

Debra Hevenstone, Oliver Hümbelin, Fabienne Kaiser, Barbara Waldis

Arbeitsgruppe der Fachkommission «Digitalisierung und Soziale Arbeit»

Dateninnovationen und Datenschutz in der Sozialen Arbeit

Unsere Arbeitsgruppe interessiert sich dafür, wie Daten von Praxisorganisationen besser für die Arbeit der Sozialen Arbeit genutzt werden können. Wie kann dabei die im Zuge der Digitalisierung entstehende Datenflut nutzbar gemacht werden ohne Personenrechte zu verletzen?

Heute werden viele Daten erfasst sei dies für Statistiken oder im Zuge der Abwicklung von administrativen Abläufen. Diese Informationen werden aber für Dateninnovationen der Praxis wenig genutzt. Dies liegt einerseits an rechtlichen Hürden, aber auch an mangelnden Möglichkeiten der Praxisorganisationen Innovationsprojekte voranzutreiben. Was wissen wir darüber, welche Daten in Praxisorganisationen gesammelt werden? Wie werden sie bisher genutzt? Wie können sie mit innovativen Techniken einen Mehrwert für die Soziale Arbeit schaffen?

Bei der Nutzung der Daten ist dabei der Schutz individueller Rechte der Adressat:innen und der Professionellen entscheidend. Wie kann auf Organisationsebene die Verantwortung ohne Bevormundung wahrgenommen werden? Wer muss wann vor wem geschützt werden? Wie ist der Schutz im Vergleich zur Niederschwelligkeit eines Angebotes zu werten? Welche Anforderungen an Datenschutz sind nötig? Wie können wir den Datenschutz wirkungsvoll und einfach in die forschende und reflektierende Berufspraxis einbeziehen?

Für die Arbeitstagung im September besteht die Idee, mit 3-4 Fachleuten (Bundesamt für Statistik, Datenschutzbeauftragte, Dienstleister der Sozialen Arbeit) die obigen Themen zu diskutieren, allenfalls anhand eines spezifischen Projektes.

Interessierte melden sich bei einem Mitglied der Arbeitsgruppe

DH, OH, FK, BW, 18.5.22

4) Soziale Arbeit pflegt einen sensiblen und bewussten Umgang mit Informationen und Daten

Digitalisierung bedeutet auch Akkumulation und die Verknüpfung von personenbezogenen Informationen und Daten. Soziale Arbeit ist oftmals mit Menschen in schwierigen Lebenssituationen befasst und erhält vertrauliche Informationen. Soziale Arbeit ist sich dessen bewusst und begegnet der Thematik wachsam und mit erhöhter Sensibilität, insbesondere im Bereich der digitalen Kommunikation mit verschiedenen Anspruchsgruppen. Neu dabei ist, dass die digitalen Datenkörper als „erweiterte Körper“ durch Smartphones, Wearables usw. zum Individuum gehören. Diese Mensch-Medien-Kopplung sowie die Entwicklung u.a. prädiktiver Verfahren sowie der künstlichen Intelligenz wird damit auch zum Gegenstand der Sozialen Arbeit.

Die Thematik des sensiblen und bewussten Umgangs mit Informationen und Daten in der Sozialen Arbeit, führt zu grundlegenden Fragen der Sicherheit von KlientInnen und Sozialarbeitenden. Diese werden jeweils dann diskutiert, wenn eine Person oder eine Gruppe eine Situation als problematisch und als existenzielle Bedrohung auffasst (Bozzini, 2017). Eine spezifische Bedrohung der Sicherheit muss in der Öffentlichkeit breit diskutiert sein, damit Vorstellungen darüber entstehen, wie mit dieser Bedrohung umzugehen ist. Beim Thema digitale Sicherheit ist das in der Sozialen Arbeit kaum der Fall.

