

Datenschutz und Anonymisierung von qualitativen Forschungsdaten

Das Teilen von Forschungsdaten wird seit einiger Zeit von Forschungsförderern wie dem Schweizerischen Nationalfonds (SNF), Fachgesellschaften aber auch Verlagen gefördert. Im Sinne der leichten Nachvollziehbarkeit sowie einfachen Nachnutzung von Forschungsergebnissen wird nahegelegt, Forschungsdaten so offen wie möglich und so geschützt wie ethisch und rechtlich nötig zugänglich zu machen.

«Der SNF erachtet den offenen Zugriff auf Forschungsdaten als einen wesentlichen Beitrag zur Wirkung, Transparenz und Reproduzierbarkeit wissenschaftlicher Forschung. Forschungsdaten sollten aus Sicht des SNF nicht nur sorgfältig aufbereitet und archiviert, sondern auch so weit wie möglich zugänglich gemacht werden. Deshalb erwartet der SNF von allen von ihm geförderten Forschenden, dass sie [...] diese Daten anderen Forschenden zugänglich machen, sofern dem keine rechtlichen, ethischen oder urheberrechtlichen Gründe, Vertraulichkeitsklauseln o. ä. entgegenstehen [...].»

Aus der [Grundsatzklärung des SNF zu Open Research Data](#).

Doch wann sind Daten schützenswert und was ist ein ausreichender Schutz? Welche datenschutzrechtlichen Vorgaben müssen Forschende berücksichtigen, wenn sie Forschungsdaten erheben, bearbeiten und teilen? Wie können sie die InterviewpartnerInnen oder TeilnehmerInnen der Feldbeobachtung gut schützen ohne das Potential ihres Forschungsmaterials und Chancen für Folgeprojekte zu minimieren? Diese Fragen schaffen bei den Forschenden oft Unsicherheiten. Die Universität und UB Basel sowie die UB Bern haben vor diesem Hintergrund zu einem Workshop mit Forschenden sowie Experten und Expertinnen aus den Bereichen Datenschutz und Informationssicherheit eingeladen. Vier beispielhaften Forschungsprojekte haben sich kurz vorgestellt und ihre Fragen und Probleme in Bezug auf den Datenschutz formuliert. Anschliessend haben die Experten ihre Einschätzung gegeben, gemeinsam mit allen Teilnehmenden die zentralen Fragen diskutiert und mögliche Lösungen aufgezeigt.



Die Beteiligten am Workshop kamen aus unterschiedlichsten wissenschaftlichen Disziplinen, darunter DatenschutzexpertInnen, WissenschaftlerInnen aus den Geistes- und Sozialwissenschaften sowie aus dem Team Forschungsunterstützung der UB Basel

Im Anschluss an die Diskussionen im Plenum hatten dann alle Teilnehmenden die Möglichkeit ihre zentralen Fragen in Kleingruppen gemeinsam mit den Expertinnen und Experten zu diskutieren und mögliche Antworten für ihre eigenen Projekte zu finden. Ziel war es Forschende mit den Rechtsexperten in Kontakt zu bringen, um zum einen möglichst viele Fragen zu klären und zum anderen zu dokumentieren, in welchen Fällen für die qualitative Forschung besonders Probleme durch den Datenschutz entstehen, welche Unterstützung die Forschenden benötigen und wo Klärungsbedarf auch von Seiten der Universität besteht.

Themenschwerpunkte des Workshops

1. Anonymisierung von Personendaten – die einfache Lösung?

Entfernt man sämtliche personenbezogenen Informationen aus den Daten, so dass eine Identifikation der untersuchten Personen nicht mehr möglich ist, spricht man von Anonymisierung. Absolut anonymisierte Daten unterliegen nicht mehr dem Datenschutz, das Forschungsmaterial kann also uneingeschränkt bearbeitet und publiziert werden. Ein Haken an der Sache ist, dass die Anonymisierung irreversibel sein muss, was heutzutage nicht mehr so einfach garantiert werden kann. Die Kombination der Daten mit anderen Datenquellen ist einfacher geworden und so ist eine Re-Identifizierung von Personen leichter möglich als noch vor 20 Jahren. Zudem läuft die technologische Entwicklung schneller und Daten, die heute als anonym gelten, können in 5 Jahren vielleicht ganz einfach re-anonymisiert werden.

Ein weiteres Problem ist, dass das erhobene Material in anonymisierter Form für die Forschung unbrauchbar sein kann. Beschäftigt sich die Forschungsfrage beispielsweise mit der

Kommunikation einer bestimmten Personengruppe, ist auch die Mimik und Gestik der Personen relevant. Um aber beispielsweise Videomaterial von der untersuchten Personengruppe zu anonymisieren, müssten die Gesichter der Personen unkenntlich gemacht werden, wodurch die Mimik und Blickrichtung der Personen nicht mehr erkennbar ist.



Anonymisierte Daten können für die Forschung unbrauchbar werden. Personen lassen sich jedoch häufig aus Kontextinformationen identifizieren, auch wenn direkte Identifikatoren entfernt wurden.

Sehr schwierig und aufwendig ist auch die Anonymisierung von qualitativen Interviews. Diese enthalten häufig viele biografische oder andere identifizierende Angaben, die nicht automatisiert entfernt werden können. Insbesondere wenn Untersuchungen zu den Lebensumständen von Personengruppen durchgeführt werden, sind solche biografischen Daten für die Beantwortung der Forschungsfrage auch relevant. Häufig sind Personen nicht aus direkten, sondern aus Kontextinformationen identifizierbar. Wenn die untersuchte Personengruppe sehr klein ist, kann eine Anonymisierung schier unmöglich werden. Beispielsweise wenn Untersuchungen innerhalb einer Institution stattfinden oder unter der strengen Aufsicht von totalitären Regimen durchgeführt werden.

