Marta Gomez-Barrero

Biometrie und Datenschutz

Obwohl die Nutzung biometrischer Informationen zahlreiche Vorteile gegenüber der Verwendung von Passwörtern bietet, wie z.B. eine stärkere Bindung zwischen der Identität und dem Subjekt, sind viele Personen wegen eines möglichen Missbrauches der biometrischen Daten besorgt. Unter anderem können biometrische Daten verwendet werden, um Krankheiten aufzudecken oder Datenbanken zu verknüpfen. Des Weiteren können die geografische Lage, Bewegungen oder Gewohnheiten durch die Auswertung der bei Anmeldungen erfassten biometrischen Charakteristika zurückverfolg werden. Um sich mit diesem Anliegen zu befassen, wurden die biometrische Daten als sensiblen *persönlichen Daten* von der Europäische Union Datenschutz-Grundverordnung 2016/679 betrachtet: biometrische Charakteristika sind ein wesentliches Teil des Menschenkörpers oder seines Verhaltens, welche im Falle von Diebstahl nicht ersetzt oder abgelegt werden können. Im Rahmen der Verordnung wurden *persönlichen Daten* wie folgt definiert: "*alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann*". Das bedeutet, dass während der *Verarbeitung* der biometrischen Daten das Recht auf Schutz der Privatsphäre gewährleistet sein muss, wobei *Verarbeitung* bedeutet "*jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung*".

Nach den genannten Definitionen muss biometrische Information sorgfältig geschützt werden, um die Privatsphäre des Subjekts zu gewährleisten. Sowohl bei der Speicherung, als auch wenn sie verarbeitet werden. Um diesen Datenschutz zu ermöglichen, müssen wir uns verschiedene Frage stellen.

Lässt sich aus den gespeicherten Templates Information zum Subjekt ableiten? Mit anderen Worten, kann man aus dem Template ein Sample synthetisieren, welches dem ursprünglichen biometrischen Sample ähnlich ist? Es hat sich gezeigt, dass ein solches *inverse biometrics* Verfahren für verschiedene biometrische Charakteristika möglich ist. Aufgrund dessen kann ein Angreifer, welcher Zugang zu gespeicherten Templates hat, ein Sample rekonstruieren, mit welchem er sich fälschlicherweise an einem System anmelden oder die Identität eines Opfers übernehmen kann, welches dessen Privatsphäre verletzen würde. Daher muss die *Irreversibilität* der Templates sichergestellt werden.

Selbst wenn die Templates irreversibel sind, sind Templates, welche in verschiedenen Systemen enrolt sind korreliert. Kann jemand durch eine Kreuzprobe der Templates meine Aktivitäten nachverfolgen? Es genügt nicht irreversibel Templates zu speichern und somit die Anfälligkeit für *irreversible biometrics* Verfahren vermeiden. Aufgrund des zunehmend verbreiteten Einsatzes biometrischer Systeme wird sich ein Subjekt, mit zunehmender Wahrscheinlichkeit, mit dem gleichen Charakteristikum oder der gleichen Instanz (z.B., rechter Zeigefinger) beim unterschiedlichen Applikationen (z.B. Gesundheitssysteme oder Onlinebanking) anmelden. Das Recht auf Privatsphäre beinhaltet, dass die Konten verschiedener Anbieter nicht mit einander verknüpft werden können. Ist diese Abkapselung der Systeme nicht gegeben, so kann ein Angreifer, welcher Zugang zu den enrolten Templates verschiedener Systemen hat, Informationen kombinieren und sie nutzen um z.B. weitere Kenntnisse über die Anzahl der Bankkonten der Opfer zu erlangen. Um dies zu unterbinden muss die *Kreuzprobe* zwischen Templates, welche in verschiedenen Applikationen verwendet werden, nicht durchführbar sein.

Was geschieht, wenn jemand das Template stiehlt, welche von meinen rechten Zeigefinger extrahiert wurde? Kann ich diesen Finger nie wieder bei einem System enrolen? Ist dieser für immer kompromittiert? Da biometrische Charakteristika nicht austauscht werden können, müssen unterschiedliche Templates einer einzigen Instanz generiert werden können, um gefährdete Templates verwerfen zu können. Darüber hinaus sollte zwischen diesen Templates kein Zusammenhang bestehen, mit Annahme der Verknüpfung mit dem Subjekt im biometrischen System. Nur so kann Identitätsbetrug im Falle von Diebstahl verhindert werden und das gewünschte Ziel der *Erneuerbarkeit* der biometrischen Templates erreicht werden. Des Weiteren wird durch das Erzeugen nicht korrelierter Templates die Möglichkeit der Kreuzprobe durch einen Angreifer vermieden.

Zusammenfassend müssen traditionelle biometrische Systeme durch *Biometric Template Protection Systems*, gemäß ISO/IEC 24745 ersetzt werden.