Covid-19 und der Schutz personenbezogener Daten beim Fernunterricht mit Zoom

Einführung

Die Pandemie, die durch das neuartige Coronavirus mit dem Krankheitsbild Covid-19 verursacht wurde, hat einen großen weltweiten Einfluss. Arbeitsplätze, einzelne Tätigkeitsbereiche und Strategien wurden angepasst. Unter anderem betraf die Pandemie auch das Bildungswesen. Gemäß Artikel 3 Absatz 1 der Verordnung der georgischen Regierung vom 23. März 2020 wurde der Unterricht im öffentlichen Bildungswesen in ganz Georgien ausgesetzt. Auf der Grundlage desselben Rechtsaktes wurde den Bildungseinrichtungen die Möglichkeit eingeräumt, die Form des Fernunterrichts zu nutzen. Infolgedessen haben viele öffentlichen und privaten Universitäten beschlossen, sich auf eine neue Form des Unterrichts umzustellen.

Der Fernunterricht hat in der Praxis neue Herausforderungen geschaffen, darunter auch den Schutz personenbezogener Daten. Einige der Dozenten oder Studenten verbreiten das Material in sozialen Netzwerken mit bestem Wissen und Gewissen (meist in Form einer Bildschirmkopie, eines sog. *Screenshot*s). Das Material im Fernunterricht enthält häufig personenbezogene Daten.

Der vorliegende Beitrag befasst sich mit der Frage, wie gut die persönlichen Daten von Einzelpersonen geschützt sind, wenn sie der Weitergabe solchen Materials nicht zustimmen. Das Staatliche Inspektorat gab dazu Empfehlungen heraus, die sich auf den Fernunterricht und den Schutz personenbezogener Daten bezogen.[1] Das zu erörternde Thema wird auch nach dem Ende der Covid-19-Pandemie rechtlich relevant sein, wenn in einigen Fällen weiterin Fernunterricht stattfinden wird.

1. Arten des Fernunterrichts

Hochschuleinrichtungen haben mehrere Arten des Fernunterrichts entwickelt. Ein erster Fall ist die Verteilung von Videomaterial, bei der der Dozent die Vorlesung individuell in Form eines Videos verfasst und den Studenten zur Verfügung stellt. Das zweite Beispiel ist die Lieferung von Audio-Material (Vertonung) der Vorlesung an die Studenten. Dies kann sowohl von einer ergänzenden Präsentation (z. B. *Power Point*) begleitet werden, als auch nur durch die Tonaufnahme geschehen. Ein drittes und in der Praxis recht häufiges Beispiel ist die Verwendung des Videokonferenzdienstes *Zoom*, wenn ein Dozent online mit den Studierenden arbeitet und so seine Vorlesung hält (einschließlich der Möglichkeit für die Studierenden, sich einzubringen und Fragen zu stellen). Angesichts der relevanten technischen Merkmale wird sich der vorliegende Beitrag auf den Fall *Zoom* fokussieren.

[1] https://personaldata.ge/ka/press/post/6349, zuletzt abgerufen am 20.09.2020.

2. Verwendung von Zoom und personenbezogene Daten

Bei der Verwendung von *Zoom* ist es technisch möglich, den Vor- und Nachnamen der Person, die daran teilgenommen hat (Anwesende), sowie bildliche Darstellungen darin anzuzeigen. In den meisten Fällen ist es dem Studierenden (und auch dem Dozenten) freigestellt, ob er die Videoübertragung einschalten und sein eigenes Bildmaterial anzeigen lassen will. In jedem Fall hat der Anwesende das Ziel, die Vorlesung zu besuchen. Er hat allerdings nicht die Vorstellung, dass sein Bild öffentlich gemacht werden kann.

3. Der Unterschied zwischen einer Online-Vorlesung und einer Hörsaal-Vorlesung (in Bezug auf den Schutz personenbezogener Daten)

Bei einer Online-Vorlesung vergibt *Zoom* einen individuellen, einmaligen Code. Insbesondere registriert der Vorlesungsveranstalter (meist der Dozent) die Fernveranstaltung. Diese erhält durch das *Zoom*-System einen individuellen, eindeutigen Code, der an die Studierenden gesendet wird, damit diese an der virtuellen Sitzung teilnehmen können.

Der Code wird nur an interessierte oder registrierte Personen gesendet. Es handelt sich nicht um eine öffentliche Information (es sei denn, der Code wird vom Veranstalter direkt an einen unbestimmten Personenkreis weitergegeben). Folglich hat nicht jede Person die Möglichkeit, an einer Online-Vorlesung teilzunehmen.

Ganz anders bei einer Vorlesung in einem Hörsaal: In der Hochschulbildung in Georgien hat in den allermeisten Fällen jede Person das Recht, eine Vorlesung zu besuchen, den Hörsaal zu betreten und dem Dozenten zuzuhören, ohne über irgendeine Zulassung oder Einschreibung zu verfügen.

