A3: GeoApps und Datenschutz am eigenen Smartphone

1. Reflektieren Sie Ihren persönlichen Umgang mit Apps und sensiblen Daten auf Ihren mobilen Geräten (Smartphone) oder bei der Nutzung des Internets (auch am Laptop).
2. Prüfen Sie die Zugriffsrechte der installierten Apps.

Vor der Erstellung dieses Reflective Papers habe ich die Zugriffsberechtigungen der Apps auf meinem Smartphone kontrolliert und gegebenenfalls modifiziert. Häufig kommt es vor, dass eine App aufgrund einer einmalig durchgeführten Aktion (zB. Das Teilen eines Artikels mit einem Kontakt) eine Zugriffsberechtigung angefordert wird (in diesem Fall der Zugriff auf die Telefonkontakte), diese gegeben und später nicht widerrufen wird. Daher habe ich den Zugriff auf Kontakte, Telefon, Kamera, Kalender, Mikrofon und Speicher bei denjenigen Apps ausgeschaltet, bei denen es mir nicht von alltäglichem und direktem Nutzen ist, dass jene Apps Zugriff auf diese Daten haben.

In Bezug auf diese Lehrveranstaltung ist besonders die Berechtigung für den Zugriff auf den individuellen Standort von großer Bedeutung. Vor meiner Bearbeitung hatten 21 meiner 52 installierten Apps und Anwendungen Zugriff auf meinen Standort. Bei einigen von diesen erscheint mir dies auch sinnvoll, weswegen ich den Zugriff teilweise weiterhin gewähre. Die Bergfex-App sowie die Lauf-App Strava benötigen den Standortzugriff um zurückgelegte Routen aufzeichnen und analysieren zu können. Auf manchen Social Media Plattformen sowie mittels Messenger-Diensten kommuniziere ich von Zeit zu Zeit meinen aktuellen Standort, beispielsweise auf Urlaubsreisen, weswegen auch für diese Anwendungen der Standortzugriff erlaubt ist. Google Maps und die DORIS-App benötigen für einige individuelle Funktionen auch den Standortzugriff. Der Standortzugriff der Kamera ermöglicht das geo-tagging von Bildern und die spätere Verortung der Aufnahmen, was mir beispielsweise beim Wandern sehr gelegen kommt und andere Apps wie Scotty Mobile und Willhaben sind mit Standortinformation schlicht und weg einfacher und unkomplizierter zu nutzen.

Generell muss dem Nutzer/der Nutzerin bewusst sein, dass viele Apps sämtliche Daten, wie auch den Standort, nicht (nur) verlangen, um das Nutzungserlebnis und die App-Performance zu verbessern, sondern dass die Daten auch weitergegeben und beispielsweise für Werbezwecke verwendet werden können. Da ich mir selbst zutraue, mit Werbung reflektiert umzugehen und weil ich in der Daten- und Standortweitergabe auch sehr viele praktische Vorteile erkenne, habe ich persönlich kein großes Problem damit, „gläsern“ zu sein und meine Daten zur Verfügung zu stellen, sofern ich – und andere – keinen Schaden davontragen.

Eine Erfahrung, die ich immer wieder mache, ist es, nach dem Besuch eines gewerblichen Ortes die Aufforderung von Google Maps zu bekommen, den Ort zu bewerten und vorhandene Fragen zu beantworten. Selbstverständlich fühle ich mich in diesen Momenten überwacht, da Google anhand des Mobilfunknetz-Zugriffs-Standortes meinen konkreten Aufenthaltsort ganz rasch nachvollziehen kann, jedoch sehe ich auch hier einen Nutzen. Indem ich Fragen über einen Ort beantworte (beispielsweise ob vor einer Apotheke behindertengerechte Parkplätze vorhanden sind, ob ein Restaurant vegetarische Gerichte anbietet, ob die eingetragenen Öffnungszeiten einer Bäckerei noch gültig sind, etc.), helfe ich anderen Nutzern, die über das Internet nach derartigen Informationen suchen. Daher sehe ich auch hier kein Risiko, sondern eine Chance.

Am Laptop sowie auch am Smartphone achte ich darauf, dass wichtige Zugangsdaten wie Passwörter und Banking Codes nicht im Speicherverlauf aufscheinen und regelmäßig aus dem Cache gelöscht werden. Außerdem vermeide ich es, das E-Mail und Bankkonto online von fremden Geräten

anzusehen und verleihe auch meinen Laptop eher ungern, da ich Angst davor habe, dass jemand an diese Zugangsdaten kommen könnte.

3. Reflektieren Sie Ihre eigenen persönlichen Profile in Social Media, im Web, ... sowie jene Ihrer "Freunde".

Abgesehen von meinen PH-Online-Profilen und Accounts auf diversen Websites, die wenig bis keine persönliche Information über mich bereitstellen, verfüge ich auch über ein Profil auf Facebook und ein Profil auf Instagram. Auf Facebook können nur „Freunde“ meine persönlichen Daten, Fotos und Einträge sehen, wobei ich dieses Netzwerk nicht aktiv nutze, sondern nur zum kommunikativen Austausch und zur Vernetzung beispielsweise als Chat mit StudienkollegInnen verwende. Auf Instagram poste ich auch aktiv Content, der öffentlich sichtbar ist. Jedoch verwende ich keine Bilder oder Kommentare, die sich in irgendeiner Weise negativ auf meine Erscheinung auf der Social Media Plattform auswirken können, mich in ein schlechtes Licht stellen oder mich bei einer zukünftigen Jobsuche behindern könnten. Letzteres kann ich von meinen „Freunden“ nicht behaupten, da ich einige Personen kenne, die Bilder mit obszönen Gesten, von scheinbar betrunkenen Feiergelegenheiten oder in nur spärlicher Bekleidung von sich öffentlich auf den Social Media Plattformen teilen. Von derartigen Verhaltensweisen distanziere ich mich konkret, da mir bewusst ist, dass die Bilder auch nach angeblichem „löschen“ weiterhin auffindbar sind und dem Urheber ein Leben lang im Weg stehen können.