Paul, Konstantin Oliver

Über den Bereichswert „Privatheit“ : Zu Aktualität und Stellung des Wertes der Privatheit bzw. Privacy in der Smart City

In:

Düchs, Martin; Illies, Christian; Sakata, Tomoki (Hrsg.), Smart in the City: eine ethische Handreichung für die Digitalisierung der Stadt, Bamberg : University of Bamberg Press, S. 81-97. 2023. DOI: 10.20378/irb-93383

Beitrag im Sammelwerk - Verlagsversion

DOI des Beitrags: 10.20378/irb-94753

Datum der Veröffentlichung: 18.04.2024

Kapitel 4.

Über den Bereichswert „Privatheit“

Zu Aktualität und Stellung des Wertes der Privatheit bzw. Privacy in der Smart City

Konstantin Oliver Paul

Erweiterte Definition: Privacy

Unter Privacy versteht man den Schutz individueller Daten, das heißt, diese dürfen immer nur 1) mit Einwilligung der Betroffen 2) zu eindeutigen, legitimen Zwecken und 3) nur so weit, wie sie wirklich relevant sind, gebraucht werden und 4) sollen zweckgebunden gespeichert werden.
Verwandte Werte: Autonomie, Gerechtigkeit, Transparenz und Partizipation.

Den Fensterladen zumachen, die Jalousien runterlassen, die Vorhänge zuziehen, die Tür hinter sich zu machen. Alle diese Handlungen markieren einen Rückzug ins Private. Der Nachbar bzw. damit sinnbildlich die Welt oder die Öffentlichkeit wird ausgeschlossen aus einem Raum, der „nur mich etwas angeht“. Wohl jeder und jede kennt solche Handlungen, die bisweilen sogar als große Gesten inszeniert werden. Und jeder und jede kennt auch das dahinterstehende Bedürfnis nach Rückzug in einen höchsteigenen, privaten Raum. In westlichen Gesellschaften gilt dieses Bedürfnis zumindest ab der zweiten Hälfte des 19. Jahrhundert als berechtigtes Anliegen und Grundrecht des Menschen. Dementsprechend hat es auch seinen gesetzlichen Niederschlag gefunden, in Deutschland beispielsweise in §140 der Paulskirchenverfassung von 1849, in Art. 6 der preußischen Verfassung von 1850 oder in Artikel 13 des Grundgesetzes. Alle genannten Rechtsnormen garantieren die so genannte Unverletzlichkeit der Wohnung. Wenn die gesetzgebenden Instanzen hier von der „Wohnung“ sprechen, dann ist damit zunächst ein physischer Raum benannt. Und lange war der Schutz dieses konkre-

ten privaten (Wohn-)Raumes ausreichend, um auch das zu schützen, was eigentlich geschützt werden sollte, nämlich die Privatsphäre jedes Individuums. Dazu gehört allerdings auch die private Kommunikation eines Individuums, weshalb mit dem Aufkommen entsprechender Telekommunikationsmittel auch für diesen Bereich entsprechende Schutzgarantien gesetzlich verankert wurden.

Eine neue Qualität der Kommunikation wird durch die digitalen Möglichkeiten erreicht. Der digitale Datenverkehr der meisten Individuen übersteigt mittlerweile bei Weitem alles, was über Telefon und Brief an Daten übermittelt wurde. Doch der digitale Datenverkehr übersteigt jeden analogen nicht nur in quantitativer Hinsicht, sondern auch in qualitativer Hinsicht ändert sich die „Datenspur", die wir hinterlassen.

Daher scheint es auch dringend geboten darüber nachzudenken, was Privatheit im digitalen Raum bedeutet und wie sie sichergestellt werden kann. Denn hier die Jalousien runterzulassen oder die Vorhänge zuzumachen ist sowohl technisch als auch lebenspraktisch nicht mehr so einfach. Tatsächlich ist der Unterschied zwischen analogem und digitalem Raum und der privaten Datenübermittlung so fundamental, dass es hier durch Verwendung des englischen Begriffs „Privacy" markiert werden soll, wenn es vor allem um diesen digitalen Raum geht.

Im Folgenden wird kurz erläutert, was unter Privacy zu verstehen ist und welche Aspekte wichtig sind. Außerdem wird angedeutet, warum die Achtung der Privacy moralphilosophisch gefordert ist.

Dazu wird zunächst anhand einer vereinfachten schematischen Skizze erläutert, wie die Datenübermittlung im digitalen Raum eigentlich stattfindet und wer beteiligt ist. Danach werden verschiedene Aspekte von Privacy kurz dargestellt und ihre moralische Relevanz diskutiert.

1. Visualisierung und Taxonomien

Mit einem einfachen Sender-Empfänger-Modell kann weder die digitale Kommunikation noch das Abrufen von Informationen im Internet adäquat verstanden werden. Um die neuartige Qualität der Datenübermittlung in digitalen Systemen zu verstehen, sei daher zunächst eine schematische Zeichnung zum Informationsfluss und eine Klassifizierung der Beteiligten gegeben (Abbildung 6).

