

Seminararbeit

Vorratsdatenspeicherung und informationelle Selbstbestimmung am Beispiel von Spusu, einem Schweizer Mobilfunkanbieter

eingereicht von:

Nils Schmid

Email: nilsfabian.schmid@uzh.ch

Stud.-Nr. 24-700-502

Seminar:

«Vorratsdatenspeicherung – Hintergründe und aktuelle Debatten»

FS26

Modulnummer: 254o104a

Betreuerin:

Alena Birrer

Institut für Kommunikationswissenschaft und Medienforschung (IKMZ) der Universität Zürich

Zürich, 26. Juni 2026

Inhaltsverzeichnis

<u>EINLEITUNG</u>	<u>1</u>
<u>THEORETISCHER RAHMEN.....</u>	<u>2</u>
INFORMATIONELLE SELBSTBESTIMMUNG	2
URSPRUNG UND DEFINITION.....	2
METADATEN UND IHRE AUSSAGEKRAFT	3
RECHTLICHER KONTEXT.....	4
BÜPF UND VORRATSDATENSPEICHERUNG IN DER SCHWEIZ	4
AUSKUNFTSRECHT (ART. 25 DSGVO).....	5
<u>FALLANALYSE: EIGENE VORRATSDATEN VON SPUSU</u>	<u>6</u>
DIE DATEN	6
ANALYSE	6
TAGESRHYTHMUS	7
SOZIALE KONTAKTE.....	9
MOBILITÄT.....	10
GRENZEN DER ANALYSE	10
<u>DISKUSSION: FOLGEN DER VDS FÜR INFORMATIONELLE SELBSTBESTIMMUNG ..</u>	<u>11</u>
<u>FAZIT.....</u>	<u>13</u>
<u>ANHANG</u>	<u>15</u>
LITERATURVERZEICHNIS	15
DATENSATZ UND PYTHON-SKRIPTS	16
LAUTERKEITSERKLÄRUNG UND VERWENDUNG VON KI.....	17

Abbildungsverzeichnis

Abbildung 1: Beispiel einer CSV-Datei.....	6
Abbildung 2: Aktivität nach Uhrzeit.....	7
Abbildung 3: Aktivität nach Wochentag.....	8
Abbildung 4: Kontakthäufigkeit	9

Tabellenverzeichnis

Tabelle 1: Orte der Nutzung	10
-----------------------------------	----

Einleitung

Ob man eine Kurznachricht verschickt, ein Telefonat führt oder etwas mit dem Handy im Internet nachschaut, es entstehen so gut wie immer digitale Spuren. Anbieter von Schweizer Fernmeldediensten sind gesetzlich dazu verpflichtet, diese sogenannten Randdaten für sechs Monate aufzubewahren (BÜPF, SR 780.1). Es werden dabei nicht die Inhalte einer Kommunikation, sondern deren Metadaten gespeichert. Metadaten sind zum Beispiel Angaben darüber, wer mit wem, wann, für welche Dauer und von wo aus telefoniert. In der öffentlichen Debatte werden solche Aufzeichnungen häufig als bloss technische Verbindungsdaten abgetan und ihre Speicherung als wenig eingriffsintensiv verharmlost.

Ob Randdaten in der Realität nur wenig Aussagekraft haben, ist allerdings fraglich. Forschungsarbeiten wie jene von Mayer et al. (2016) zeigen, dass man allein aus Verbindungsdaten weitreichende Schlüsse über das Privatleben einer Person ziehen kann. So lassen sich Rückschlüsse auf soziale Beziehungen, Aufenthaltsorte und teilweise sogar auf sensible persönliche Merkmale ziehen. Hier rückt eine Frage in den Vordergrund. Wenn anlasslos gespeicherte Metadaten derartige Merkmale einer Person preisgeben, was bedeutet ihre Speicherung dann für das Recht, selbst über die Preisgabe und Verwendung der eigenen Daten zu bestimmen? Was bedeutet es also für die informationelle Selbstbestimmung?

Die vorliegende Arbeit beschäftigt sich mit der Frage: Welche Rückschlüsse lassen sich auf das Alltagsverhalten von Personen anhand von Vorratsdaten ziehen, welche von Schweizer Mobilfunkanbietern gespeichert werden?

Zur Beantwortung dieser Frage wird eine Einzelfallanalyse gemacht. Den empirischen Kern bilden die eigenen Vorratsdaten des Autors, die dieser mit Hilfe des datenschutzrechtlichen Auskunftsrechts von seinem Mobilfunkanbieter Spusu bezogen hat. Danach wird der Datensatz untersucht. Im Zentrum der Untersuchung steht: Welche Informationen über Tagesrhythmus, Mobilität und soziale Kontakte sich aus den gespeicherten Metadaten erschliessen lassen. Es handelt sich hierbei um einen Einzelfall. Die Analyse stützt sich auf Daten einer Einzelperson. Sie erlaubt also keine verallgemeinernden Aussagen. Das Ausmass der Aussagekraft solcher Daten kann aber dennoch gut veranschaulicht werden.

Die Arbeit ist wie folgt aufgebaut: Im nächsten Kapitel wird der theoretische Rahmen entwickelt. Das Recht auf informationelle Selbstbestimmung wird hergeleitet und die Aussagekraft von Metadaten wird anhand des Forschungsstandes dargelegt. Das darauffolgende Kapitel ist eine rechtliche Einordnung der Vorratsdatenspeicherung. Es behandelt sowohl das BÜPF als auch das Auskunftsrecht nach Art. 25 DSG. Danach wird die Fallanalyse durchgeführt, mit den eigenen Daten von Spusu. Es werden auch ihre Grenzen aufgezeigt. Das letzte Kapitel behandelt die empirischen Befunde, die mit dem theoretischen und rechtlichen Rahmen zusammengeführt werden und die Folgen für die informationelle Selbstbestimmung diskutiert. Zum Schluss werden im Fazit die Ergebnisse gebündelt und eingeordnet.

Theoretischer Rahmen

Hinterlässt man beim Telefonieren Spuren, wird man lesbar. Um zu verstehen, wie aus isolierten Einzeldaten ein konkretes Bild eines Menschen entstehen kann, bedarf es theoretischen Hintergrundwissens. Dieses setzt sich aus zwei Perspektiven zusammen, die sich ergänzen: einer rechtlich-philosophischen und einer empirischen. Erst wird aufgezeigt, wie sich der Schutz der eigenen Daten als Basis für die persönliche Freiheit überhaupt historisch und normativ begründen lässt. Danach wird der Blick auf den aktuellen Forschungsstand gelegt. Es wird darauf eingegangen, warum die Trennlinie zwischen harmlosen Randdaten und dem eigentlichen Gesprächsinhalt in der Realität eher dünn ist.

Informationelle Selbstbestimmung

Ursprung und Definition

Das Recht auf informationelle Selbstbestimmung geht auf das Volkszählungsurteil vom 15. Dezember 1983 des deutschen Bundesverfassungsgerichts zurück (BVerfG, 1983). Es wurde durch ein Volkszählungsgesetz veranlasst, welches eine umfassende Erhebung personenbezogener Daten vorsah und unter anderem den Abgleich eben dieser Daten mit den Melderegistern erlaubte. Aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) leitete das Gericht ein eigenständiges Grundrecht ab. Es wird so definiert, dass jeder Einzelne die Befugnis hat, "grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" (BVerfG, 1983, Rn. 147).

Tragend für diese Begründung war, dass sich die technischen Bedingungen für die Verbreitung von Daten grundsätzlich verändert haben. Personenbezogene Daten lassen sich technisch unbegrenzt speichern, von jedem Ort der Welt aus abrufen und mit weiteren Datensammlungen zu einem persönlichen Profil zusammenfügen. Die betroffene Person hat dabei keine Kontrolle darüber, was mit ihren Daten geschieht, noch weiss sie unter Umständen, dass es überhaupt geschieht. Daraus zog das Gericht eine zentrale Folgerung: Unter der Bedingung der automatischen Datenverbreitung gebe es "kein 'belangloses' Datum mehr" (BVerfG, 1983, Rn. 150). Die Sensibilität, welche ein Datum hat, werde nicht daran gemessen, was allein dessen Inhalt ist, sondern vielmehr an Zweck, Verknüpfungs- und Verwendungsmöglichkeiten, in deren Zusammenhang es steht.

