Faites Vos Jeux

So viele Daten sind das ja nicht... oder?

Etienne Palanga

12. Juni 2022

Inhaltsverzeichnis

1 Einleitung **2**

2 Grundlagen **3**
2.1 Gesetz und Ethik 3
2.2 Privatsphäre, Sicherheit und Vertrauen 4
2.3 Datenschutz 4
2.3.1 Konsequenzen mangelnden Datenschutzes 5

3 Faites Vos Jeux **7**
3.1 AC-Games in Not 7
3.2 Das Angebot 7
3.3 Der Wert der Daten 8

4 International Data Privacy Principles **9**

5 DSGVO **9**

6 Quellen **10**

1 Einleitung

Das Thema Datenschutz wird in der heutigen Zeit von Tag zu Tag relevanter. Beispielsweise bei Verträgen, durch Bildaufnahmen an öffentlichen Orten, sowie in vielen anderen Situationen, werden Daten über Personen erhoben. Doch ist in den vergangenen Jahrzehnten ein besonders wichtiger Anwendungsbereich entstanden, den Datenschutz betrifft. Dieser Anwendungsbereich ist das Internet.

Es ist nicht nur so, dass das Internet zu diesem Zeitpunkt von fast fünf Milliarden Menschen genutzt wird.[5] Denn es werden unbeschreibliche Datenmengen von diesen Nutzerinnen und Nutzern sowohl generiert, als auch gesammelt. Aus einer Studien von Seagate aus dem Jahr 2018 geht hervor, dass zu diesem Zeitpunkt etwa 33 Zettabyte ($10^{21} Bytes$) an Daten im Umlauf waren.[8] Das bedeutet, dass diese Zahl, heute in 2022, höchstwahrscheinlich noch sehr viel größer sein wird.

Die Sammlung dieser Daten kann dabei auf verschiedene Art und Weise erfolgen. Einerseits können Daten explizit und für die Nutzerinnen und Nutzern deutlich erfolgen. Dies ist etwa der Fall, wenn ein Konto für einen Online-Shop erstellt wird, bei dem Namen, Adressen und andere Daten an Unternehmen oder Privatpersonen übergeben werden.

Darüber hinaus sind auch soziale Medien ein signifikanter Teil der Diskussion um Datenschutz. Mit schätzungsweise über viereinhalb Milliarden Gesamtnutzern und Nutzerinnen[5] ist dies ein Thema, das über 90% der Internetnutzenden betrifft. Hier werden oft Nachrichten verschickt und eigene Inhalte, darunter auch persönliche und private Inhalte, in sehr großem Ausmaß hochgeladen. Allein auf YouTube[1] wurden zum Anfangdes Jahres 2020 *pro Minute* 500 Stunden Videomaterial hochgeladen.[9]

Ebenfalls werden häufig Daten ohne das direkte Mitwissen der Nutzerinnen und Nutzer erhoben. Dies kann etwa durch Tracker auf Internetseiten geschehen, die das Verhalten der Nutzenden während des Besuchs aufzeichnen. Das kann prinzipiell bei dem Besuch jeder Website geschehen. Selbst wenn also möglicherweise ein allgemeines Verständnis bei den Nutzerinnen und Nutzer davon herrscht, dass durch den Besuch der Website Daten aufgezeichnet werden, ist es doch schwierig, möglicherweise sogar unmöglich, konkret zu wissen, welche Daten nun tatsächlich aufgezeichnet wurden.

Wie bereits angedeutet, können diese Daten verschiedenster Art sein. Insbesondere der Schutz persönlicher Daten wird für die Nutzerinnen und Nutzer von größter Wichtigkeit sein. Da Diese ebenfalls, wie zuvor beschrieben, entweder ausdrücklich oder im Hintergrund gesammelt werden, ist es nun wichtig, dass diese Daten auch angemessen geschützt werden.