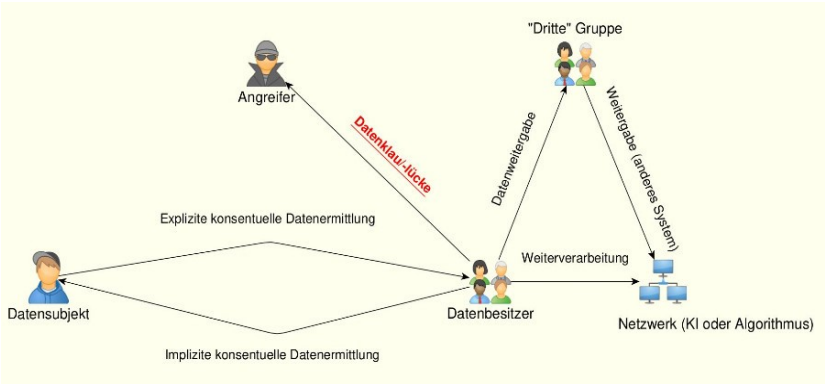

Abbildung 6. Vereinfachte Übersicht des Datenflusses und der Beteiligten, basierend auf der Privacy-Taxonomie von David Solove (2006, S. 490, Figure 1)

Wichtig ist dabei, dass der Begriff „Daten“ im Kontext von Privacy sich vorwiegend auf personenbezogene Daten bezieht, z. B. Name, Adresse, Geschlecht usw. Oder allgemeiner ausgedrückt auf Daten, die eine (natürliche) Person identifizierbar machen. Diese Unterscheidung ist deswegen wichtig, da es möglich sein soll, sensible Daten (z. B. gesundheitsbezogene) zu veröffentlichen, ohne dass ein Betroffener über den Datensatz identifiziert werden kann, z. B. indem Alter, Geschlecht und Adresse kombiniert werden.

Datensubjekt: Das zu beobachtende Subjekt, von dem Daten erhoben werden (implizite Datenerhebung) oder welches Daten explizit von sich gibt.
Datenbesitzer: Der *Datenbesitzer* (nicht zu verwechseln mit dem Dateneigentümer!) beschreibt die Instanz (wie Institution und Unternehmen), die für die Datensammlung zuständig ist. Unter Umständen können Datenbesitzer auch die Daten verarbeiten.
“Dritte” Gruppe: Ein zusätzlicher (dritter) Datenverarbeiter, der dieselbe Funktion ausübt bzw. Rechtsgrundlage benötigt wie der Datenbesitzer. Eine „dritte Gruppe“ könnte z. B. ein Unternehmen im EU-Ausland sein.
Angreifer: Jemand, der sich *unberechtigten* Zugang zu erhobenen Daten verschafft über Sicherheitslücken oder das Aushebeln von Sicherheitsvorkehrungen.

Die möglichen Interaktionen zwischen den Beteiligten sind:

Explizite konsensuelle Datenübermittlung: Dies beschreibt das Sammeln über explizite Formen der Datenerfassung, z. B. Formulare, Uploads, Fragebögen. Allgemein also Datenübermittlungen, die der Nutzer (Datensubjekt) *aktiv* anstoßen muss. In diesem Fall gibt er seine Einwilligung (eng. „consent") explizit.

Implizite konsensuelle Datenübermittlung: Dies beschreibt Methoden, die im Hintergrund sammeln, ohne dass es dem Nutzer unmittelbar bewusst ist, z. B. über Interaktionen wie das Klicken von "Like"-Buttons, das Abgeben von Kommentaren, das allgemeine Suchverhalten, die verwendeten Suchbegriffe, ggf. Video- und Audioaufzeichnungen. In der Informatik wird diese Art der Datenerhebung unter dem Begriff *data mining* zusammengefasst.

Datenweitergabe: Hiermit ist die Weitergabe von Daten an Dritte (z. B. zur Analyse, visuellen Aufbereitung) gemeint. Diese Weitergabe an *Dritte,* besonders an *Drittländer* ist gesetzlich geregelt [2, vgl. Kapitel V: Artikel 44–50].

Weiterverarbeitung beschreibt die über das Sammeln hinausgehende Verarbeitung. Gemeint sind lesende, schreibende, löschende oder analysierende Zugriffe. Besonderes Augenmerk liegt auf der Analyse, z. B. durch automatisierte Gesichtserkennungssoftware (vgl. biometrische Überwachung in Deutschland 2022) oder Verknüpfung von gesammelten Daten des „Datensubjekts" mit anderen Daten.

2. Aspekte von Privacy und deren moralische Probleme

Es wurde bereits darauf hingewiesen, dass sich der Begriff *Daten* im Kontext von Privacy vorwiegend auf *personenbezogene* Daten bezieht. Die im April 2016 verabschiedete so genannten Datenschutz-Grundverordnung (DSGVO; eng. GDPR: General Data Protection Regulation) der EU stellt ganz zu Beginn fest: „Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht". Insofern ist es konsequent, wenn Privacy im deutschen bzw. europäischen Recht auch das *Recht auf informationelle Selbstbestimmung* genannt wird. Was allerdings bedeutet das konkret? Hierbei muss man verschiedene Aspekte unterscheiden.