2. Informierte Einwilligung

Ein Weg, wie man auch mit den Personendaten arbeiten kann ohne sie vollständig anonymisieren zu müssen, ist das Einholen einer Einwilligung von den betroffenen Personen. Hierbei sind unter anderem folgende Spielregeln zu beachten:

- Die betroffene Person muss vollständig darüber informiert werden, welche Daten zu welchem Zweck und in welcher Form erhoben und bearbeitet werden. Wenn eine Publikation oder Archivierung der Daten nach dem Projekt geplant ist, muss die betroffene Person auch darüber informiert werden, denn in juristischen Sinn ist auch dies ein «Bearbeiten von Daten».
- Die Einwilligung muss so formuliert sein, dass die betroffene Person verstehen kann, in was sie einwilligt – das Gesetz spricht von «angemessener Information».
- Die Einwilligung erfolgt immer vor der Datenerhebung, nicht danach
- Die Einwilligung erfolgt zweckgebunden. Falls im Verlauf oder nach dem Forschungsprojekt eine Änderung des Zwecks der Datenbearbeitung erfolgt, müssen die betroffenen Personen erneut um entsprechende Einwilligung angefragt werden.

Eine Einwilligung muss immer freiwillig erfolgen. Es ist darauf zu achten, dass durch die Wortwahl oder auch das Setting in dem die Einwilligung eingeholt wird, die Freiwilligkeit gewährleistet ist. Der betroffenen Person dürfen keine Nachteile entstehen, wenn sie die Einwilligung verweigert, dies ist insbesondere bei Abhängigkeitsverhältnissen zu beachten.



Im Vorfeld des Workshops ist auch ein Fact Sheet zum Thema Einwilligungen entstanden. Dieses wird zusammen mit weiteren Handreichungen, die noch in der Ausarbeitung sind, in Kürze auf unseren Webseiten zur Verfügung gestellt.

Die informierte Einwilligung ermöglicht die Durchführung vieler Forschungsprojekte. Die Probleme entstehen da, wo es niemanden mehr gibt, den man um Einwilligung fragen kann. Grundsätzlich erlischt das Persönlichkeitsrecht mit dem Tod der betroffenen Person, jedoch ist dies kein Freischein um Daten von Verstorbenen beliebig zu nutzen, denn es gibt den sogenannten «Andenkenschutz» der Angehörigen. Eine informierte Einwilligung kann auch dann nicht eingeholt werden, wenn man einen explorativen Forschungsansatz verfolgt, also zunächst Informationen beschafft und die Untersuchungsfrage erst zu einem späteren

Zeitpunkt definiert. Der Zweck der Datenerhebung kann also vorab gar nicht formuliert werden. Dies ist momentan noch ein ungelöstes Problem, dem wir noch nachgehen müssen.

3. Technische Infrastruktur – Datenschutztechnologie

Ein weiteres wichtiges Thema im Zusammenhang mit dem Datenschutz ist die Informationssicherheit und der technische Schutz der Daten, beispielsweise durch Verschlüsselung und Zugriffskontrollen. Die IT Dienste der Universitäten empfehlen, die von ihnen gepflegten universitären Server zu verwenden und bei besonders schützenswertem Material, wie besonderen Personendaten, zusätzliche Sorgfalt walten zu lassen. Beispielsweise können die verwendeten Rechner bzw. die Daten selbst verschlüsselt werden.



Weitere Informationen und hilfreiche Hinweise zum Umgang mit sensiblen Daten und zum Thema Verschlüsselung finden Sie auf den Seiten der IT-Services der Universität Basel.

Bei der Verwendung von Sharing Diensten und Cloud Speichern, sollte man strenge Sorgfalt walten lassen, wenn man mit sensiblen Daten arbeitet. Vor der Verwendung eines solchen Dienstes sollte man die datenschutzrechtlichen Bestimmungen genau ansehen und prüfen, wo die physischen Standorte der Server liegen, denn nicht in allen Ländern sind die Datenschutzstandards gleich streng. Falls man dennoch einen solchen Dienst nutzen muss oder möchte, sollte man die Daten unbedingt verschlüsselt übermitteln.

Wie geht es weiter?

Das Organisationsteam, das sich aus der Fachstelle [Forschungsunterstützung der UB Basel](#), Mitarbeiterinnen des [Open Science Teams UB Bern](#) und der [Datenschutzbeauftragten der Universität Basel](#) zusammensetzt, hat die Fragen der TeilnehmerInnen des Workshops und die Einschätzungen der Experten gesammelt und erstellt daraus in den nächsten Wochen

generalisierte Handlungsempfehlungen und Anleitungen zum Umgang mit Personendaten in der qualitativen Forschung. Handouts, die bereits im Vorfeld des Workshops entstanden sind, werden zudem in den nächsten Wochen überarbeitet und ergänzt. Diese Handreichungen und Unterlagen aus dem Workshop werden dann auf den Webseiten zum Forschungsdatenmanagement der [Universitäten Basel](#) und [Bern](#) zu Verfügung stellen.

Weitere Workshops und Schulungen, wie beispielsweise Writing Labs für Einwilligungserklärungen, ein Workshop zum Umgang mit Personendaten bei quantitativer Forschung und Workshops zu anderen Rechtsthemen sind bereits geplant.

iris.lindemann@unibas.ch

Publiziert am 18.06.2019 auf <https://blog.ub.unibas.ch/>