Dazu müssen wir uns erst mit den Aufgaben befassen, die Datenschutz betreffen, sowie den Folgen, sollte Datenschutz nicht eingehalten worden sein. Wir betrachten hierzu das Paper von Lee et al. „An Ethical Approach to Data Privacy Protection“.[6]

[1] `https://www.youtube.com/`

2 Grundlagen

Zunächst wollen wir uns mit dem Zusammenhang von Gesetz und Ethik, sowie mit Datenschutz auseinandersetzen. Ersteres ist wichtig für die spätere Evaluation des Fallbeispiels, während Letzteres das Fundament für die Diskussion der Hauptthematik des Fallbeispiels bildet.

2.1 Gesetz und Ethik

So wie Privatsphäre, Sicherheit und Vertrauen verwandt sind, so sind es auch Ethik und das Gesetz. Auf der einen Seite bietet das Gesetz einem ethischen Prinzip die Möglichkeit, das Prinzip tatsächlich in der Gesellschaft durchzusetzen.[6]

Beispielsweise kann man aufgrund eines individuellen ethischen Verständnisses zu dem Schluss kommen, dass stehlen falsch ist. Es ist natürlich auch so, dass die meisten Menschen dieses Verständnis im Allgemeinen teilen. Allerdings ist das allein nicht genug, damit dieses Verständnis in der Gesellschaft auch durchgesetzt werden kann. Denn einerseits kann es Menschen geben, die zwar dieses gleiche Verständnis besitzen, dies aber brechen. Andererseits kann es auch sein, dass Menschen dieses Verständnis nicht teilen und aus diesem Grund stehlen. Das Gesetz kann nun durch den Staat dieses Verständnis umsetzen, indem die, die dieses Gesetz – und damit das ethische Prinzip – brechen, strafrechtlich verfolgt werden können.

Abbildung 1: Wechselwirkung von Gesetz und Ethik.

Auf der anderen Seite bietet Ethik Kontext für bestehende Gesetze. Ein Beispiel hierfür ist etwa das Auslagern von Arbeitsplätzen in ein Niedriglohnland. Dies ist zwar hierzulande legal, allerdings lässt es sich streiten, ob dies ethisch korrekt ist.

Zudem existieren unbestimmte Rechtsbegriffe, wie hierzulande beispielsweise „Treu und Glauben“ (zum Beispiel § 242 BGB). Dieser sagt aus, dass man sich um dem jeweiligen Gesetz zu entsprechen „anständig und redlich verhalten“ habe.[1] Wenn also festgestellt werden soll, ob eine Person entsprechend „Treu und Glauben“ gehandelt hat, können durchaus auch ethische Überzeugungen mit einfließen.

Diese Wechselwirkung ist in Abbildung 1 visualisiert.

Wie bereits in diesem Beispiel angedeutet, können Gesetze auch oft aus ethischen Überzeugungen entstehen. Daher kann es bei der Evaluation ethischer Vertretbarkeit einer Handlung auch von Nutzen sein, die gesetzliche Lage zu

betrachten, sollten die zugrundeliegenden ethischen Überzeugungen erkennbar sein.

2.2 Privatsphäre, Sicherheit und Vertrauen

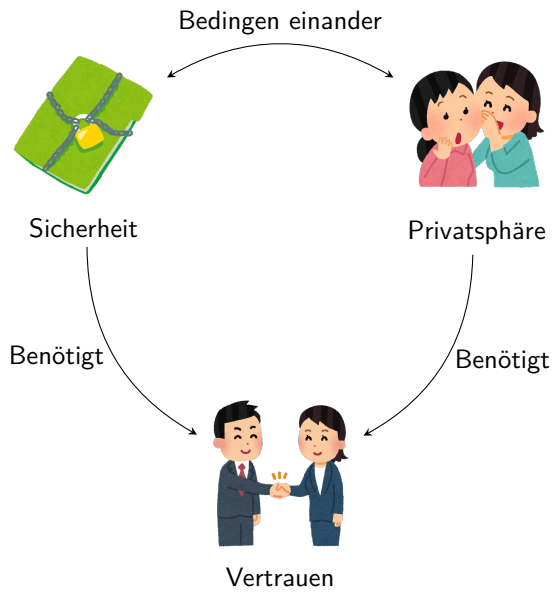

Abbildung 2: Wechselwirkungen von Sicherheit, Privatsphäre und Vertrauen.