Ein hilfreiches Konzept zur Erklärung der allgemeinen Wichtigkeit der Zustimmung zur Übermittlung von Daten wurde von Helen Nissenbaum (2010) entwickelt. Sie spricht vom *framework of contextual integrity* (Nissenbaum 2010, S. 129ff.) Das Herzstück dieser kontextuellen Integrität bestimmt sich wie folgt: Zunächst bestreitet Nissenbaum, dass eine Information von Natur aus geheim oder privat ist. Die Behauptung, sie sei privat, ist *immer implizit kontextabhängig*. Neue Informationspraktiken sollten im Hinblick auf kontextbezogene Normen geprüft und nur dann akzeptiert werden, wenn sie die Ziele und Werte des betreffenden Bereichs besser fördern als die Alternativen (vgl. Nissenbaum 2010; Doyle 2011, S. 100).

Die kontextuelle Integrität besteht dann aus folgenden Bereichen:

(1) Kontext, in dem Informationen erfasst/analysiert/ausgetauscht werden,

(2) Akteure: Betroffener von Information,

(3) Attribute: Beschreibt den Typ von Information.

(4) Übermittlung: Wer übermittelt an Wen und Warum?

Gerade der (1) Kontext bezieht sich auf *soziale Sphären*, welche unterteilt sind in Bildung, Gesundheitswesen und Politik. Den Ausdruck *soziale Sphären* entlehnt Nissenbaum dabei von Michael Walzers Buch „Spheres of Justice“ (Walzer 2010). Für Walzer sollte die Stellung einer Person in einer sozialen Sphäre ihre Stellung in einer anderen Sphäre nicht beeinträchtigen. Gerade wegen einer „Nichtbeeinträchtigung“ ist die (4) Übermittlung so wichtig, da mit ihr *der Informationsfluss kontrolliert wird,* z. B. indem *vorhergehende Zustimmung des Akteurs* (consent) erforderlich ist.

Die Smart City stellt nun hinsichtlich der Übermittlung privater Daten bzw. hinsichtlich der Privacy einen spezifischen und besonders relevanten Fall dar, der viel diskutiert wird. Schon etwas älter ist ein Artikel von Lilian Edwards (2015), in dem sie Probleme und Lösungsstrategien hinsichtlich Privacy für den besonderen Fall der Smart Cities aufzeigt. Ihr Artikel stellt die Probleme in einem Vergleich von EU-Recht (DSGVO/GDPR) und US-Recht dar. Zunächst führt sie Smart Cities als Erweiterung von Online-Gemeinschaften (z. B. Facebook, Instagram, Foren) und Suchmaschinen (Google, DuckDuckGo) ein. Bei den Online-Gemeinschaften bewege sich die Informationsgesellschaft

in virtuellen Räumen, die von privaten Interessen kontrolliert würden, allerdings hätten diese Räume einen quasi-öffentlichen Charakter erlangt, vergleichbar zu Marktplätzen oder öffentlichen Bibliotheken, bei denen auch ein öffentlicher Austausch von Meinungen und Versammlungen stattfindet. In der Smart City hingegen funktioniere das gleichsam „umgedreht", da viele Bereiche des öffentlichen Lebens (Dorfplätze, Straßen, öffentlicher Nahverkehr, Gesundheits- und Polizeisysteme) entweder „privat betrieben oder zumindest mit privat betriebenen Sensoren ausgestattet werden, deren gesammelte Daten in privaten Datenbanken gespeichert werden." (Edwards 2015, S. 13, eigene Übersetzung). Demnach könnten wir von nun an auch von privat-öffentlichen Orten sprechen (Edwards 2015, S. 13: „The new PPP: Private-public-places").

Was sind die verschiedenen Aspekte, die hinsichtlich Privacy und Smart City in den gegenwärtigen Diskussionen als problematisch betrachtet werden?

- Internet of Things (IoT)

Dazu gehört *erstens* die prinzipielle Unmöglichkeit, *keine* Datenspur zu hinterlassen, wenn man am sozialen Leben teilhaben möchte. Es ist klar, dass wir uns von der Idee der Privatsphäre als physischen Orts verabschieden können. Ein zentraler Punkt bei der *Öffentlichkeit* von Smart Cities ist, dass die Preisgabe von Daten durch die Bewohner einer "intelligenten" Stadt einfach nicht zu vermeiden ist.[35] In anderen Worten: Bei einer Online-Plattform, wie Facebook oder einem Onlineshop, kann (theoretisch) auf Alternativen zugegriffen werden, beim öffentlichen Nahverkehr, Straßen, Parks, etc. in der Stadt nicht (vgl. Edwards 2015, S. 13f.). Dazu trägt auch die zunehmende Vernetzung von verschiedensten mit Sensoren ausgestatteten Dingen bei, die unter dem Stichwort „Internet of Things" (IoT) oder vor allem von Informatikern auch „ubiquitous computing" (ubicomp) diskutiert wird und selbstverständlich gerade in der Smart City von besonderer Relevanz ist. Das Internet of Things (IoT) beschreibt Edwards (2015, S. 11) als eine globale, un-