Der Schutz wird vom Gericht nicht nur individualrechtlich, sondern auch demokratietheoretisch begründet. Rechnet man damit, dass das, was man macht, gespeichert wird, verhält man sich anders. So eine Beeinträchtigung verändert nicht nur die Entfaltung des Einzelnen, sondern auch das Allgemeinwesen, da Selbstbestimmung eine "elementare Funktionsbedingung" einer freiheitlich demokratischen Ordnung sei (BVerfG, 1983, Rn. 146). Damit dient es nicht zum Selbstzweck, Kontrolle über die eigenen Daten zu haben, sondern ist die Voraussetzung für eine freie Kommunikation Einzelner. Es gibt ihnen die Möglichkeit, sich uneingeschränkt am gesellschaftlichen Leben zu beteiligen. Gleichzeitig stellt das Gericht klar, dass das Recht nicht schrankenlos gilt. Einschränkungen können gemacht werden, wenn ein überwiegendes allgemeines Interesse besteht. Diese Einschränkungen bedürfen aber einer gesetzlichen Grundlage, welche dem Gebot der Normenklarheit genügt und müssen verhältnismässig sein (BVerfG, 1983, Rn. 148–149).

Während das Volkszählungsurteil das Recht rechtsdogmatisch fasst, wird in Rössler (2001) dessen normative Begründung geliefert. In *Der Wert des Privaten* werden drei Dimensionen von Privatheit unterschieden. Eine dezisionale, informationelle und eine lokale Privatheit. Informationelle Privatheit wird so verstanden, dass man die Kontrolle darüber hat, was andere über eine Person wissen. Privatheit ist dabei die Bedingung individueller Autonomie und wird nicht als Selbstzweck verstanden. Nur wenn man einschätzen kann, was andere über einen wissen, kann man sein Handeln selbstbestimmt gestalten. Es gibt zur juristischen Definition also auch eine philosophische Perspektive, die erklärt, weshalb der Verlust an Datenkontrolle die Freiheit der Person trifft.

Da das Konzept seine Ursprünge im deutschen Verfassungsrecht hat, ist nun zu klären, wie es in das Schweizer Recht überführt wurde. Der Schutz vor Missbrauch persönlicher Daten ist in der Schweiz in Art. 13 Abs. 2 BV festgehalten. Darunter wird vom Bundesgericht auch der Anspruch auf informationelle Selbstbestimmung verstanden. Dies wird unter anderem im hier behandelten Urteil zur Vorratsdatenspeicherung festgehalten (BGE 144 I 126, E. 4).

Metadaten und ihre Aussagekraft

Im Kommunikationsrecht wird zwischen Inhalt einer Kommunikation und deren begleitenden Metadaten unterschieden. Metadaten sind beispielsweise Angaben darüber, wer mit wem, wann, wie lange und von wo aus kommuniziert. Während der Inhalt einer Kommunikation einem eher strengeren Schutz unterliegt, werden Metadaten als weniger sensibel angesehen und daher weniger geschützt (Mayer et al., 2016). Diese Unterscheidung ist auch die Grundlage der Vorratsdatenspeicherung, welche nicht die Inhalte eines Gesprächs, sondern dessen Randdaten des Fernmeldeverkehrs aufzeichnet. In der öffentlichen Debatte werden diese Aufzeichnungen häufig als blosse technische Verbindungsdaten verharmlost. Ob diese Einschätzung tatsächlich die Aussagekraft von Metadaten beschreibt, ist fraglich.

Mayer et al. (2016) beschäftigen sich eingehender mit dieser Frage. Die Autoren sammelten mithilfe einer Android-Anwendung die Telefonmetadaten von 823 Freiwilligen. Insgesamt handelte es sich um 251'788 Anrufe und 1'234'231 Kurznachrichten. Diese Daten wurden anschliessend mit den Facebook-Profilen der Teilnehmenden verknüpft, welche als Vergleichsgrundlage für die Überprüfung der gezogenen Rückschlüsse dienten. Danach wurde untersucht, welche Informationen sich allein aus den Verbindungsdaten einer einzelnen Person herleiten lassen.

Die Ergebnisse des Experiments widersprachen der Annahme, dass Metadaten harmlos seien, klar. Schon die Zuordnung der Telefonnummern zu konkreten Personen konnte mit geringem Aufwand gemacht werden. Rund ein Drittel der Nummern konnten durch automatisierte Verfahren identifiziert werden. Mit zusätzlicher manueller Recherche konnte eine Trefferquote von über vier Fünfteln erreicht werden (Mayer et al., 2016). Auch der Wohnort konnte bei einem Teil der Teilnehmenden mit einer Genauigkeit von 57% nur durch das Anrufverhalten bestimmt werden. Über die einzelnen Personen hinaus konnten soziale Beziehungen erfolgreich zugeordnet werden. In manchen Fällen war sogar erkennbar, wer, zum Zeitpunkt der Datenspeicherung, mit wem in einer Beziehung war. Am schwersten wiegt für diese Arbeit aber ein anderer Befund: Die Metadaten geben sensible persönliche Merkmale preis. So konnten von einem erheblichen Teil der Teilnehmenden Kontakte zu sensiblen Organisationen wie

Finanzdienstleistern oder dem Gesundheitswesen festgestellt werden. Einzelne Anrufmuster halfen, Hinweise auf Erkrankungen, Waffenbesitz oder reproduktive Entscheidungen zu gewinnen (Mayer et al., 2016).

Von Mayer et al. (2016) wird daraus der Schluss gezogen, dass dicht vernetzte Telefonmetadaten leicht re-identifizierbar sind und so ohne grossen Aufwand Rückschlüsse auf sensible Eigenschaften, Beziehungen und Aufenthaltsorte zulassen. Deshalb ist die Geringschätzung von Metadaten im Recht und in der Gesellschaft empirisch nicht haltbar. Auch ohne in Kenntnis der Kommunikationsinhalte zu sein, entsteht ein aussagekräftiges Bild einer Person. Die Autoren räumen ein, dass ihre Stichprobe nicht repräsentativ ist, halten die auftretenden Muster aber für übertragbar.

Dieser Forschungsstand wird von Birrer et al. (2023) bestätigt. Metadaten seien nicht weniger, sondern anders invasiv als Inhalte. Kombiniert man verschiedene Metadaten, so lassen sich Gesundheitsmerkmale, politische Einstellung oder sexuelle Orientierung ableiten. Eine strikte Trennung von Metadaten und Inhalten gilt daher zunehmend als überholt.

Die Befunde dieser Studien bilden die theoretische Grundlage für die vorliegende Arbeit. Wenn schon eine begrenzte Menge an Metadaten solche Rückschlüsse ziehen lässt, sollte man sich fragen, welches Bild man erstellen kann, wenn man Zugriff auf die über mehrere Monate gespeicherten Vorratsdaten eines einzelnen Mobilfunkanschlusses hat. Gleichzeitig verbindet sich hier die Aussagekraft der Metadaten mit dem im vorherigen Kapitel entwickelten Recht auf informationelle Selbstbestimmung. Wenn ein anlasslos gespeicherter Datensatz Dinge über eine Person preisgibt, dann wird in deren Recht eingegriffen. Sie kann nicht mehr selbst über die Verwendung der eigenen Daten bestimmen.

Rechtlicher Kontext

BÜPF und Vorratsdatenspeicherung in der Schweiz

Für eine rechtliche Grundlage der Vorratsdatenspeicherung sorgt in der Schweiz das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1). Durch dieses Gesetz werden die Anbieter von Fernmeldediensten dazu verpflichtet, Randdaten des Fernmeldeverkehrs ihrer Kunden für sechs Monate zu speichern (Art. 26 Abs. 5 BÜPF). Es werden also nicht die Kommunikationsinhalte gespeichert, sondern nur Metadaten. Die Speicherung wird anlasslos vorgenommen, das heisst, es besteht kein konkreter Verdacht und sie erfolgt bei allen Nutzern. Nur klassische Fernmeldeanbieter sind von der vollen Speicherpflicht betroffen. Abgeleitete Kommunikationsdienste wie Messenger- oder E-Mail-Dienste haben eine reduzierte Pflicht und müssen Daten nicht auf Vorrat speichern.