Ebenfalls beschreiben Lee et al., dass die Gewährleistung von Privatsphäre und Sicherheit eng mit dem Vertrauen in Dritte auch eine Wechselwirkung haben.[6] Soll die Privatsphäre einer Person geschützt, oder die Sicherheit einer Person garantiert werden, insbesondere durch Dritte, so muss Vertrauen in diese Dritten herrschen.

In beiden Fällen muss den Dritten Zugang zu dem privaten Bereich der Person gegeben werden. Soll im Fall von Privatsphäre beispielsweise eine andere Person das eigene Tagebuch verwahren, so muss das Vertrauen in diese andere Person herrschen, dass diese nicht selbst unerlaubt in dem Tagebuch liest. Im Allgemeinen muss man Anderen vertrauen können, sollte man diesen Zugriff auf einen privaten Bereich geben.

Im Falle Sicherheit muss beispielsweise ein Bodyguard in der Nähe der zu schützenden Person bleiben. Dabei muss natürlich das Vertrauen herrschen, dass der Bodyguard selbst keine schlechten Absichten hat. Allgemeiner, muss einem „Anbieter“ von Sicherheit vertraut werden, dass dieser seine Arbeit gut und gewissenhaft tut.

Diese Zusammenhänge sind in Abbildung 2 visualisiert.

Diese Aspekte finden sich im Datenschutz ebenfalls wieder.

2.3 Datenschutz

Datenschutz befasst sich mit dem Umgang mit den privaten Daten eines Subjekts. Dazu zählt etwa wie auf diese zugegriffen werden darf, wie sie gesammelt werden dürfen oder von einer dritten Partei genutzt werden dürfen. Besondere Wichtigkeit haben hier die Rechte, die das Subjekt selbst an ihren eigenen Daten hat. Die Hauptaspekte lassen sich folgendermaßen zusammenfassen:[6]

Eine Instanz, die Daten Anderer verwaltet und Datenschutz betreibt, muss folgendes gewährleisten:

- Schutz vor unauthorisiertem Zugriff
- Sicherstellen angemessener Benutzung der Daten
- Richtigkeit und Vollständigkeit gesammelter Daten über Personen oder Firmen
- Verfügbarkeit der Daten für das Subjekt und das Recht des Subjekts die Daten zu besitzen
- Das Recht des Subjekts, die Daten zu inspizieren, zu aktualisieren oder zu korrigieren

Solange die Daten allein in der Hand ihres Eigentümers oder Eigentümerin sind, ist kein Datenschutz vonnöten, da es hier unstrittig ist, ob auf die Daten zugegriffen werden darf oder ob sie verwendet werden dürfen. Wir befassen uns also damit, was gelten soll, wenn die Daten in die Hände Anderer übergeben werden.

Wie wir bereits gesehen haben, hängen Privatsphäre, Sicherheit und Vertrauen zusammen. Dies ist auch bei Datenschutz nicht anders. Denn all diese drei Aspekte sind für Datenschutz nötig. Durch den Schutz der privaten Daten des Subjekts wird dessen *Privatsphäre* gewahrt. Darüber hinaus muss die Daten schützende Instanz, die Daten in Hinblick auf die oben genannten Aspekte *absichern*. Die Instanz, die dies durchführt, benötigt das *Vertrauen* dies gewissenhaft durchzuführen.

2.3.1 Konsequenzen mangelnden Datenschutzes

Natürlich ist Datenschutz aus dem Grund nötig, dass das Nicht-Schützen von Daten negative Konsequenzen mit sich zieht. Dementsprechend muss sich Datenschutz auch mit diesen befassen, damit solche negativen Konsequenzen nach Möglichkeit vermieden oder zumindest vermindert werden können. Nach Lee et al. lassen sich diese Konsequenzen in sogenannte *Soft Costs* und *Hard Costs* aufteilen. [6]

Dabei handelt es sich bei Hard Costs um materielle Konsequenzen, wie finanzielle oder durch strafrechtliche Verfolgung entstehende Kosten.