[35] Kelsey Finch und Omar Tene haben dieses Phänomen in Anlehnung an ein Panopticon einfallsreich Metropticon getauft. Vgl. Finch und Tene (2014)

sichtbare, vernetzte Umgebung, die durch die kontinuierliche Verbreitung von intelligenten Sensoren, Kameras, Software, Datenbanken und riesigen Datenzentren in einem weltumspannenden Informationsnetz entsteht. Das große Problem mit IoT ist, neben Sicherheitsproblemen (eng. security and safety problems), dass IoT als Werkzeug der allumfassenden Überwachung dienen kann. Das Hauptproblem für Privacy bei IoT ist, dass diese Geräte nur dann gut funktionieren, wenn sie im Hintergrund mit der Umgebung (oder uns) verschmelzen. Dieser Komfort geht aber mit der Aufgabe einer expliziten Einwilligung der persönlichen Datenweitergabe einher, die für unsere kontextuelle Integrität und Autonomie erforderlich wäre. Stellen wir uns vor, unsere Stadt ist mit Kameras und Sensoren ausgestattet, dann würde die gesamte Stadt zur sozialen Sphäre werden, wobei das dem Begriff (wie oben mit Walzer definiert) entgegenlaufen würde, da sich das Datensubjekt bewusst von Sphäre zu Sphäre „bewegen“ können sollte. Diese „Bewegung“ würde in einem Metropticon (einer überwachten Smart City) weniger bewusst vollzogen werden und, selbst wenn sie bewusst stattfindet, kann keine informierte Einwilligung (oder Ablehnung) über die Sammlung von Daten erteilt werden (Edwards 2015, S. 16f.).

Ein aktuelles (und leider reales) Beispiel ist Peking, dort hat der Künstler Deng Yufeng in einer Kunstaktion im Jahr 2021 in einem bestimmten Bezirk Kameras identifiziert und einen „unbeobachteten“ Weg erarbeitet, um herauszufinden, wie weit man sich, ohne von einer Kamera erfasst zu werden, durch die Stadt bewegen kann. Im Ergebnis hat Yufeng gemeinsam mit einigen Freiwilligen für einen Weg von 1 Kilometer ca. 2 Stunden benötigt. Dieses Werk durfte er innerhalb China nicht veröffentlichen (vgl. Tamara et al. 2021, 11:00-14:30 min).

- Big Data

Das *zweite* Problemthema ist „Big Data“; ein Modewort, das mit Volumen, Geschwindigkeit und Vielfalt von Daten verknüpft wird. Gerade in Zeiten von günstigem Speicherplatz und immer besser werdenden *data mining* Techniken zur Analyse von großen Datenmengen wird das Thema zunehmend relevant. Da es sich hier häufig um persönliche Daten handelt, ist das Thema Big Data vor allem für den Aspekt der Privacy wichtig.

Der Ausdruck Big Data verrät bereits eine wichtige Eigenschaft derselben: die Datenmengen müssen immens sein, damit die Versprechen funktionieren. Es geht nicht nur um Antworten über die „bekannten Unbekannten" (eng. „known unknowns"), z. B. Korrelation bekannter Datensätze, sondern auch über die „unbekannten Unbekannten" (eng. „unknown unknowns") (vgl. Borne 2013). Die DGSVO/GDPR versucht den Schutz des Individuums vor diesem Hintergrund hauptsächlich über *Zweckbindung, Datenminimierung* und *Speicherbegrenzung* (DGSVO, Art. 5) zu gewährleisten. Hier allerdings treten weitere Folgeprobleme auf.[36]

Zweckbindung steht im Widerspruch zu Big Data, aufgrund der unbekannten Unbekannten und der Tatsache, dass die meisten innovativen Ideen zum Zeitpunkt der Datenerfassung und -analyse noch gar nicht erkannt sind.

Grundsätzlich muss die Erhebung von Daten gemäß dem Grundsatz der *Datenminimierung* erfolgen. Das heißt: „Personenbezogene Daten müssen [...] dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung")" (DGSVO, Art. 5–1c). Allerdings ergeben sich bei einer nicht näher bestimmten oder sehr weiten Interpretation vom Zweck erneut Probleme. Gerade, weil die Auffassung: *„alles was mit personenbezogenen Daten möglich ist, soll auch gemacht werden"* in der Tendenz steigend ist.

Die *Speicherbegrenzung* bezieht sich auf die Dauer, „die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;" (DGSVO, Art. 5–1e). Allerdings gilt diese Einschränkung nicht, wenn die Daten richtig anonymisiert sind; dann können Daten beliebig lang aufbewahrt werden. Dazu ist anzumerken: Abgesehen davon, dass es unter technischen Fachleuten keine Einigkeit darüber gibt, was die richtige Technik zur Anonymisierung ist, bietet diese auch keinen vollständigen Schutz

[36] Probleme, die im Folgenden nicht behandelt werden, sind: algorithmische Transparenz und algorithmische Diskriminierung, sowie eine ökologische Betrachtung von Big Data, die meist zu kurz kommt. Diese Probleme werden hier nicht weiter behandelt, da für sie andere Grundwerte „zuständig" sind.

vor Identifizierung (eng. „singled out“) des Individuums. Überdies kann algorithmische Diskriminierung auch von anonymen Bürgern (bzw. Profilen) stattfinden (vgl. Edwards 2015, S. 20-25).

