

# Vertrauenswürdige Überwachung

**Thomas Winkler** entwickelt Kameras, die die Identität der gefilmten Personen schützen. Der Zugriff auf diese Informationen ist für Behörden aber trotzdem möglich.

✦ VON VERONIKA SCHMIDT

Smarte Systeme in Kameras – das kennt jeder vom digitalen Fotoapparat, der Gesichter erkennt oder erst knipst, wenn der Fotografierte lächelt. Thomas Winkler hat sich in seiner Dissertation (Alpen-Adria Universität Klagenfurt, Technische Wissenschaften, Betreuer Bernhard Rinner) mit Fragen der Sicherheit und Privatsphäre in smarten Kamerasystemen beschäftigt: „Man ist auf öffentlichen Plätzen ständig von Überwachungskameras umgeben. Außerdem geht der Trend zu Kameras im sehr privaten Bereich. Etwa bei der Altenbetreuung sollen Kameras melden, wenn die Person gestürzt ist.“ Da fragen natürlich viele Bürger, ob solche Kamerasysteme sicher sind, ob die Privatsphäre geschützt ist, obwohl die digitalen Daten lange gespeichert und durchsucht werden können. „Es muss bei aufgezeichneten Bilddaten si-

chergestellt werden, dass sie authentisch und unmanipuliert sind, und wer Zugriff hat: Der Schutz soll nicht nur nach außen gehen, sondern es geht auch um die Sicherheit gegenüber Insidern, also dem Betreiber des Kamerasystems etwa, der ja Zugriff auf die Daten haben muss.“ Die Gratwanderung ist dabei: Wie viele und welche Daten sind notwendig, um eine sinnvolle Überwachung zu gewährleisten?

Im Vordergrund steht meist das Verhalten der Personen, nicht aber die Identität. „Die wird erst dann wichtig, wenn etwas Gravierendes wie ein Verbrechen passiert“, sagt Winkler. Er hat ein System entworfen, das mit Hilfe eines Crypto-Chips unterschiedliche Zugriffsebenen ermöglicht: „Wir haben die Bildanalyse auf die Kamera gebracht.“ Sensitive Bildregionen werden geschützt, noch bevor sie die Kamera

verlassen. Gesichter, Personen oder Autokennzeichen – die Kamera erkennt diese Regionen und verpixelt sie oder ersetzt Personen durch Silhouetten. Die Daten werden außerdem verschlüsselt. „Für den Wachmann sind dann nur die Verhaltensinformationen sichtbar, er hat nur das Passwort für diese Ebene. Doch wenn etwas Gravierendes passiert, kann z. B. eine Behörde auf die verschlüsselten Identitätsinformationen zugreifen. Am besten im Vier-Augen-Prinzip, also wenn mindestens zwei Verantwortliche kooperieren.“ Die Originaldaten gehen bei der Verschlüsselung nicht verloren und lassen eine Verfolgung der handelnden Personen zu. Winkler stieß bei seiner Arbeit auf immer neue Fragen und hat einen Antrag auf Förderung weiterführender Forschung eingereicht.



///