Soft Costs sind dabei andere Konsequenzen, wie zum Beispiel der Verlust des Vertrauens der Kunden oder der Verlust eines guten Rufs.

Facebook Datenleck 2021 Ein Beispiel für solche negativen Konsequenzen ist ein Datenleck bei Facebook[2], der im Jahr 2021 entdeckt wurde.[3] Hier wurden in 2021 die Daten von über *533 Millionen* Nutzern und Nutzerinnen veröffentlicht. Diese Daten beinhalten die Facebook IDs, Namen, Wohnorte, Geburtsdaten und weitere private Daten. Nach Aussage von Facebook konnten die Daten aufgrund einer Sicherheitslücke in 2019 von Facebook erhoben werden.[2]

[2] `https://www.facebook.com/`

Die Veröffentlichung solcher Datensätze kann Identitätsdiebstahl vereinfachen. Böswillige Parteien können mithilfe dieser Daten andere Personen imitieren um so potentiell an weitere persönliche Daten zu gelangen.

Zu diesem Vorfall sagte Alon Gal, der technische Direktor des Cyberkriminalität-Intelligenz-Unternehmens Hudson Rock[3] (übersetzt):

> Individuen, die sich bei einem reputablen Unternehmen wie Facebook registrieren, vertrauen ihnen mit ihren Daten und Facebook sollte mit den Daten mit höchstem Respekt umgehen. [...] Dass die persönlichen Daten von Nutzern geleakt wurden, ist ein riesiger Vertrauensbruch und sollte auch so behandelt werden. ([3])

Auch aus diesem Zitat sehen wir, dass die Themen Vertrauen, Privatsphäre und Sicherheit sehr große Bedeutung für Datenschutz haben.

Obwohl die genaue Wahrnehmung von Privatsphäre sich etwas von Kultur zu Kultur unterscheiden mag, gibt es einen groben Konsens, dass Privatsphäre ein wichtiges, sozial vorteilhaftes Gut ist.[6]

[3] `https://www.hudsonrock.com/`

3 Faites Vos Jeux

Zum Thema Datenschutz betrachten wir nun das Fallbeispiel „Faites Vos Jeux“[4] aus dem Informatik Spektrum 2017.

3.1 AC-Games in Not

Walter ist seit nun fast 2 Jahrzehnten Geschäftsführer einer kleinen Spielfirma namens AC-Games, die ein kostenloses Spieleportal für Online-Spiele betreibt. (siehe Abbildung 3) Lange Zeit lief das Geschäft gut, die Firma hatte einen gesunden Stamm von Nutzern und Nutzerinnen. Die Einnahmen setzten sich aus Käufen virtueller Gegenstände, sowie Werbeeinnahmen zusammen. Allein durch die 100 meist-zahlenden Nutzern und Nutzerinnen konnte AC-Games seine Kosten decken.

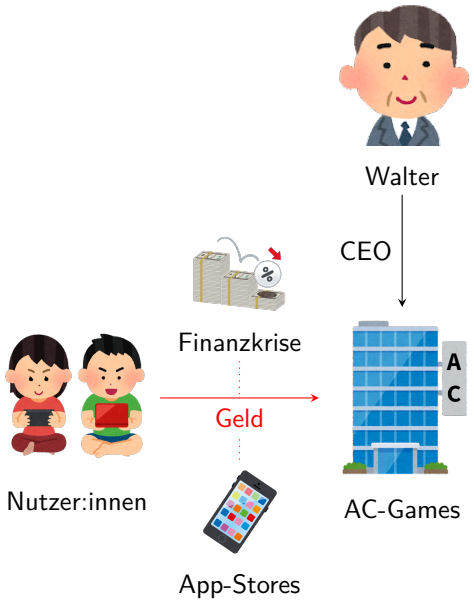

Abbildung 3: Die Situation von AC-Games.