Etwas salopp ausgedrückt kann man die Probleme von Big Data für die Privacy wie folgt fassen: Knicken wir vor den Versprechungen von Big Data ein, so muss sich der Datenschutz auf die zweite Linie der Verteidigung, also auf die Einschränkung der Verarbeitung zurückziehen. Das heißt konkret, dass zunächst alle Daten anonymisiert (wo sinnvoll) zu sammeln sind und dann eine (hoffentlich transparente) Auswertung, Verteilung und Weiterverarbeitung durch den Datenbesitzer zu erfolgen hat. Allerdings wird es schwierig sein, ab diesem Zeitpunkt einen Konsens darüber zu finden, welche Verwendungen besonders *schädlich* sind oder sein können (vgl. Edwards 2015, S. 25). Dabei kann man allerdings wieder auf die kontextuelle Integrität zugreifen, indem das Datensubjekt definiert, welche Daten es in diesem spezifischen Kontext erfasst haben will. Zusätzlich sollten Domänenexperten (z. B. Mediziner) unveräußerliche Verwendungszwecke oder zu erfassende Datenpunkte domänenspezifisch in Ergänzung zur Autonomie definieren (vgl. Nissenbaum 2019).

- Transparenz

Als drittes Thema ist Transparenz in Bezug auf Privacy anzusprechen. Diese kann in zweierlei Hinsicht verstanden werden:

> (1) Transparenz bzw. Offenheit des gesammelten Datenmodells für die Datensubjekte.
>
> (2) Der Datenbesitzer muss seine Verarbeitung und Zwecke den Datensubjekten offenlegen.[37] Nur dadurch kann das Vertrauen zwischen beiden Parteien, also Datensubjekt und Datenbesitzer wachsen. Eine Datenschutzfolgeabschätzung (sofern vorhanden) muss ebenfalls dem Datensubjekt *verständlich* gemacht werden, damit sich der Nutzer über Risiken eines Datendiebstahls bzw. Datenverlustes bewusst ist.

[37] Allerdings ist hierbei zu beachten, dass die Verarbeitung im Bereich der künstlichen Intelligenz eine gewisse Schwierigkeit mit sich bringt, wobei hier auf „explainable AI” (XAI) gesetzt werden sollte.

- Partizipation

Partizipation tangiert Privacy im Kontext von personalisiertem „Adtargeting", z. B. über Social Media. Weitere Beispiele sind die personalisierten Werbekampagnen von Cambridge Analytica oder so genannte, durch Überwachung ausgelöste „chilling effects" (Verhaltensanpassung an eine Norm, vgl. Solove 2006, S. 487). Bei diesem „klassischen" Problem kann sich das Verhalten der Überwachten ändern (eng. „chilled"), wodurch sich beispielsweise die Teilnahme bei Protesten verringert oder populäre Ansichten seltener kritisiert werden. Es spielt dabei im Übrigen keine Rolle, ob sich die Person der Überwachung bewusst ist oder nicht. Bewusste permanente Überwachung kann zudem Gefühle der Angst und des Unbehagens beim Überwachten auslösen (Solove 2006, S. 493ff.). Es versteht sich mehr oder weniger von selbst, dass derartige Effekte bzw. auf der nicht-konsensuellen Auswertung von privaten Daten basierende „Anwendungen", die letztlich mit einer Verletzung der Privatsphäre gleichen, aus moralphilosophischer Sicht abzulehnen sind.

3. Aspekte von Privacy und deren Beitrag zum guten Leben

Neben den geschilderten moralisch problematischen Aspekten beim Thema Privacy gibt es auch einige positive Aspekte bzw. Entwicklungen, die hier Erwähnung finden sollen. In den letzten Jahren ist sowohl in der Wissenschaft als auch bei der allgemeinen Bevölkerung die Sensibilität für Privacy gestiegen. Das ist grundsätzlich positiv zu bewerten. Ihren Niederschlag findet das gewachsene Bewusstsein für die Wichtigkeit von Privacy zum einen in entsprechenden Gesetzen und zum anderen in der Entwicklung von datenschützenden Programmen und Anwendungen. Entsprechend kann man zwischen Privacy by Law (durch Gesetze gesicherter Datenschutz) und Privacy by Technology (durch Technik gesicherter Datenschutz) unterscheiden.

- Durch Gesetze gesicherter Datenschutz (Privacy by Law)

Ein Beispiel für gesetzliche Regelungen zur Förderung von Privacy ist die schon mehrfach erwähnte, 2016 europaweit eingeführte Global Data Protection Rule bzw. Datenschutz-Grundverordnung (GDPR/DGSVO).

