LE05: Pegasus - (k)ein Segen

Der inhaltliche Fokus der Lerneinheit liegt auf der kritisch-reflexiven Auseinandersetzung mit dem Skandal um die Spyware Pegasus. Im Licht einer theoretischen Auseinandersetzung mit der Entstehung und Nutzung, der Entdeckung und der Vor- und Nachteile der laut der Zeit „mächtigsten“ Spyware der Welt und deren Folgen, werden die Relevanz und Notwendigkeit der DSGVO diskutiert. Ziel dessen ist es, die Lernenden für die Funktionen und Folgen von Pegasus zu sensibilisieren und ein Nachdenken über den eigenen Umgang mit personen- und standortbezogenen Daten anzuregen.

Inhalte der Lerneinheit

- Kritisch-reflexive Auseinandersetzung mit den Funktionen und Folgen der Spyware Pegasus
- Die Relevanz und Notwendigkeit der DSGVO

Materialien

- AB05-1: Die Spyware Pegasus - Fluch oder Segen?
- AB05-2: Pegasus und die DSGVO
- M05-1: Malware, Spyware, Pegasus
- M05-2: Die DSGVO

Lernergebnisse und Kompetenzen

Nach Abschluss der Lerneinheit können Sie…

- Die Intention und das Vorgehen der NSO in der Entwicklung von Pegasus skizzieren.
- Die Funktionen, Folgen, Vor- und Nachteile der Spyware Pegasus diskutieren.
- Die Relevanz und Notwendigkeit der DSGVO im Hinblick auf den Umgang mit personen- und standortbezogenenen Daten reflektieren.

Pegasus, das geflügelte Pferd

Der Mythos um das geflügelte Pferd Pegasus stammt aus der Mythologie der griechischen Antike, in der Pegasus, das Kind des Meeresgottes Poseidon und der Gorgone Medusa, einer geflügelten Schreckgestalt mit Schlangenhaaren ist. Symbolisch steht das geflügelte Pferd für die neun Musen der Künste, ist in zahlreichen Statuen, in Bildern, auf Vasen und anderen Gegenständen verewigt und prangt nachts als Sternbild am Himmel. Das Motiv des geflügelten Pferds ist Markenzeichen der türkischen Pegasus Airline und Namensgeber eines Spähtrojaners, dessen Entdeckung den bis dato größten globalen Cyber- bzw. Spyware-Skandal auslöste. Entwickelt vom israelischen Start-up NSO für Strafverfolgungsbehörden und Geheimdienste, um aus der Ferne und im Verborgenen wertvolle Informationen von praktisch jedem mobilen device abzugreifen und Terrorismus und Kriminalität wirksam zu bekämpfen. Doch was passiert, wenn die Software entgegen dieses ambitionierten Ziels eingesetzt wird, um politische Größen, Separatisten, Oppositionelle, Menschenrechtsaktivist*innen, Mitglieder der EU-Kommission und NGOs, investigativ Journalist*innen und Staats- und Regierungschefs zu bespitzeln und die Erkenntnisse gegen sie zu verwenden?