Ein Gericht überprüfte, ob die Speicherung der Daten verfassungsmässig ist. Eine Beschwerde, die von der Digitalen Gesellschaft erstellt wurde, gelangte bis vor das Bundesgericht. Dieses beurteilte die Vorratsdatenspeicherung im Urteil vom 2. März 2018 als verfassungs- und EMRK-konform (BGE 144 I 126; Reinle & Bühlmann, 2018). Es wurde anerkannt, dass durch die Speicherung der Randdaten in die Grundrechte eingegriffen wird. Besonders in das Recht auf Achtung des Privatlebens, welches einen Anspruch auf informationelle Selbstbestimmung

mitumfasst (BGE 144 I 126, E. 4). Jedoch wird die Intensität des Eingriffs relativiert, da der tatsächliche Inhalt des Gesprächs nicht mitaufbewahrt wird.

Die rechtliche Auseinandersetzung ist noch nicht abgeschlossen. Die Digitale Gesellschaft reichte gegen das Urteil Beschwerde beim Europäischen Gerichtshof für Menschenrechte (EGMR) ein, welcher die Schweiz zur Stellungnahme eingeladen hat und der Sache grundsätzliche Bedeutung beimisst (Walter, 2023). Ein Urteil steht jedoch (Stand Juni 2026) noch aus (Digitale Gesellschaft, o. J.).

Die Schweizer Lösung erscheint im Vergleich zu anderen europäischen Ländern als Sonderfall, da der Gerichtshof der Europäischen Union (EuGH) die EU-Richtlinie zur Vorratsdatenspeicherung 2014 für ungültig erklärte. In der Folge präziserte er strenge Bedingungen und untersagte die anlasslose Speicherung zur Kriminalitätsbekämpfung. Einzig für die nationale Sicherheit wird sie unter strengen Bedingungen zugelassen. Entsprechend wurden nationale Regelungen, wie etwa in Deutschland, wiederholt für unionsrechtswidrig erklärt. Das Bundesgericht hält dennoch an der anlasslosen Speicherung fest und widerspricht damit der Rechtsprechung anderer höchster Gerichte in Europa. Die Untersuchung von Birrer et al. (2023) zeigt, dass kein flächendeckender Rückgang der anlasslosen Speicherung von Kommunikationsmetadaten in Europa zu verzeichnen ist. Eher im Gegenteil, sie weitet sich aus. Ausserdem sehen die Gesetze nur unzureichende Schutzmechanismen gegen die Risiken vor, die mit der Speicherung verbunden sind. Die Schweiz ist somit Teil einer trotz anhaltender grundrechtlicher Bedenken fortbestehenden Entwicklung der Vorratsdatenspeicherung.

Auskunftsrecht (Art. 25 DSG)

Während durch das BÜPF die Speicherung von Metadaten angeordnet wird, regelt das Datenschutzgesetz (DSG, SR 235.1), welche Rechte eine betroffene Person gegenüber jenen Stellen hat, die ihre Daten bearbeiten. Zentral für die Rechte einer betroffenen Person ist Art. 25 DSG, der das sogenannte Auskunftsrecht regelt. Art. 25 Abs. 1 DSG hält fest: “Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.” Die Auskunft muss alle Informationen enthalten, die erforderlich sind, damit die betroffene Person ihre Rechte wahrnehmen kann und die Bearbeitung nachvollziehbar wird. Darunter fallen die Identität des Verantwortlichen, welche Daten bearbeitet werden, zu welchem Zweck die Bearbeitung stattfindet, wie lange die Daten aufbewahrt werden, von woher sie kommen und allfällige Empfänger (Art. 25 Abs. 2 DSG). Sie muss grundsätzlich kostenlos (Art. 25 Abs. 6 DSG) und in der Regel innerhalb von 30 Tagen erteilt werden (Art. 25 Abs. 7 DSG). Auf das Auskunftsrecht kann zudem nicht im Voraus verzichtet werden (Art. 25 Abs. 5 DSG).

Das Auskunftsrecht gilt als Basis des Datenschutzrechts und erfüllt eine Kontrollfunktion. Eine Person muss wissen, welche Daten über sie bearbeitet werden. Ansonsten kann sie nicht überprüfen, ob dies im Einklang mit den datenschutzrechtlichen Grundsätzen geschieht. Falls dies nicht der Fall ist, kann sie einen Anspruch auf Berichtigung oder Löschung der Daten geltend machen. Das Auskunftsrecht ist also eng mit dem in Kapitel 2 behandelten Recht auf informationelle Selbstbestimmung verbunden. Ohne die Möglichkeit, Kenntnis über die bearbeiteten Daten zu erlangen, lässt sich die Kontrolle darüber schwer ausüben. Das DSG wird

vom Bundesrat demnach als Konkretisierung der informationellen Selbstbestimmung verstanden (Bundesrat, 2017). In der Lehre wird aber kritisiert, inwiefern dieses Recht tatsächlich vom DSGVO umgesetzt wird (Thouvenin, 2023).

Für diese Arbeit ist das Auskunftsrecht von grosser Bedeutung. Es bietet die rechtliche Grundlage dafür, dass der Autor die über ihn gespeicherten Randdaten beziehen und im nachfolgenden Kapitel durch eine Fallanalyse verwerten kann.

Fallanalyse: Eigene Vorratsdaten von Spusu

Es sei explizit darauf hingewiesen, dass es sich bei der vorliegenden Analyse um einen Einzelfall handelt. Die Aussagen basieren auf den Daten des Autors und repräsentieren keine über diesen Fall hinausgehende Allgemeingültigkeit.

Die Daten

Wie oben erwähnt, hat man in der Schweiz das Recht, die eigenen, von den Mobilfunkkonzernen aufgezeichneten Daten einzusehen. Diese Daten müssen der betreffenden Person zugänglich gemacht werden. In der Regel sollte es möglich sein, diese über ein Onlineformular oder einen Anruf beim Mobilfunkanbieter zu beantragen.

Im Fall des Autors gibt es beim Anbieter „Spusu“ die Möglichkeit, die Daten online abzurufen. Allerdings nur jene der letzten vier Monate. Nach Kontaktaufnahme mit dem Kundendienst und der Erklärung, was Vorratsdaten überhaupt sind, verging ca. eine Woche, bis eine unverschlüsselte E-Mail mit einer CSV-Datei zugestellt wurde. Eine Comma-Separated-Values-Datei (CSV) ist ein Speicherformat, das tabellarische Werte mit Kommas abgrenzt und so einfacher computerlesbar macht. Für Menschen ist es aber eher unvorteilhaft, da es das normale Lesen erschwert, wie man in Abbildung 1 erkennen kann.

```
1 Datum;Von;Nach;Ereignis;Anzahl;Dauer;Zone;Kosten (netto);Daten (empfangen);Daten (gesendet)
174 30.01.2026 11:54;417941****;;Datentransfer;1;02:48:51;Schweiz Daten kostenlos;0,00 251,61 KB;293,68 KB
175 30.01.2026 11:46;417941****;;Datentransfer;1;00:12:17;Schweiz Daten kostenlos;0,00 15,59 KB;23,56 KB
176 29.01.2026 20:16;+41786****;417941****;Anruf;1;00:08:14;Schweiz;0,00 0 KB;0 KB
177 29.01.2026 17:51;417941****;+417988****;Anruf;1;00:01:24;Schweiz;0,00 0 KB;0 KB
178 29.01.2026 17:43;+41792****;417941****;Anruf;1;00:01:29;Schweiz;0,00 0 KB;0 KB
```

Abbildung 1: Beispiel einer CSV-Datei

Zunächst musste die Datei also in eine Excel-Tabelle übertragen werden. Mithilfe eines kleinen Python-Skripts war dies in wenigen Minuten erledigt. Das Skript anonymisierte die Daten noch einmal, nachdem Spusu dies bereits getan hatte. Die verschiedenen Nummern wurden mit Buchstaben versehen, um sie vollständig zu anonymisieren. Somit ist der Datensatz bereit zur Analyse.

Analyse

In der erstellten Exceltabelle befinden sich 1353 Einträge über einen Zeitraum von 208 Tagen (vom 1. August 2025 bis zum 25. Februar 2026), also knapp sieben Monate. (Obwohl die Daten nach sechs Monaten gelöscht werden sollten.) Von den 1353 Einträgen sind 1290 Datentransfers, 61 Anrufe und zwei SMS. Alles mit 24 verschiedenen Gesprächspartnern.

