehrplänen verorten?

Als Expert*innen für ihre Lehrpläne haben Lehrer*innen den besten Einblick, welche (über-) fachlichen Kompetenzen sie im Rahmen dieser digital-demokratischen Herausforderungen fokussieren wollen und in welchen inhaltlichen Schwerpunkten sich diese Fragen verorten lassen. Wir möchten Ihnen hier exemplarisch einige thematische Anknüpfungspunkte aus den unterschiedlichen Fächern aufzeigen.

Folgende Themenfelder könnten dabei angesprochen werden:

- Mediennutzung, Medien als Informationsmittel, soziale Medien (z. B. in den Fächern Deutsch, Sachunterricht, Fremdsprachenunterricht)
- Politische Meinungsbildung, Einfluss der öffentlichen Meinung auf politische Entscheidungen, Manipulation der Meinungsbildung (z. B. im Fach Politik/Gesellschaft oder auch anhand politischer Beispiele aus anderen Ländern in den Fremdsprachen)
- Algorithmen, Programmieren von Bots (z. B. in den Fächern Mathematik oder Informatik)
- Einsatz von Bots im Marketing, Kundenbetreuung (z. B. im Fach Wirtschaft)
- Verantwortung (z. B. im Fach Ethik)
- Social Bots können im Zusammenhang mit Themen, die stark von Aktivitäten von Bots betroffen sind, aufgegriffen werden z. B. bewaffnete Konflikte, Wahlen, Extremismus

Besondere Potential für und von LdE

Kinder und Jugendliche verbringen einen erheblichen Anteil ihrer Zeit in den sozialen Medien und online-Plattformen und werden dort mit digitalen Herausforderungen auf unterschiedliche Arten und Weisen konfrontiert. Schule erreicht als gesellschaftliche Institution alle Kinder und Jugendliche abseits von Filterblasen und Echokammern und öffnet Räume, in denen sich Schüler*innen lösungsorientiert und begleitet mit digitalen Themen auseinandersetzen können. Im Sinne von LdE geht es dabei nicht nur um die kognitive Aneignung eines (digitalen) Themas, sondern vor allem um die aktive, reflektierte und handlungsgeleitete Auseinandersetzung mit diesen: indem sie Projekte entwickeln und durchführen, die auf realen Bedarfen beruhen, setzen sich Schüler*innen tiefgreifend und umfassend mit digitale-demokratischen Themen auseinander und entwickeln gemeinschaftlich und ko-kreativ Lösungsansätze. Durch den handlungsbasierten Ansatz von Lernen durch Engagement wird theoretisches Wissen zur Grundlage des Handelns im Engagement und verknüpft beide Ebenen gezielt miteinander. Wissen und Handeln bedingen und stärken sich im Prozess gegenseitig und wirken als “logische Einheit” für junge Menschen motivierend, da sie sie sich als informiert, und in ihrem Handeln als wirksam erleben, was wiederum zu einer nachhaltigen Verankerung des Wissens führt (Vansteenkiste et al. 2004).

Ideen für LdE-Projekte zum Thema Social Bots

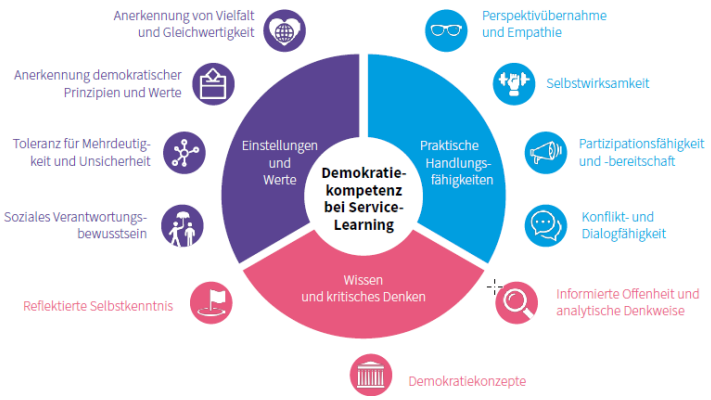
Schüler*innen setzen sich in den Naturwissenschaften mit Ursachen des Waldsterbens und Einfluss des Menschen auf Ökosysteme auseinander und analysieren in Deutsch Rhetorik rund um Klimaaktivist*innen in Medien und sozialen Netzwerken. In Zusammenarbeit mit einem Experten der Hacker School programmieren sie im Informatikunterricht einen Bot für Twitter, der – erkennbar als automatisierte Nachricht – auf die Begriffen wie „Klima-Kleber“ mit Fragen reagiert, die Mitlesende zum Nachdenken anregen sollen.