Aber auch außerhalb Europas wächst das Datenschutz-Bewusstsein. So hat selbst China am 1. November 2021 sein eigenes Gesetz zum Schutz von Privacy erlassen: Personal Information Protection Law (PIPL). Allerdings gilt die PIPL nur für in- und ausländische Unternehmen und dem Schutz von Kunden. Das Social-Credit-System der Regierung, das auf einer weitgehenden Überwachung aller Aktivitäten der Bürger beruht, gilt also weiterhin. In den USA bzw. für kalifornische Konsumenten gilt seit 2018 ein vergleichbares Gesetz: California Consumer Privacy Act (CCPA),[38] welcher zumindest Lese-, Löschrechte, sowie das Recht, dem Verkauf ihrer persönlichen Daten zu widersprechen, und ein Recht auf Nicht-Diskriminierung ermöglicht. Es gibt allerdings Ausnahmen, etwa beim Verkauf von persönlichen Daten. Dabei sollte die eigentliche Frage sein: Warum ist es nicht andersherum? Warum also sollte ein Unternehmen sich das Recht auf Verkauf der Kundendaten nicht explizit beim Kunden holen müssen, so wie es beispielsweise in der DGSVO/GDPR geregelt ist (DGSVO, Art. 25: privacy by default)?

- Durch Technik gesicherter Datenschutz (Privacy by Technology)

Eine weitere positive Entwicklung lässt sich auf technischem Gebiet feststellen. So gibt es mittlerweile einige Programme und anderweitige Anwendungen, die den Datenschutz bzw. Privacy explizit in den Mittelpunkt stellen und damit zu einer Art Geschäftsmodell bzw. Alleinstellungsmerkmal machen. Die Idee ist dabei sehr einfach, nämlich explizit für den Datenschutz sensible Nutzer anzusprechen und diese zu eigenen Kunden zu machen. Beispiele sind: Signal, DuckDuckGo oder Brave (Webbrowser).

Signal[39] ist ein Messenger mit starkem Fokus auf Privacy. Alle Nachrichten zwischen Benutzern sind von Ende-zu-Ende verschlüsselt und die einzigen Informationen, die für jedes Benutzerkonto auf den Signalservern gespeichert werden, sind die registrierte Telefonnummer, das Eintrittsdatum bzw. das Datum der Benutzerregistrierung und das letzte bzw. aktuellste Anmeldedatum am Benutzerkonto. Zu den Infor-

[38] Vgl. dazu https://oag.ca.gov/privacy/ccpa, letzter Aufruf: 12.01.2023
[39] https://signal.org/de/, letzter Aufruf 12.01.2023

mationen, die nicht gespeichert werden, gehören insbesondere Kontakte, Kontaktinformationen, Gruppen des Benutzers oder Aufzeichnungen darüber, mit welchen Benutzern kommuniziert wurde.[40] Signal ist also ein Messenger, bei dem die Kommunikation nur zwischen den Beteiligten abläuft und der Dienstanbieter (fast) keine Informationen über die Kommunikation hat. Hier bleibt die Privacy der Benutzer gewahrt.

DuckDuckGo[41] ist eine Internet-Suchmaschine, die sich selbst mit folgendem Slogan bewirbt: „Your personal data is nobody's business. [...] For everyone who's had enough of online tracking, DuckDuckGo lets you take back your online privacy now."[42] Sie existiert seit ca. 2008 und seither sind noch eine Menge verschiedener Services hinzugekommen, z. B. ein „Protect your Inbox"[43] (E-Mailschutz). Genauer gesagt ist „DuckDuckGo Email Protection" ein kostenloser E-Mail-Weiterleitungsdienst, der verschiedene Arten von versteckten E-Mail-Trackern entfernt und einem Nutzer die Möglichkeit gibt, eine unbegrenzte Anzahl von einzigartigen privaten E-Mail-Adressen zu erstellen.[44]

Am 13. September 2022 sandten DuckDuckGo zusammen mit anderen „privacy-focused" Technologieunternehmen einen Brandbrief an mehr als 100 Mio. amerikanische Nutzer, um den „American Innovation and Choice Online Act (AICOA)" zu unterstützen, damit dieser sich zu einem schnellen Abschluss finde.[45] Sie fassten die Probleme rund um Privacy am „freien" Markt gut zusammen:

> Our companies and organizations offer privacy protective alternatives to the services provided by dominant technology companies. While more and more Americans are embracing privacy-first technologies, some dominant firms still use their gatekeeper

[40] vgl. https://restoreprivacy.com/secure-encrypted-messaging-apps/signal/, letzter Aufruf 01.01.2023
[41] benutze Suchmaschine über https://duckduckgo.com/
[42] vgl. https://duckduckgo.com/about, letzter Aufruf: 12.01.2023
[43] vgl. https://duckduckgo.com/email/
[44] vgl. https://www.spreadprivacy.com/protect-your-inbox-with-duckduckgo-email-protection/, letzter Aufruf 12.01.2023
[45] vgl. https://spreadprivacy.com/privacy-companies-call-for-vote/, letzter Aufruf 12.01.2023

> power to limit competition and restrict user choice. [...]
> Massive tech platforms can exert influence over society and the digital economy because they ultimately have the power to collect, analyze, and monetize exorbitant amounts of personal information. This is not by accident, as some of the tech giants have intentionally abused their gatekeeper positions to lock users into perpetual surveillance while simultaneously making it difficult to switch to privacy-protective alternatives.[46]

Gerade der letzte Punkt, nämlich der Wechsel zu „privacy-focused“ Unternehmen, ist zwar mit Hindernissen verbunden, aber durchaus möglich, wie die Beispiele von Signal, DuckDuckGo oder Brave[47] zeigen. Die Entscheidung für einen Service und damit gegen Privacy ist also nicht zwingend. Beides kann bei Kommunikation (Signal) und Suche (Brave, DuckDuckGo) zusammengehen. Hinsichtlich des Bereichswertes Privacy sind die genannten Beispiele positiv zu werten und sie bilden eine Grundlage für Diskussionen und Entwicklung von und für Technologien in der Smart City.