61 Anrufe in knapp sieben Monaten klingen nach sehr wenig Telefonaten. Dies liegt daran, dass Mobilfunkanbieter Anrufe, die über Apps wie beispielsweise WhatsApp, Telegram oder Signal getätigt werden, nicht aufzeichnen. Die Analyse der Daten beschränkt sich also auf die Nutzung, die wirklich im Mobilfunknetz stattgefunden hat.

Mithilfe eines weiteren Python-Skripts werden die Daten nun in die drei Kategorien „Tagesrhythmus“, „Kontakte“ und „Mobilität“ unterteilt. Zudem werden passende Visualisierungen sowie Tabellen erstellt. Die Abbildungen zeigen stets alle Daten gleichzeitig. Das heisst, wenn man beispielsweise die einzelnen Stunden der Nutzung sieht, werden alle zu dieser Uhrzeit erhobenen Daten angezeigt.

Tagesrhythmus

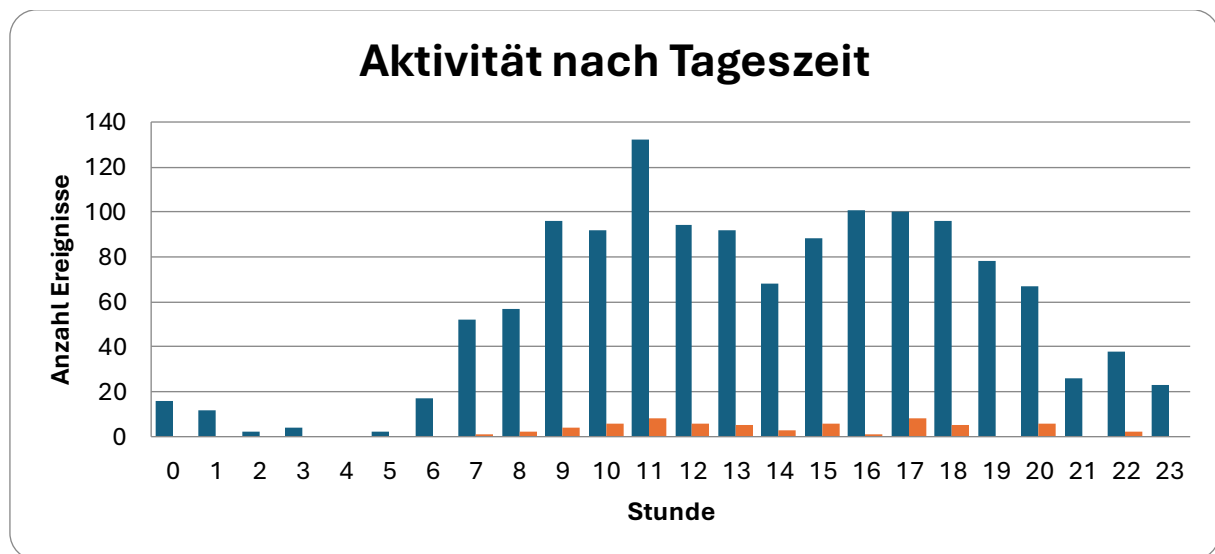


Abbildung 2: Aktivität nach Uhrzeit

In Abbildung 2 ist zu erkennen, zu welcher Uhrzeit die verschiedenen Aktivitäten in den sieben Monaten der Datenaufzeichnung entstanden sind. Anrufe und SMS werden als eigene Kategorie (rot) aufgezeigt, während mobile Daten in (blau) dargestellt sind. Allein anhand dieser Abbildung lässt sich ablesen, dass der Autor mit grosser Wahrscheinlichkeit von 2:00 Uhr bis 5:00 Uhr schläft, da zu dieser Zeit sehr wenige bis gar keine Daten erhoben wurden. Ausserdem lässt sich die Zeit ablesen, in der der Autor sein Smartphone am aktivsten nutzt. Die meisten Ereignisse finden um 11 Uhr statt. Eine erhöhte Aktivität ist aber auch zwischen 16:00 Uhr und 18:00 Uhr festzustellen.

Nun kann man sich nicht nur die einzelnen Stunden, sondern auch die einzelnen Tage anschauen.

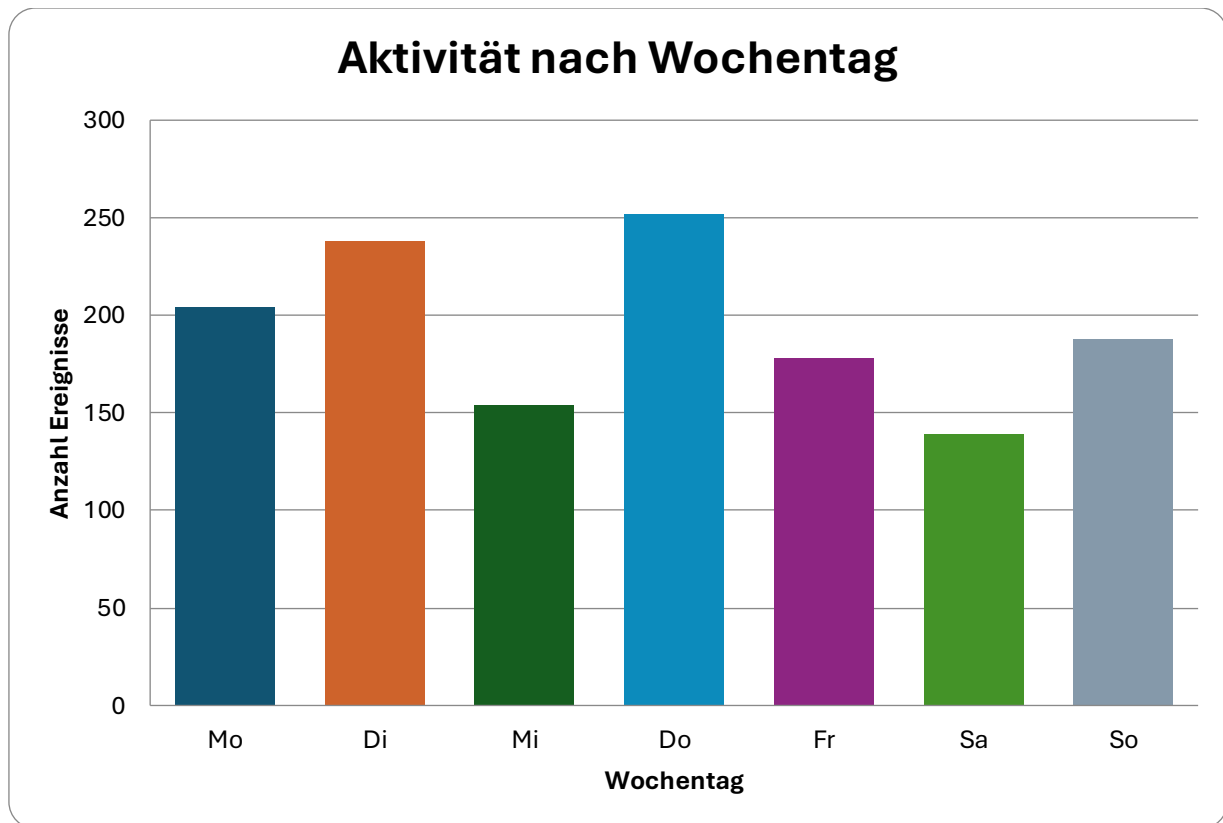


Abbildung 3: Aktivität nach Wochentag

Abbildung 3 zeigt, wie viele Einträge an welchem Tag entstanden sind. Deutlich erkennbar sind die aktivsten Tage Dienstag und Donnerstag, während das Smartphone am Samstag am wenigsten genutzt wird. Es lässt sich ein akademischer bzw. beruflich geprägter Rhythmus erkennen. Da Dienstag und Donnerstag Kernarbeitstage sind, kann die hohe Aktivität darauf hindeuten, dass das Gerät stark in den Alltags-, Arbeits- oder Studienbetrieb eingebunden ist. Am Mittwoch zeigen sich die wenigsten Einträge der Arbeitswoche. Das kann zum einen bedeuten, dass es ein Tag ist, an dem der Autor frei hat, oder dass der Autor an diesem Tag zu beschäftigt ist, um das Handy zu nutzen. Auch Samstag ist ein eher ruhiger Tag, was die Einträge angeht. Daher kann man schliessen, dass der Autor an diesem Tag entweder sein Handy weglagt, um Zeit mit Familie, Freunden oder Ähnlichem zu verbringen. Aktivitäten also, die offline stattfinden. Oder er ist zu beschäftigt, um sein Handy zu nutzen.