Schüler*innen suchen in Philosophie nach Antworten zu den Alleinstellungsmerkmalen des Menschen in Abgrenzung zu Tieren/Maschinen. Sie vertiefen ihr Wissen zu den Funktionsweisen und Einsatz von KI und suchen nach Beispielen, wo sie Maschinen nicht identifizieren können. Sie erarbeiten Kriterien, nach denen Social Bots erkannt werden können und entwickeln ein Spiel, bei dem Spieler*innen entscheiden, ob es sich bei einem Account in sozialen Medien um einen Bot oder einen Menschen handelt. Sie organisieren einen Workshop mit anschließender Erprobung des Spiels im Hort der benachbarten Grundschule.

Schüler*innen setzen sich in dem Fach Politik, Gesellschaft, Wirtschaft und in Deutsch mit Desinformationskampagnen im Zusammenhang mit dem Ukraine Konflikt auseinander und analysieren, wie Falschinformationen, u.a. durch den Einsatz von Bots, massenhaft verbreitet werden konnten. Sie starten eine Unterschrifts-Kampagne auf Change.org, die eine Kennzeichnungspflicht für automatisch generierte Inhalte in sozialen Netzwerken fordert.

Anregungen für Fragestellungen im Unterricht

Hier finden Sie einige Fragestellungen als Anregung, um sich im Unterricht mit dem Thema auseinanderzusetzen. Die Fragen orientieren sich an den Teilbereichen des Demokratiekompetenzmodells, dass die Stiftung Lernen durch Engagement gemeinsam mit der LMU München entwickelt hat.



Wissen und kritisches Denken

- Welche Art von Bots gibt es und wie unterscheiden sich „good“ und „bad“ Bots?
- Welche Anwendungsfelder gibt es für Bots?
- Welche Berührungspunkte – bewusst oder unbewusst – habe ich mit Social Bots gehabt? Welche Auswirkungen hat das – möglicherweise – auf meine Wahrnehmung gehabt?
- Wer setzt Social Bots ein und welche Auswirkungen können sie haben?
- Was sind typische Merkmale von Social Bots? Warum ist zunehmend schwer, Social Bots zu erkennen?
- In welchen Bereichen/Themen werden Bots häufig eingesetzt?
- Welche Vorgehensweisen können Social Bots zu großer Wahrscheinlichkeit erkenntlich machen?

Einstellung und Werte

- Sollte es eine Kennzeichnungspflicht für automatisch generierte Inhalte geben?
- Wie positionieren wir (als Klasse/als Gesellschaft) uns zu dem Einsatz von Bots? Welche Potenziale und welche Risiken gibt es?
- Unter welchen Bedingungen ist der Einsatz von Social Bots ethisch vertretbar und sogar produktiv?
- Stellt der Einsatz von Bots eine Gefahr für demokratische Prozesse dar?
- Welche Richtlinien sollte es für den Einsatz von Bots geben?
- Wer trägt die Verantwortung für den Umgang mit Bots?

Praktische Handlungsfähigkeit

- Wie können wir das Wissen zu Social Bots in unserer Umgebung erhöhen?
- Wie verhalten wir uns, wenn uns deutlich ist, dass Bots eine Diskussion antreiben/verbreiten?
- Wie können wir die Technologie für gute Zwecke in einem ethisch vertretbaren Rahmen anwenden?
- Wie können wir mit politischen Entscheidungsträger*innen zu Social Bots in einen Dialog kommen?

Video

Schnitt: Amelie Haffner

Für den Expert*innen-Impuls danken wir Lena Clever, PostDoc am Institut für Wirtschaftsinformatik der WWU Münster. Ihre Forschungsschwerpunkte liegen u.a. auf Social Media Analytics und Machine Learning.

Quellen

Bendel, O. (2021) Definition Social Bots. Gabler Wirtschaftlexikon. Online abrufbar unter https://wirtschaftslexikon.gabler.de/definition/social-bots-54247/version-384530 [05.05.2023]

BSI (Online Quelle ohne Datum). Exkurs: Social Bots und Chatbots. Online abrufbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/Exkurs-bots/social-bots.html#:~:text=Social [05.05.2023]

Clever, L. , Klapproth, J., & Frischlich, L. (2022). Automatisierte (Gegen-)Rede? Social Bots als digitales Sprachrohr ihrer Nutzer*innen. In Ernst, J., Trompeta, M., & Roth, H.-J. (Eds.), Gegenrede digital (pp. 11–26).