Doch dann begann vor etwa 10 Jahren die Wirtschaftskrise. Seitdem ging es mit AC-Games langsam bergab. Dies war allerdings nicht allein der Wirtschaftskrise geschuldet. Weitere Entwicklungen über die letzten 10 Jahre wirkten sich ebenfalls negativ auf AC-Games aus.

Beispielsweise wurden durch die Ausbreitung von Smartphones auch die damit einhergehenden App-Stores zum Problem für AC-Games. Vor allem für Gelegenheitsspieler eignen sich Spiele aus solchen App-Stores und löst damit einen wichtigen Teil von Spieleportalen ab. Darüber hinaus führte die Popularität von App-Stores dazu, dass Spielentwickler weniger dazu geneigt waren, Spiele für Spieleportale zu entwickeln, im Vergleich zu App-Stores. Darüber hinaus sanken auch sowohl die Werbeeinnahmen, sowie die Zahl der Käufe virtueller Gegenstände und seit etwa 2-3 Jahren hat AC-Games Schwierigkeiten die eigenen Mitarbeiter und Mitarbeiterinnen zu bezahlen.

3.2 Das Angebot

Zu diesem Zeitpunkt bekommt Walter ein Angebot: Ein Datenhändler namens *Data Broker GmbH* möchte die Firma übernehmen und bietet eine sehr große Geldsumme. Die hohe Geldsumme verwunderte die Mitglieder von AC-Games, doch nach einer Diskussion entschließt sich Walter, die Firma an Data Broker zu übergeben. Der Hauptgrund für diese Entscheidung, ist Walters Ansicht, dass AC-Games nur für Transaktionen nötige Daten speichert. Es sei unproblematisch, diese Daten an Data Broker zu übergeben.

Doch tatsächlich speicherte AC-Games mehr Daten als von Walter angenommen. Hierzu müssen wir an den Anfang von AC-Games zurückgehen. Zu dieser Zeit war es Walter und seinen Mitgründern nicht sehr wichtig, auf Datenschutz zu achten.

In einem alten Blogpost stellt Walter seine Gedanken über eine sogenannte *ultimative Slot-Machine* dar. Diese soll ein Glücksspiel sein, das sich den Spielern und Spielerinnen anpasst. Dazu müssten natürlich Verhaltensdaten gesammelt werden. Darüber hinaus wurden weiter Überlegungen angestellt, wozu solche Daten noch dienen könnten. Dies wurde aber ausschließlich intern besprochen. Beispielsweise könne man Spielern künstlichem Stress aussetzen, um ihr Entscheidungsverhalten zu ihren Ungunsten zu beeinflussen. Diese Ideen wurden allerdings wieder verworfen, inklusive der ultimativen Slot-Machine.

Allerdings wurden die angesprochenen Verhaltensdaten tatsächlich von AC-Games gesammelt und auch bis heute gespeichert. Eine Mitarbeiterin namens Kathleen war die einzige, die einen Überblick darüber hatte, welche Daten nun tatsächlich gesammelt und gespeichert wurden. Doch konnte sie mangels Ressourcen die Systeme nicht umprogrammieren, um die Datensammlung zu beenden.

Es wurde auch in einem Datenschutzaudit angemerkt, dass die Menge der gesammelten Daten eigenartig sei. Allerdings wurde diesbezüglich nichts unternommen, da dies rechtlich legitim schien und die Nutzer und Nutzerinnen in AGB eingewilligt haben, die diese Datensammlung erlauben.

Tatsächlich hat dieser Datenschutzaudit Data Broker erst auf AC-Games aufmerksam gemacht, da dieser öffentlich zugänglich war. Im Idealfall für Data Broker müssten auch nicht die AGB geändert werden, sodass die Übernahme sogar ohne das Mitwissen der Nutzer und Nutzerinnen geschehen kann.

3.3 Der Wert der Daten

Typ	**Nutzer**		
Stress	Bob L.	Lina M.	...
Neugier	Katie A.	Chris O.	...
⋮	...		

Tabelle 1: Hanks Kategorisierung der Nutzer und Nutzerinnen.