Nicht nur die Zeit und die Tage, an denen das Handy genutzt wurde, lassen sich durch die Metadaten erschliessen, sondern auch die verschiedenen Personen, mit denen Kontakt aufgenommen wurde.

Soziale Kontakte

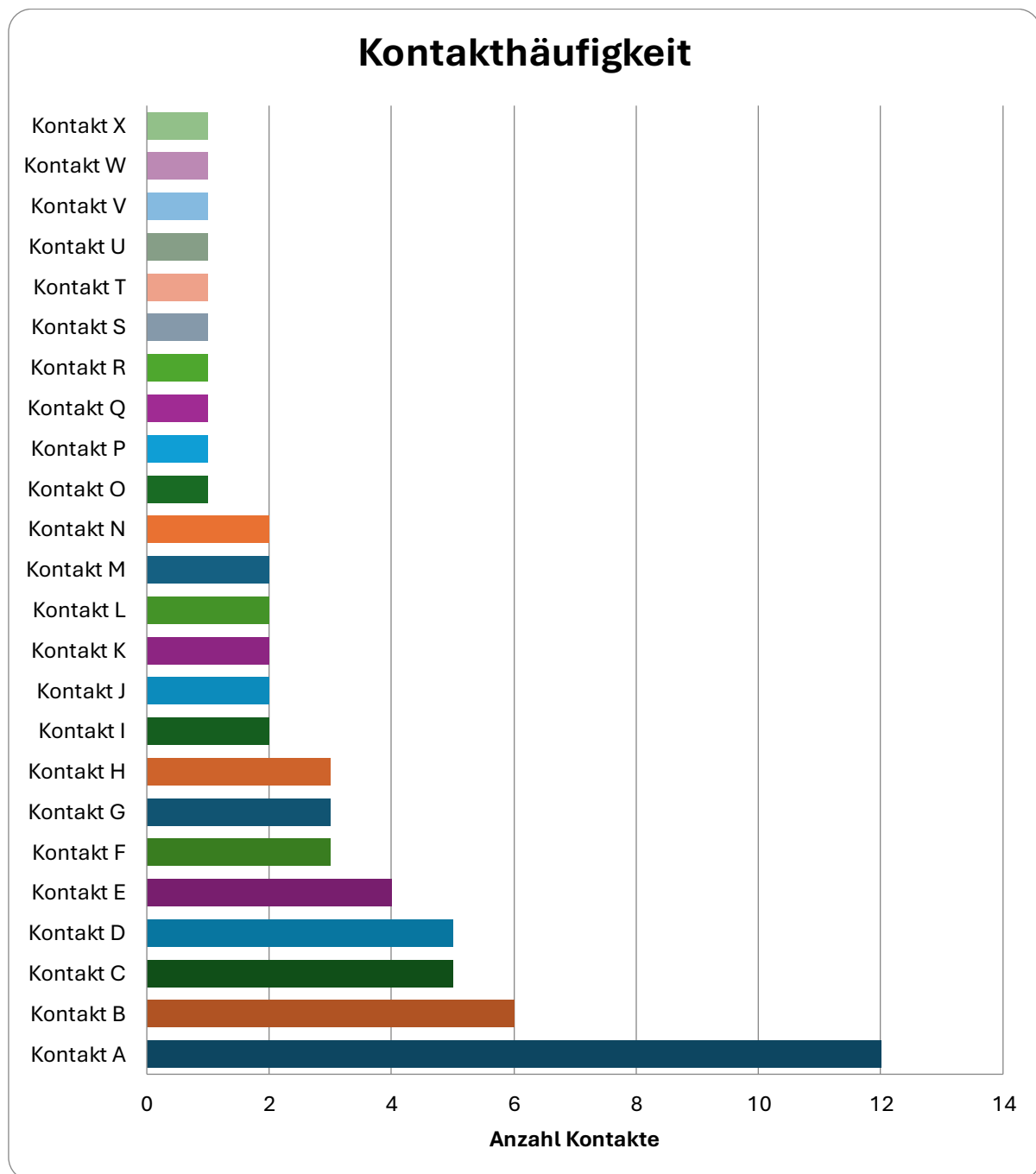


Abbildung 4: Kontakthäufigkeit

In Abbildung 4 sticht vor allem A mit doppelt so vielen Kontaktaufnahmen wie B heraus. Daraus kann man schliessen, dass dieser Kontakt dem Autor beruflich oder privat sehr nahesteht. Auch mit den Kontakten B, C, D und E hatte der Autor in rund sieben Monaten häufiger Kontakt. In den Originaldaten kann man auch den Ort sehen, an dem sich der Autor befand, sowie ob der Anruf ein- oder ausgegangen ist. Diese Angaben erlauben Rückschlüsse auf die Nähe und Rolle der Kontakte.

Mobilität

Zone	Anzahl	Anteil
Schweiz Daten kostenlos	1250	92.4%
Schweiz	60	4.4%
Italien Mobil Roaming Daten kostenlos	40	3.0%
Schweiz SMS kostenlos	2	0.1%
Italien Roaming Passiv kostenlos	1	0.1%

Tabelle 1: Orte der Nutzung

Aus den Daten kann man unter anderem herauslesen, wo sich die Person zum Zeitpunkt eines Telefonats oder der Nutzung von mobilen Daten befunden hat. Bei Spusu kann man keine genauen Standorte sehen, allerdings ist das Land erkennbar, in dem sich die Person befand. In Tabelle 1 kann man sehen, dass sich der Autor die meiste Zeit der Datenaufzeichnung in der Schweiz befand. Allerdings sind auch 3.1 % der Einträge in Verbindung mit einem italienischen Telefonmast entstanden, was bedeutet, dass der Autor für eine gewisse Zeit in Italien war. Wenn man sich das Datum der Verbindungen anschaut, kann man den Zeitraum, in dem sich der Autor in Italien befand, genau bestimmen. Dazu vergleicht man den Tag und die Zeit der ersten und letzten Verbindung mit Schweizer Telefonmasten und erhält so ein genaues Bild. So lässt sich auch die Aufenthaltsdauer in den jeweiligen Ländern ermitteln. Würde er im Ausland arbeiten, würde man vermehrt sehen, dass sich das Gerät in einem anderen Land ins Netz einloggt, was hier nicht der Fall ist.

Grenzen der Analyse

Die Analyse unterliegt methodischen Einschränkungen. Wie zu Beginn betont, handelt es sich hierbei um einen Einzelfall. Die Daten des Autors repräsentieren eine Person und lassen somit keine verallgemeinernden Aussagen zu. Dazu kommt, dass Metadaten zwar Rückschlüsse, aber keine Gewissheit zulassen. Aus dem Zeitstempel der Daten lässt sich zwar eine Schlafenszeit vermuten, ob das Gerät während dieser Zeit aber genutzt wurde, bleibt offen. Eine Besonderheit der Selbstanalyse ist, dass der Autor die Schlüsse, die gezogen werden, an seinem eigenen Verhalten messen kann. Dies ist eine Vergleichsgrundlage, über die ein aussenstehender Beobachter nicht verfügt. Dadurch wird zwar die Deutung erleichtert, jedoch eine Übertragung erschwert. Was hier als zutreffend erscheint, müsste eine unbeteiligte Person mit deutlich grösserer Unsicherheit erschliessen.

Weitere Grenzen gehen von dem Datensatz selbst aus. Spusu zeichnet ausschliesslich Randdaten der Kommunikation auf, die über das Mobilfunknetz läuft. Wenn ein Nutzer überwiegend Dienste wie beispielsweise WhatsApp, Signal oder Telegram nutzt, werden diese Daten nicht aufgezeichnet, was deren Interpretation ungenauer macht. Im Fall des Autors werden eben diese Dienste des Öfteren genutzt, was sich auch in den Zahlen widerspiegelt. Von den 1353 Einträgen über knapp sieben Monate sind nur 61 Einträge Anrufe und zwei SMS. Für

die Interpretation sind genau diese Einträge am aussagekräftigsten. Sie fallen in diesem spezifischen Fall zahlenmässig gering aus und machen das Bild unschärfer. Schliesslich wird der Standort auf Länderebene ausgegeben, womit man Auslandsaufenthalte erschliessen, genaue Bewegungen innerhalb des Landes aber nicht analysieren kann. Die Auswertung, die hier möglich ist, bildet also nur einen Ausschnitt ab von dem, was gespeicherte Vorratsdaten tatsächlich preisgeben.