4. Offene Fragen

Bereits eingangs wurde die Taxonomie (vgl. Abbildung 6) von David Solove (2006, S. 490f.) zur Beschreibung der Systematik von Datenübermittlungen im digitalen Raum aufgegriffen. Diese und die hier angeführte Abbildung 7 ermöglichen dem Anwender ein systematisches Nachdenken über Privacy-Probleme. Besagte Taxonomie enthält bereits viele Elemente, die unter anderem Namen in der DGSVO/GDPR ebenfalls Einzug genommen haben. So wird z. B. dem *secondary use* (= Zweitverwendung, ohne Einwilligung) durch die „Zweckbindung“ (DGSVO, Art. 5-1) entgegengewirkt. Im Folgenden sind anstelle eines Fazits oder Ausblicks weitere Fragen zusammengestellt, die ein

[46] vgl. https://spreadprivacy.com/privacy-companies-call-for-vote/, letzter Aufruf 12.01.2023

47 Ein Webbrowser mit starkem Fokus auf Privacy (inkludiert Abwehr gegen u. a. Tracking, Malware und Phishing). Diesen gibt betriebssystemübergreifend seit 2016: https://brave.com/

Bewusstsein von Privacy, über die Verwendung der DGSVO/GDPR hinaus, schaffen können und auch in der App zur Einschätzung moralischer Probleme der Smart City hilfreich sein dürften.

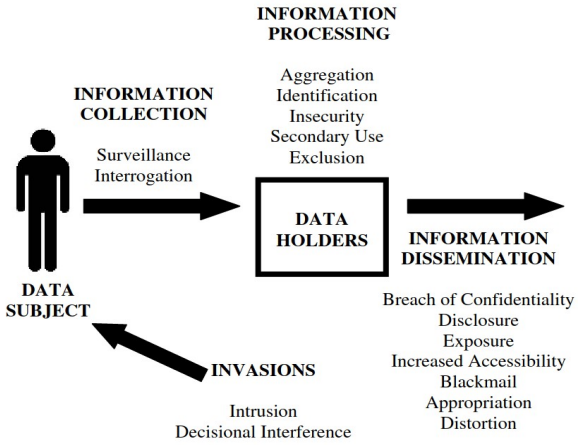

Abbildung 7. Privacy-Taxonomie aus der Sicht des Überwachten in grafisch aufbereiteter Form. (Vgl. Solove 2006, S. 490, Figure 1)

Die *Fragetypen* sind dabei binär (0 = nein oder 1 = ja), komparativ ({0, 1, 2, ..., 10}) oder qualitativ (z.B. freie Textantworten, Mehrfachantworten). Wenn in den Fragen von *Daten* die Rede ist, wird meist von *personenbezogenen (nicht anonymisierten) Daten* ausgegangen. Bei jeder Frage ist versucht, ihr Ziel in der DGSVO/GDPR und in der Privacy-Taxonomie (vgl. Abbildung 7) von David Solove abzubilden.

1. Wird die DSGVO bzw. GDPR eingehalten? (Fragetyp: *binär*, Privacy-Taxonomie: *keine Angabe*, GDPR-Artikel: *keine Angabe*)
   Erläuterungen (inkl. Beispiele): Es gibt eine Datenschutzerklärung und Zweckbindung, zu denen der Benutzer zugestimmt hat.
2. Sind personenbezogene Daten vor unbefugtem Zugriff geschützt? (Fragetyp: *binär*, Privacy-Taxonomie: *Insecurity*, GDPR-Artikel: *6, 32*)
   Erläuterungen (inkl. Beispiele): Geeignete technische und organisatorische Maßnahmen treffen, z.B. Verschlüsselung der Daten und Zugriffminimierung.