Bei der täglichen Nutzung von Applikationen oder Programmen, von Internet, von Smartphones, von sensor- oder computergestützten Geräten am Körper, oder von digital gestützten Analysen steht der Nutzen der Anwendung im Vordergrund. Natürlich sind Geräte und Anwendungen passwortgeschützt und insofern gesichert. Nur werden neben Telefonnummern, Sprachnachrichten, Musikpräferenzen oder Herzfrequenzen beispielsweise auch die Art, digitale Medien zu benutzen oder die gesuchten Begriffe im Netz gesammelt. Jede Bewegung im Netz gibt über Neigungen und Eigenschaften einer Person Auskunft. Das schafft Möglichkeiten für weitere Verfahren mit Metadaten, aber auch Unsicherheit. Diese wird dadurch verstärkt (Bozzini 2016), dass jedes Gerät, Programm oder Applikation über Schlupflöcher für externe Kontrollen verfügt; die Anwendenden kaum genau um Sicherheitsmängel wissen; und unklar ist, was wichtige Informationen sind. Im Bereich digitaler Sicherheit besteht also ein Paradox zwischen zunehmender Notwendigkeit die

eigenen Daten zu schützen einerseits und andererseits der wachsenden Menge versteckter, für die Anwendenden selbst unkontrollierbarer digitaler Daten.

In Anbetracht dieser latent konstant vorhandenen Unsicherheit ist es nur ein kleiner Trost, wenn laut der Europäischen Datenschutzverordnung (2018) Konsumierende insbesondere das Recht haben, Informationen über gesammelte Daten oder das Löschen dieser Daten verlangen zu können. Ähnlich limitiert sind die Auswirkungen zu «besonders schützenswerten Personendaten» im Schweizerischen Bundesgesetz über den Datenschutz (1992; Art.3 lit. c DSG). Damit sind folgende Bereiche bezeichnet: religiöse und gesellschaftspolitische Ansichten; Daten zur Gesundheit und zu ethnischer oder sexueller Zugehörigkeit; Massnahmen der sozialen Hilfe; administrative oder strafrechtliche Sanktionen. Die Frage stellt sich, wie digitale Sicherheit in der Sozialen Arbeit diesbezüglich gehandhabt wird für Analysen und Forschungen mit digitalen Daten.

Was bedeutet es weiter für Sozialarbeitende in der Berufspraxis mit digitalen Daten bewusst umzugehen, angesichts der Unmöglichkeit den Datenfluss und deren Verwendung zu kontrollieren, respektive diesen selbst zu benutzen? Neben dem eigenen, privaten Bereich sind Sozialarbeitende bei ihrer Arbeit insbesondere in folgenden Gebieten mit digitaler Sicherheit konfrontiert: im mündlichen und schriftlichen Kontakt; bei der Dokumentation der Arbeit mit der Klientel; beim Verwenden von Metadaten; und bei der interinstitutionellen Zusammenarbeit.

Grundsätzlich sollen bei den Handlungsstrategien die Sicherheitsrisiken für die Klientel aber auch für die Sozialarbeitenden so klein wie möglich sein. Erstens ist fortlaufend erweiterte digitale Nutzungskompetenz der Sozialarbeitenden gefragt, damit sie die digitalen Medien, die sie verwenden, sichere Software, open source Programme oder wearables, gut kennen und bestmögliche Sicherheitsstandards einsetzen. Zweitens sind Niederschwelligkeit eines Angebotes, Nutzen und Sicherheitsrisiko für die Klientel gegeneinander abzuwägen. Drittens ist Notwendigkeit und Verhältnismässigkeit des Einsatzes digitaler Medien oder digitaler Analysen zu überlegen, wobei das kleinstmögliche Risiko für die Klientel auch bedeuten kann, auf digitale Medien zu verzichten.

(M.Doerk, A.Huber, M.Luginbühl, S. Sierra Barra, P.Stade, O.Steiner, B.Waldis (2022), «Soziale Arbeit und Digitalisierung: Sechs Thesen», *Unsere Jugend*, Jg. 74, 3, S. 102-114)