Diskussion: Folgen der VDS für informationelle Selbstbestimmung

Die Fallanalyse zeigt, dass sich aus den Vorratsdaten von Spusu ein Alltagsbild des Autors zeichnen lässt. Aus den Zeitstempeln sind Schlafenszeit und Aktivitätsspitzen ersichtlich, während aus der Verteilung der Wochentage ein beruflich/akademisch geprägter Rhythmus erschlossen werden kann. Aus der Häufigkeit der Verbindungen kann die Nähe zu einzelnen Kontakten bestimmt werden und aus den Standortdaten kann eine klare Abgrenzung einer Italienreise gemacht werden. Damit kann die Forschungsfrage, welche Rückschlüsse auf das Alltagsverhalten von Personen sich anhand von Vorratsdaten, welche von Schweizer Mobilfunkanbietern gespeichert werden, ziehen lassen, beantwortet werden. Bereits durch einen dünnen Datensatz kann man Aussagen zur Tagesstruktur, Mobilität und den sozialen Beziehungen einer Person machen. Bloss technische Verbindungsinformationen können also zu einem Profil verdichtet werden.

Der Befund bestätigt in kleinem Massstab, was Mayer et al. (2016) gezeigt haben. Man braucht nicht zwingend den Inhalt der Kommunikation, um bestimmte Verhaltensmuster, soziale Kontakte oder Aufenthaltsorte bestimmen zu können. Dass dies in der Analyse sogar mit deutlich weniger Anrufen gemacht werden kann, unterstreicht die Übertragbarkeit der dort beschriebenen Muster. Damit wird auch klar, was vom Bundesverfassungsgericht im Volkszählungsurteil, in Verbindung mit den Bedingungen automatischer Datenverbreitung, mit “kein belangloses Datum mehr” gemeint ist (BVerfG, 1983, Rn. 150). Die einzelnen Einträge im Datensatz des Autors sagen alleinstehend nichts aus. Wenn man sie miteinander verknüpft, erzeugen sie Aussagewerte, die die Sensibilität der Daten ausmachen. Genau diese Verknüpfungs- und Verwendungsmöglichkeit macht laut Gericht die Schutzbedürftigkeit aus. Nicht der Inhalt des einzelnen Datums.

Hier kann man eine Spannung zur Begründung des Bundesgerichts sehen. Es anerkennt im Urteil vom 2. März 2018, dass die Speicherung der Randdaten in das Recht auf Achtung des Privatlebens eingreift. Es greift damit auch in die informationelle Selbstbestimmung ein (BGE 144 I 126, E. 4). Allerdings relativiert es die Intensität des Eingriffs und stützt sich auf die folgenden drei Punkte. Es würden nie Inhalte gespeichert, die Daten würden nicht von den Anbietern verknüpft und die Behörden könnten nur im Strafprozess darauf zugreifen (BGE 144 I 126, E. 5). Diese Relativierung kann man auf die Unterscheidung von schützenswertem Inhalt und vermeintlich harmlosen Metadaten zurückführen. Durch die Fallanalyse wird diese Unterscheidung jedoch in Frage gestellt. Wenn man nur mithilfe der Randdaten bereits Schlaf, Arbeit, enge Bezugspersonen und Auslandsreisen ablesen kann, ist das Nichtaufzeichnen von Inhalten kein verlässlicher Massstab für die Schwere des Eingriffs. Diese Kritik ist kein

Einzelfall. Laut Birrer et al. (2023) wird eine Unterscheidung zwischen Inhalt und Metadaten in der Forschung als zunehmend überholt angesehen. Selbst der EuGH anerkennt zunehmend, dass Metadaten ebenso sensibel sein können wie die Inhalte. Hinzu kommt, dass mit 61 Anrufen der Datensatz des Autors eher dünn ist. Mayer et al. (2016) konnten mit mehr Daten sogar Hinweise auf Beziehungen, Gesundheit und weitere sensible Merkmale gewinnen. Es ist anzunehmen, dass eine behördliche Auswertung eines Bestandes über sechs Monate ein noch schärferes Bild zeigen könnte als das, das die vorliegende Analyse zeigt. Der Schutz der Inhalte bringt daher weitestgehend wenig, wenn man vergleichbar sensible Informationen ohnehin aus der Verknüpfung der Metadaten ziehen kann. Wenn man das aus Sicht der informationellen Selbstbestimmung betrachtet, wiegt die anlasslose Speicherung schwerer, als es durch die juristische Relativierung nahegelegt wird. Es ist nicht bloss ein Randbereich der Kommunikation betroffen, sondern die Möglichkeit, selbst darüber zu bestimmen, wer ein solches Profil über einen anlegen darf und wer nicht. Nicht davon berührt sind die fehlenden Verknüpfungen und die Schranken, welche die Strafprozessordnung vorgibt.

Die Tragweite des Eingriffs erschöpft sich nicht im Individuellen. Eine demokratietheoretische Begründung wird im Volkszählungsurteil gegeben. Wer damit rechnet, dass alles, was er tut, registriert und weitergegeben werden kann, passt sich an und versucht, möglichst unauffällig zu leben (BVerfG, 1983, Rn. 146). Selbstbestimmung ist für das Gericht deshalb nicht nur Selbstzweck, sondern dient als Bedingung für das Funktionieren einer freiheitlich-demokratischen Gesellschaft. Überträgt man das auf die Vorratsdatenspeicherung, bedeutet es, dass bereits das Wissen um die anlasslose und flächendeckende Speicherung von Verbindungs- und Standortdaten ein solches Anpassungsverhalten begünstigen kann. Dies ist nicht eine rein theoretische Annahme aus dem Jahr 1983. Birrer et al. (2023) verweisen auf Befunde, nach denen schon das reine Wissen über die Vorratsdatenspeicherung Menschen von vertraulicher Kommunikation abhalten kann. Solche abschreckenden Effekte (Chilling Effects) stützen die Befürchtungen aus dem Volkszählungsurteil und gelten als gesellschaftliche Folge einer modernen staatlichen Überwachung. Der entscheidende Punkt ist dabei die Anlasslosigkeit. Die eigenen Daten werden nicht aufgrund eines konkreten Verdachts gespeichert, sondern im Voraus und bei allen Nutzern gleichzeitig. Nicht ein späterer Zugriff der Behörde auf die Daten beeinträchtigt die informationelle Selbstbestimmung, sondern bereits die bloße Existenz des Datensatzes. Die in der öffentlichen Debatte verbreitete Verharmlosung der Metadaten zeigt, dass die Betroffenen die Aussagekraft eines solchen Datensatzes unterschätzen.

An dieser Stelle gewinnt Art. 25 DSG, das Auskunftsrecht, an Bedeutung. Dieser Artikel ist das Instrument, mit dem Betroffene Kenntnis über gespeicherte Daten von ihnen erlangen und so Kontrolle darüber ausüben können. In der Theorie wird damit die anlasslose Speicherung korrigiert. Die Erfahrung des Autors zeigt jedoch, dass das in der Praxis nur teilweise funktioniert. Über das Onlineportal seines Anbieters waren nur die letzten vier Monate abrufbar. Auch der Kundendienst musste zunächst über den Begriff der Vorratsdaten aufgeklärt werden, bevor man die Daten überhaupt anfordern konnte. Zu guter Letzt wurden die Daten durch eine unverschlüsselte E-Mail zugestellt. Das Recht besteht formal, scheitert aber an der Ausübung, der mangelnden Verfügbarkeit, dem mangelnden Bewusstsein und unsicherer Übermittlung. Somit kann es seine Kontrollfunktion nur unzureichend erfüllen. Die Lücke zwischen dem

Recht auf informationelle Selbstbestimmung und deren tatsächlicher Einlösbarkeit ist hier gut ersichtlich.

Von Birrer et al. (2023) wird nahegelegt, dass es sich bei dieser Lücke nicht um ein Einzelphänomen handelt. Bei Vorratsdatenregelungen sind Auskunfts- und Benachrichtigungsrechte selten ausdrücklich vorgesehen. Sie sind mehr dem allgemeinen Datenschutzrecht überlassen. Aus diesem Grund wird die Speicherung nicht auf dem gleichen Niveau geschützt wie die Datenbearbeitung durch private Unternehmen (Birrer et al., 2023). Auch in der Schweiz ist das Auskunftsrecht im DSG und nicht im BÜPF untergebracht.