3. Werden Daten richtig anonymisiert? (Fragetyp: *qualitativ (Mehrfachantwort)*, Privacy-Taxonomie: *Identification, Aggregation*, GDPR-Artikel: *25, 32*)
Erläuterungen (inkl. Beispiele): Werden technische Maßnahmen wie Pseudonymisierung oder Differential-Privacy benutzt, um Daten vor Linking-Angriffen zu schützen?
4. Welche Art von Zugriff hat der Nutzer bzw. Datensubjekt auf seine Daten? (Fragetyp: *qualitativ (Mehrfachantwort: Lesen, Ändern, Löschen)*, Privacy-Taxonomie: *keine Angabe*, GDPR-Artikel: *12–22*)
5. Werden für den Zweck des Projektes unnotwendige Daten erhoben? (Fragetyp: *binär*, Privacy-Taxonomie: *Information Collection, Aggregation*, DGSVO-Artikel 5)
Erläuterungen (inkl. Beispiele): Es sollten nur Daten, die für den Zweck notwendig sind, erhoben werden. Der Zweck muss so konkret und verständlich wie möglich beschrieben werden. (Stichwörter: Zweckbindung, Datenminimierung, DGSVO-Artikel: 5-1)
6. Wird beim Erfassen der Daten *privacy by default* angewandt? (Fragetyp: *binär*, Privacy-Taxonomie: *Information Collection*, GDPR-Artikel: *5, 7, 8, 11, 25*)
Erläuterungen (inkl. Beispiele): Voreinstellungen bei der Datenerfassung und -verwaltung sind *standardmäßig,* also ohne Aufwand des Benutzers, im Sinne des Benutzers. Mögliche Maßnahmen: keine „dark patterns“ im Design, keine unnötigen Unterbrechungen des Dienstes für die Datenerfassung.
7. Wird der Schutz des Individuums gewährleistet, bei einer Datenweitergabe *nach Außen?* (Fragetyp: *qualitativ,* d.h. *offen, Mehrfachantwort)*, Privacy-Taxonomie: *Appropiation*, DGSVO-Artikel: 35)
Erläuterungen (inkl. Beispiele): Diese Frage zielt auf den Schutz einer Person vor einem falschen oder verzerrten Bild in der Öffentlichkeit ab, z. B. durch Datenverlust oder Werbung, wobei Daten eines Individuums oder einer Gruppe nach Außen gegeben werden (vgl. „Datenschutz-Folgeabschätzung“, DGSVO, Art. 35).
8. Liegt eine Datenschutz-Folgeabschätzung vor? (Fragetyp: *binär*, Privacy-Taxonomie: *Information Dissemination*, DGSVO-Artikel: 35)

9. Werden die erfassten Daten *regelmäßig auf Richtigkeit* überprüft? (Fragetyp: *komparativ (Zeitperiode (inklusive 0))*, Privacy-Taxonomie: *Distortion*, GDPR-Artikel: *keine Angabe*)
Erläuterungen (inkl. Beispiele): Die Richtigkeit kann entweder durch den Benutzer bzw. Datensubjekt selbst erfolgen oder muss vom Datenbesitzer selbst übernommen werden. (sinngemäß nach Erwägungsgrund DGSVO Art. 39). Mit der Richtigkeit sollen z. B. Fake-News und Verleumdungen eingedämmt werden.
10. Bis zu welchem Grad ist dem Projektteam *Privacy by Design* bekannt? (Fragetyp: *komparativ*, Privacy-Taxonomie: *all*, GDPR-Artikel: *keine Angabe*)
Erläuterungen (inkl. Beispiele): Diese Frage zielt darauf ab, den Bekanntheitsgrad bzw. das Bewusstsein darüber im Projektteam abzufragen, ob *Privacy by Design* als gesamtes Konzept bekannt ist.
11. Bis zu welchem Grad wird während des Projekts *Privacy by Design* praktiziert? (Fragetyp: *komparativ*, Privacy-Taxonomie: *all*, GDPR-Artikel: *keine Angabe*)
Erläuterungen (inkl. Beispiele): Diese Frage zielt darauf ab, die Anwendung von *Privcacy by Design* während des Projekts sicherzustellen.

Literaturverzeichnis

Anthony, T., Bölinger, M., Eckert, S. und Satra, D. (2021) „China - Überwachungsstaat oder Zukunftslabor?“ Weltbilder. https://www.ardmediathek.de/video/weltbilder/china-ueberwachungsstaat-oder-zukunftslabor/ndr/Y3JpZDovL25kci5kZS8wNmJjZDc1OS02ZDI5LTRhZWItODNjMi03YzBhMmM3NWFlOWE

Borne, K. (06.04.2013) „Big Data, Small World: Kirk Borne at TEDxGeorgeMasonU“. You Tube. https://www.youtube.com/watch?v=Zr02fMBfuRA

Doyle, T. (2011) „Helen Nissenbaum. Privacy in Context: Technology, Policy, and the Integrity of Social Life“. *The Journal of Value Inquiry* 45 (1), 97–102. https://doi.org/10.1007/s10790-010-9251-z

EU (2016) *EU-Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DatenschutzGrundverordnung)*. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=EN (zuletzt aufgerufen am 07.12.2022).

Edwards, L. (2015) *Privacy, Security and Data Protection in Smart Cities: a Critical EU Law Perspective*. https://doi.org/10.5281/zenodo.34501 (zuletzt aufgerufen am 01.08.2023)

Finch, K. und Tene, O. (2014) „Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town“. *Fordham Urban Law Journal* 41(5), 1581-1615.

Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

Nissenbaum, H. (2019) „Helen Nissenbaum on Post-Consent Privacy“. You Tube. https://www.youtube.com/watch?v=CPKo1ThUkZE

Rössler, B. (2001) *Der Wert des Privaten*. Frankfurt am Main: Suhrkamp.

Solove, D. J. (2006) „A Taxonomy of Privacy“. *University of Pennsylvania Law Review* 154(3), 477–564.

Solove, D. J. (2008) *Understanding Privacy*. Cambridge, MA [u.a.]: Harvard University Press.

Walzer, M. (2010) *Spheres of Justice: A Defense of Pluralism and Equality*. NewYork: Basic Books.