Trotz dieser Unterschiede sollten die personenbezogenen Daten sowohl der Online- als auch der Hörsaalbesucher nicht ohne deren Zustimmung verarbeitet oder veröffentlicht werden. Dies gilt sowohl für das Fotografieren/bildliche Wiedergeben (insbesondere bei der Verbreitung) als auch für die Weitergabe von Daten zu Vor- und Nachnamen an einen unbestimmten Personenkreis, das Erstellen eines *Screenshots* o.ä. Die hier erforderliche Einwilligung erfordert einerseits den Aufruf (die Erklärung) des Dozenten (Organisators), die Herstellung entsprechender Umstände (wie Veranstaltungshinweise) und andererseits die Willensbekundung der anwesenden Person (positive Handlung oder Untätigkeit auf den Aufruf hin).

4. In sozialen Netzwerken verbreitete Daten

Nach Beginn des Fernstudiums gab es in Georgien mehrere Fälle, in denen ein Dozent oder ein Student *Screenshots* oder Videos einer Vorlesung in Form eines *Zoom*-Formats in sozialen Netzwerken mitteilte. In den meisten Fällen (soweit derzeit bekannt) hatten die anderen Teilnehmer nicht eingewilligt, dieses Bildmaterial zu verbreiten. Folglich konnten diejenigen, die in keiner Verbindung mit der Vorlesung (Veranstaltung) standen, auf personenbezogene Daten zugreifen.

5. Einwilligung der Anwesenden zur Verbreitung von personenbezogenen Daten

Wie in der Einleitung erwähnt, empfahl das georgische Staatliche Inspektorat bei der Verteilung von Video- und Fotomaterial, das den Online-Vortrag über soziale Netzwerke betrifft, (wie

stets) das Interesse der betroffenen Person zu berücksichtigen. Dies setzt an sich schon die Einwilligung der Anwesenden voraus. Die Frage wird rechtlich im Rahmen von Artikel 5 (in Einzelfällen Artikel 6) des georgischen Gesetzes über den Schutz personenbezogener Daten behandelt.

Eine Einwilligung zu erteilen bedeutet nicht, eine Einwilligung zu unterzeichnen oder auf eine besondere Art und Weise zu erteilen. Dies kann vielmehr auf verschiedene Weise geschehen:

a) durch Ankündigung der individuellen Einwilligung im Nachrichtenaustausch (*Chat*) im *Zoom*-Format;

b) durch mündliche Zustimmung;

c) durch konkludentes (schlüssiges) Handeln. Zum Beispiel, wenn ein Dozent (Administrator, Organisator oder Teilnehmer) erklärt, dass er Material in Form eines Bildschirmfotos (*Screenshot*) verbreiten will und die anderen Teilnehmer sich damit einverstanden zeigen (z. B. durch Kopfnicken);

d) durch konkludentes Handeln, das sich in Untätigkeit trotz Verkehrserwartung zeigt. Das letzte Beispiel würde so abgeändert, dass die Teilnehmer (Anwesende) trotz Ankündigung keine abweichende Meinung äußern. Einige von ihnen schalten möglicherweise das Videoaufnahmesystem ganz aus, verlassen aber die Veranstaltung nicht;

e) wenn alle anderen Teilnehmer (Anwesende) im Voraus vom Dozenten (oder Teilnehmer) darauf hingewiesen wurden, dass Fotos oder Videos aufgenommen und dann verbreiten werden, und wenn sich der Studierende in der Kenntnis dessen an der Sitzung beteiligt, darf dies als Einwilligung angesichts der erwarteten Veröffentlichung personenbezogener Daten gewertet werden.

Ähnlich ist es bei Online-Vorlesungen. Da es praktisch schwierig ist, Verstöße (unangemessene Nutzung) im Voraus zu vermeiden, sollte der präventive Zweck darin bestehen, die Einwilligung zu erhalten und, falls eingewilligt wird, die begründeten Erwartungen einzuhalten. Allerdings sind auch hier bestimmte Bedingungen zulässig: der Umfang der Nutzung, die Voraussetzungen für die Beschränkung und das Verbreitungsgebiet, deren Verletzung jeweils eine Haftung nach sich ziehen kann.

Zusammenfassung

Der Einsatz jeder neuen Technologie geht mit der Frage des Schutzes personenbezogener Daten einher. Eine Vorlesung mit *Zoom* bedeutet nicht, dass sie frei vom Schutz personenbezogener Daten ist. Vielmehr müssen die Rechte jeder Person in der gleichen Weise geschützt werden wie beispielsweise bei Programmen wie *Skype*, *Viber* und dergleichen.

Daher stellt die Einstellung von Online-Video- oder Fotomaterial ohne vorherige Einwilligung (Willensäußerung) eine Verletzung der personenbezogenen Daten dar, und der Einsteller wird gemäß der Gesetzgebung Georgiens dafür zur Verantwortung gezogen. Es ist bemerkenswert, dass es in solchen Fällen keine Rolle spielt, ob die Handlung des Verbreiters personenbezogener Daten einem positiven oder einem negativen Zweck diente. In beiden Fällen besteht die Notwendigkeit des Schutzes personenbezogener Daten.

Sergi Jorbenadze