Zusammengefasst zeigen die Befunde auf, dass die Gesellschaft und teilweise auch das Recht die Metadaten und deren Aussagekraft als zu gering einschätzen. Die anlasslose Vorratsdatenspeicherung greift tiefer in die informationelle Selbstbestimmung ein, als die Beschränkung auf Randdaten vermuten lässt. Ausserdem vermag das Auskunftsrecht diesen Eingriff in der Praxis nur bedingt auszugleichen. Welche Schlüsse für die Bewertung der Schweizer Regelung daraus gezogen werden können, ist Gegenstand des abschliessenden Fazits.

Fazit

Die vorliegende Arbeit ist der Frage nachgegangen, welche Rückschlüsse sich auf das Alltagsverhalten von Personen aus den von Schweizer Mobilfunkanbietern gespeicherten Vorratsdaten ziehen lassen. Eine Fallanalyse wurde mit den eigenen, von Spusu erhobenen Daten des Autors gemacht. Es wurde gezeigt, dass bereits mit einem einzelnen und vergleichsweise dünnen Datensatz ein aussagekräftiges Bild des Autors gemacht werden kann. Tagesrhythmus, soziale Nähe und die Mobilität des Autors konnten dargestellt werden. Der Einzelfall bestätigt somit die Befunde von Mayer et al. (2016) im Kleinen. Es wird vor Augen geführt, was das Bundesverfassungsgericht mit der Feststellung, dass es unter den Bedingungen automatischer Datenverbreitung kein belangloses Datum mehr gebe, meinte (BVerfG, 1983, Rn. 150). Mit diesem Hintergrundwissen erweist sich die Geringschätzung von Metadaten in der öffentlichen Debatte als nicht tragfähig.

Wenn man den Sachverhalt aus der Perspektive der informationellen Selbstbestimmung betrachtet, bedeutet dies, dass die anlasslose Speicherung der Randdaten tiefer in das Recht eingreift, als die juristische Beschränkung auf blosser Metadaten nahelegt. Das Bundesgericht versucht, den Eingriff damit zu relativieren, dass die Gesprächsinhalte nicht gespeichert werden (BGE 144 I 126). Hier greift es jedoch zu kurz. Vor diesem Hintergrund erscheint es kritikwürdig, dass die Schweiz an einer anlasslosen, flächendeckenden Speicherung der Daten festhält. Zumal der EuGH und andere höchste Gerichte eine solche anlasslose Speicherung untersagt haben und Birrer et al. (2023) zugleich auf unzureichende Schutzmechanismen verweisen. Wie die Erfahrung des Autors mit dem Datenbezug gezeigt hat, vermag auch das Auskunftsrecht nach Art. 25 DSG seine Kontrollfunktion in der Praxis nur bedingt zu erfüllen. Es könnte den Eingriff aber abfedern, wenn es denn richtig angewendet würde.

Diese Einschätzungen sind mit dem Wissen zu betrachten, dass die empirische Grundlage der Arbeit ein Einzelfall ist. Sie erlaubt keine verallgemeinernde Aussage. Es wird jedoch

anschaulich illustriert, was bereits ein begrenzter Datenbestand preisgeben kann. Es lässt sich auch erahnen, welches Bild sich ergeben könnte, wenn ein vollständiger Bestand behördlich ausgewertet würde. Wie die rechtliche Auseinandersetzung ausgeht, bleibt offen. Das Verfahren am Europäischen Gerichtshof für Menschenrechte, welches von der Digitalen Gesellschaft geführt wird, ist noch hängig (Walter, 2023; Digitale Gesellschaft, o. J.). Sein Ausgang dürfte allerdings für die Zukunft der Vorratsdatenspeicherung in der Schweiz richtungsweisend sein. Diese Fallanalyse könnte man mit weiteren Untersuchungen stärken. Man könnte mehrere Datensätze vergleichen, um die Eindrücke, die hier gewonnen wurden, zu bestätigen.

Anhang

Literaturverzeichnis

Art. 1 GG - Einzelnorm. (o. J.). Abgerufen 23. Juni 2026, von https://www.gesetze-im-internet.de/gg/art_1.html

Art. 2 GG - Einzelnorm. (o. J.). Abgerufen 23. Juni 2026, von https://www.gesetze-im-internet.de/gg/art_2.html

BGE 144 I 126. (2018). *Urteil vom 2. März 2018, 1C_598/2016.*

https://www.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F144-I-126%3Ade%E2%9F%A8=de&zoom=&type=show_document

Birrer, A., He, D., & Just, N. (2023). The state is watching you—A cross-national comparison of data retention in Europe. *Telecommunications Policy*, 47(4), 102542. <https://doi.org/10.1016/j.telpol.2023.102542>

Bundesrat. (2017). *Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz.*

<https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2017/2057/de/pdf-a/fedlex-data-admin-ch-eli-fga-2017-2057-de-pdf-a-1.pdf>

BVerfG. (1983). *Urteil vom 15. Dezember 1983.*

https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html

Digitale Gesellschaft. (o. J.). Vorratsdatenspeicherung. *Digitale Gesellschaft.*

<https://www.digitale-gesellschaft.ch/dossier/vorratsdatenspeicherung/>

Mayer, J., Mutchler, P., & Mitchell, J. C. (2016). Evaluating the privacy properties of telephone metadata. *Proceedings of the National Academy of Sciences*, 113(20), 5536–5541. <https://doi.org/10.1073/pnas.1508081113>

Reinle, M., & Bühlmann, L. (2018, April 15). BGER: Schweizer Vorratsdatenspeicherung ist verfassungsmässig. *MLL News Portal*. <https://www.mll-news.com/bger-schweizer-vorratsdatenspeicherung-ist-verfassungsmaessig/>

Rössler, B. (2001). *Der Wert des Privaten*. Suhrkamp.

SR 101—*Bundesverfassung der Schweizerischen Eidgenossenschaft*. (o. J.). Fedlex. Abgerufen 23. Juni 2026, von https://www.fedlex.admin.ch/eli/cc/1999/404/de#art_13

SR 235.1—*Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG)*. (o. J.). Fedlex. Abgerufen 23. Juni 2026, von <https://www.fedlex.admin.ch/eli/cc/2022/491/de>

SR 780.1—Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). (o. J.). Fedlex. Abgerufen 23. Juni 2026, von https://www.fedlex.admin.ch/eli/cc/2018/31/de#art_26

Thouvenin, F. (2023). *Informationelle Selbstbestimmung: Intuition, Illusion, Implosion*. Helbing Lichtenhahn.

Walter, A. (2023, Februar 10). Vorratsdatenspeicherung in der Schweiz steht vor der Beurteilung durch den Europäischen Gerichtshof für Menschenrechte. *Digitale Gesellschaft*. <https://www.digitale-gesellschaft.ch/2023/02/10/vorratsdatenspeicherung-in-der-schweiz-steht-vor-der-beurteilung-durch-den-europaeischen-gerichtshof-fuer-menschenrechte-ausstehender-entscheid-von-bedeutung/>

Datensatz und Python-Skripts

Nun noch der Link zu einem Google-Drive-Ordner. Darin sind der anonymisierte Datensatz und die Excel-Datei, die für die Fallanalyse verwendet wurde, zu finden. Des Weiteren befinden sich in dem Ordner zwei Python-Skripte, die zur Erstellung der Excel-Dateien genutzt wurden. Das erste Skript wandelt den Spusu-Vorratsdaten-Export (CSV) in eine bereinigte und anonymisierte Excel-Datei um. Dieses Skript ist der erste Schritt der Fallanalyse, da es die Datengrundlage erzeugt, auf der die eigentliche Auswertung (Schritt 2) aufbaut. Das zweite Skript wertet die in Schritt eins aufbereitete Excel-Datei aus und erstellt eine Auswertungsdatei mit den drei Informationskategorien der Fallanalyse und den dazugehörigen Grafiken.

Google Drive Ordner

Lauterkeitserklärung und Verwendung von KI



Universität
Zürich^{UZH}

Philosophische Fakultät

Universität Zürich
Philosophische Fakultät
Rämistrasse 69
8001 Zürich
www.phil.uzh.ch

Selbstständigkeitserklärung der Philosophischen Fakultät

Hiermit erkläre ich, Schmid Nils (Name, Vorname)

dass ich die eingereichte schriftliche Arbeit/Qualifikationsarbeit

mit dem Titel Vorrelatenspeicherung und informationelle Selbstbestimmung am Beispiel von Spusu, einem Schweizer Mobilfunkanbieter.