Hank ist ein neuer Mitarbeiter bei AC-Games und der Datenbankadmin. Auch er weiß von der Übernahme durch Data Broker und ist über die hohe Geldsumme verwundert. Er schließt dadurch, dass die Daten von AC-Games nicht wertlos sind. Da er von Walters alten Blog—Posts weiß und er nicht die Absicht hat, lange bei AC-Games zu bleiben, ist er bereit etwas zu experimentieren.

Er stellt Berechnungen auf den Daten an und kategorisiert so die Nutzer und Nutzerinnen in verschiedene Gruppen. (siehe Tabelle 1) Mithilfe dieser Daten fügt er dem In-Game Shop ein neues Element hinzu. Er fügt einen Zähler hinzu, der die verbleibende Anzahl jedes Produkts darstellen soll. Die angezeigte Zahl ist aber unecht.

Er passt die genaue Darstellung dieses Zählers auf die Nutzer und Nutzerinnen der Kategorien an, die er mithilfe der Berechnungen erstellt hat. So wird

für „Stress-Typen“ der Zähler zu Anfang auf eine zweistellige Zahl gesetzt und diese Zahl langsam dekrementiert. Bei „Neugier-Typen“ hingegen wird stattdessen ein „Vorrat prüfen“-Knopf angezeigt. Wird dieser geklickt, wird ein Fenster mit dem Text „Nur noch ein Exemplar verfügbar!“ angezeigt.

Am nächsten Tag prüft Hank die Verkaufszahlen und bemerkt, dass sich diese signifikant erhöht haben. Er fragt sich, was noch mit diesen Daten angestellt werden könnte und überlegt, was er in dieser Situation tun sollte. Er hat zwar Anweisungen bekommen, nicht tief in die Datenbank einzugreifen, doch spielt er mit dem Gedanken, entgegen dieser Anweisungen zu handeln.

4 International Data Privacy Principles

5 DSGVO

6 Quellen

Alle verwendeten Illustrationen stammen von Irasutoya.[7]

[1] Lennart Alexy u. a. *Treu und Glauben*. In: *Das Rechtslexikon. Begriffe, Grundlagen, Zusammenhänge*. 1. Aufl. J.H.W. Dietz Nachf., Sep. 2019. URL: https://www.bpb.de/kurz-knapp/lexika/recht-a-z/324163/treu-und-glauben/ (besucht am 09. 06. 2022).

[2] Mark Clark. *The Facts on News Reports About Facebook Data*. Meta. 6. Apr. 2021. URL: https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/ (besucht am 09. 06. 2022).

[3] Aaron Holmes. *533 million Facebook users' phone numbers and personal data have been leaked online*. Business Insider. 3. Apr. 2021. URL: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 (besucht am 09. 06. 2022).

[4] Benjamin Kees und Stefan Ullrich. „Faites Vos Jeux". In: *Informatik-Spektrum* 40.5 (1. Okt. 2017), S. 466–491. ISSN: 1432-122X. DOI: 10.1007/s00287-017-1065-y. URL: https://doi.org/10.1007/s00287-017-1065-y (besucht am 26. 05. 2022).

[5] Simon Kemp. *Digital 2022: Global Overview Report*. DataReportal – Global Digital Insights. 26. Jan. 2022. URL: https://datareportal.com/reports/digital-2022-global-overview-report (besucht am 08. 06. 2022).

[6] Wanbil W. Lee, Wolfgang Zankl und Henry Chang. „An Ethical Approach to Data Privacy Protection". In: *ISACA Journal* 6.2016 (24. Dez. 2016).

[7] Takashi Mifune. *Irasutoya*. Irasutoya. URL: https://www.irasutoya.com/ (besucht am 08. 06. 2022).

[8] David Reinsel, John Gantz und John Rydning. „The Digitization of the World from Edge to Core". In: (2018), S. 28. URL: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (besucht am 08. 06. 2022).

[9] Susan Wojcicki. *YouTube at 15: My personal journey and the road ahead*. blog.youtube. 14. Feb. 2020. URL: https://blog.youtube/news-and-events/youtube-at-15-my-personal-journey/ (besucht am 08. 06. 2022).