Clever, L. et al. (2020). Demystifying social bots: On the intelligence of automated social media actors. Social media — society, 00.

Gallwitz, F. & Kreil, M. (2020, 27. November). Die Mär von „Social Bots“ Tagesspiegel, Online abrufbar unter https://background.tagesspiegel.de/digitalisierung/die-maer-von-social-bots [05.05.2023]

Gumz, J. & Mohabbat Kar, R. (2017). Social Bots, Kompetenzzentrum Öffentliche IT. Online abrufbar unter https://www.oeffentliche-it.de/-/social-bots [05.05.2023]

Hasson, E. (2022). Evasive Bots Drive Online Fraud - 2022 Imperva Bad Bot Report, 18.05.2022 https://www.imperva.com/blog/evasive-bots-drive-online-fraud-2022-imperva-bad-bot-report/

Ionos (2022). Social Bots: Was können die Meinungsroboter wirklich?, 31.03.2022, Online abrufbar unter https://www.ionos.de/digitalguide/online-marketing/social-media/social-bots-was-koennen-die-meinungsroboter-wirklich/ [05.05.2023]

Keller, T. (2019). Social Bots: Zwischen Phänomen und Phantom, 02.05.2019, Online abrufbar unter https://www.bpb.de/themen/medien-journalismus/digitale-desinformation/290555/social-bots-zwischen-phaenomen-und-phantom/ [05.05.2023]

Kollanyi, B. et al. (2016) Bots and Automation over Twitter during the U.S. Election. Data Memo 2016.4. Oxford, UK: Project on Computational Propaganda. Online anrufbar unter http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2016/11/Data-Memo-US-Election.pdf [05.05.2023]

Varol, O. et al. (2017). Online Human-Bot Interactions: Detection, Estimation and Characterization, Proceedings of the Eleventh International AAAI Conference on Web and Social Media. Online abrufbar unter https://ojs.aaai.org/index.php/ICWSM/article/download/14871/14721 [05.05.2023]

Sorge, A. (2022). Digitaler Bundestagswahlkampf 2021: Desinformation, Microtargeting und Social-Bots - Die Integrität der Willensbildung in Gefahr. MIP 2022 (1), S. 31-53. Online abrufbar unter https://mip.pruf.hhu.de/article/view/475/494 [05.05.2023]

Pescetelli, N., Barkoczi, D. & Cebrian, M. (2022). Bots influence opinion dynamics without direct human-bot interaction: the mediating role of recommender systems. Appl Netw Sci 7, 46. Online abrufbar unter https://doi.org/10.1007/s41109-022-00488-6 [05.05.2022]

Vansteenkiste, M. (2004). Motivating Learning, Performance, and Persistence: The Synergistic Effects of Intrinsic Goal Contents and Autonomy-Supportive Contexts. Journal of Personality and Social Psychology, 87(2), 246–260. Online abrufbar unter: https://doi.org/10.1037/0022-3514.87.2.246 [31.05.2023]

IMPRESSUM

Herausgeberin

Stiftung Lernen durch Engagement – Service-Learning in Deutschland SLIDE gGmbH
Brunnenstr. 29 | 10119 Berlin
www.lernen-durch-engagement.de
www.facebook.com/StiftungLdE | www.twitter.com//StiftungLdE

Autorinnen

Leonie Mikulla, Anna-Lilja Edelstein, Yasmin Fahimi

Hinweise zum Urheberrecht und zur Nutzung der in diesem Dokument enthaltenen Inhalte

Texte

Sofern im Dokument nicht anders angegeben, stehen die Texte dieses Dokumentes unter der folgenden Lizenz: Creative Commons Namensnennung-Share Alike 4.0 International Public License, abrufbar unter https://creativecommons.org/licenses/by-sa/4.0/legalcode.de. Eine Nutzung der Texte darf nur unter Einhaltung der Lizenzbedingungen der vorgenannten Lizenz erfolgen.

Bildmaterial, Icons und Logos

Sofern im Dokument nicht jeweils ausdrücklich angegeben, stehen sämtliches Bildmaterial, Icons und Logos **nicht** unter einer Creative Commons Lizenz. Jede Nutzung von Bildmaterial, Icons und Logos bedarf der vorherigen schriftlichen Zustimmung der Stiftung Lernen durch Engagement. Bitte richten Sie Ihre Lizenzanfragen an: kommunikation@lernen-durch-engagement.de.

Dieses Material ist entstanden im Programm „Lernen durch Engagement – #netzrevolte“. Das Programm wird gefördert von der Freudenberg Stiftung.