- ohne unerlaubte Hilfsmittel und in eigenen Worten verfasst habe,
- dass ich die Grundsätze wissenschaftlicher Integrität eingehalten habe (vgl. https://api.swiss-academies.ch/site/assets/files/25852/kodex_layout_de_web.pdf)
- und dass ich die vorliegende Arbeit nicht bereits einmal zur Abgeltung anderer Studienleistungen an der Universität eingereicht habe.

Deklaration zur Verwendung von Quellen und Hilfsmitteln (entweder A oder B ankreuzen)

A Der/die Dozent:in hat das Verwenden von generativen KI-Tools *nicht erlaubt* (= KI als unerlaubtes Hilfsmittel).

☐ Ich bestätige, dass ich die vorliegende Arbeit in allen Teilen selbstständig angefertigt und keine anderen als die in der Arbeit angegebenen Quellen und Hilfsmittel benutzt habe. Sämtliche wörtlichen oder sinngemässen Übernahmen und Zitate sind kenntlich gemacht und nachgewiesen. Ich habe in der Arbeit keine KI-generierten Textpassagen oder Inhalte verwendet.*

B Der/die Dozent:in hat das Verwenden von generativen KI-Tools *erlaubt* (= KI als erlaubtes Hilfsmittel).

☒ Ich bestätige, dass ich die vorliegende Arbeit selbstständig angefertigt und keine anderen als die in der Arbeit angegebenen Quellen und Hilfsmittel benutzt habe. Sämtliche wörtlichen oder sinngemässen Übernahmen und Zitate sowie KI-basierte Inhalte (einschliesslich Abbildungen, Tabellen, Grafiken u.a.), welche in der obengenannten Arbeit enthalten sind, habe ich als solche gekennzeichnet und mit einem Hinweis auf das verwendete KI-basierte Programm versehen,*

- dass ich etwaige Richtlinien, die auf der Homepage des Seminars/ Instituts oder direkt durch die Dozentin oder den Dozenten oder die Betreuungsperson kommuniziert worden sind, befolgt habe,
- dass ich die volle Verantwortung für die Auswahl, Übernahme und Einbeziehung von KI-generierten Ergebnissen trage.

Allgemeine Information zum Verfahren bei Verdacht auf unlauteres Verhalten

Ich nehme zur Kenntnis, dass schriftliche Arbeiten, die diese Bestimmungen der Selbstständigkeitserklärung missachten, gemäss § 30 der RVO als unlauteres Verhalten betrachtet werden können und rechtliche sowie disziplinarische Konsequenzen nach sich ziehen können.

Wird unlauteres Verhalten gemäss § 30 der RVO geltend gemacht, wird der Leistungsnachweis durch den oder die Studiendekan:in als «nicht bestanden» bzw. mit der Note «1» bewertet. Der oder die Studiendekan:in entscheidet, ob ein Disziplinarverfahren beantragt wird.

Ort, Datum

Unterschrift

Bubikon, 26.6.26

N. Schmid

* Hinweis: Orthografische, grammatikalische und stilistische Textverbesserungen durch KI-basierte Tools sind grundsätzlich erlaubt und müssen nicht eigens nachgewiesen werden, es sei denn, der/die Dozent:in oder die Betreuungsperson kommuniziert schriftlich eine andere erforderliche Praxis.



Guideline and Template to Disclose the Use of (Generative) AI Tools¹ in the Seminar “Vorratsdatenspeicherung – Hintergründe und aktuelle Debat-ten” (FS2026)

Zurich, 23 June 2026

Basic principles

The following basic principles need to be adhered to if AI tools are used in any assignment:

1. AI tools are used to *assist* with the work, rather than to do the work.
2. All usage of AI tools must be documented in the disclosure form below.
3. *Responsible* use of AI tools includes the careful verification of any resulting text or code. Students are fully responsible for the correctness and quality of any content used in their assignment, including content that was created or edited using AI tools.

Disclosure Form for the Usage of AI Tools in Assignments

Please indicate whether you used any artificial intelligence (AI) tools to create or edit any content or code used within or for this assignment²:

- ☒ Yes, I used an AI tool to assist me with the present work.
☐ No, I did not use any AI tools to assist me with the present work.

If you selected "Yes", you must fill out the table below that includes all the purposes that you used AI tools together with your assignment. In it, please specify:

- For what purpose did you use (an) AI tool(s) (see list below)?
- Specify your use for this purpose and, if applicable, declare what rough percentage of the assignment was created or changed using AI tools for this purpose.
- Which AI tool(s) did you use for this purpose?

Non-exhaustive list of purposes:

1. Research design
 - a. Generating problem statements
 - b. Generating research questions
 - c. Deriving hypotheses
 - d. Suggesting appropriate methodologies for research objectives
 - e. Suggesting concepts or variables to consider

¹ This guideline and disclosure form was developed by the IKMZ Division “Media Change and Innovation” and builds on the [use of AI tools by the University of Zurich](#) and the [guidelines of the Department of Psychology](#).

² The declaration does not apply to the use of basic tools with the sole purpose of checking grammar or spelling (e.g., Microsoft Word Thesaurus).

2. Literature review
 - a. Finding relevant literature
 - b. Generating summaries of research papers
 - c. Identifying the state of research (themes, trends, etc.) on a topic
 - d. Locating research gaps
3. Data analysis and interpretation
 - a. Choosing appropriate method of data analysis
 - b. Suggesting data analysis steps
 - c. Generating code snippets for data cleaning, analysis or visualization (e.g., for R)
 - d. Debugging existing code and suggesting improvements
 - e. Providing interpretation of (quantitative or qualitative) data
4. Writing
 - a. Generating text
 - b. Rephrasing text
 - c. Language editing (checking for errors, providing suggestions to improve clarity or flow, etc.)
 - d. Creating outline for assignment
 - e. Generating images
5. Citation and referencing
 - a. Formatting citations
 - b. Creating the bibliography / reference list
 - c. Checking for citation errors or inconsistencies

Please disclose the use of (generative) AI tools in this table:

For what purpose did you use (an) AI tool(s)?	Specify your use for this purpose and, if applicable, declare what rough percentage of the assignment was created or changed using AI tools for this purpose.	Which AI tool(s) did you use for this purpose?
To correct grammar/spelling mistakes	I used it all over the paper. And corrected a lot of spelling and grammar mistakes with it	deepi write
To correct logical errors.	Also used it over the whole paper I looked up where I had sentences that don't make sense or are cut of.	claude
Bug fixing	I used claude to fix the python-scripts I wrote	claude
...	...	...
...	...	...

For further documentation of your use of AI tools, the following rules apply:

If you (directly or indirectly) cite content that was generated by an AI tool, you must save the prompt as well as the output generated by the AI tool that you reference in your assignment. This documentation must be submitted to the course instructor if requested.

It is in the students' interest to further keep a record of all the inputs (i.e., prompts) and the outputs (i.e., generated content) that were produced using AI tools (e.g., as a saved conversation in the tool, exported to a separate folder, or with screenshots). In case of doubts as to whether the use of AI tools adheres to this guideline, this documentation can help the students demonstrate their individual contributions to the assignment and provide more context for the cases in which AI tools were used.

Declaration

"I hereby confirm that the present work is my original work. I declare that I have not used any AI tools for this work, except as noted in the disclosure form. I am aware that I bear full responsibility for the selection, adoption and results of the AI-generated outputs I used. I also declare that all use of generative AI is fully disclosed. I have listed the generative AI tools used along with their product names and purpose in the disclosure form. I acknowledge that work that violates the principles set out in this disclosure form may have legal and disciplinary consequences. If ChatGPT or other AI-based tools are used without the explicit consent of the lecturer and without providing transparency regarding the use of the tool, this will be sanctioned as plagiarism and, in terms of ghostwriting, as a deliberate attempt to defraud. By signing this disclosure form, I confirm that I answered truthfully."

Title of assignment: *Vorratsdatenspeicherung und informationelle Selbstbestimmung am Beispiel von Spusu, einem Schweizer Mobilfunkanbieter.*

Name of the Student: *Nils Schmid*

Date: *26.6.26*

Signature: *N. Schmid*