ARTIKEL-29-DATENSCHUTZGRUPPE

00727/12/DE
WP 192

Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten

Angenommen am 22. März 2012

1. Einleitung

In den letzten Jahren hat sich die Gesichtserkennungstechnologie sehr schnell verbreitet und ist genauer geworden. Darüber hinaus wurde diese Technologie für die Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung von natürlichen Personen in Online- und Mobilfunkdienste integriert. Die Technologie, die einst Science Fiction war, steht heute sowohl öffentlichen als auch privaten Stellen zur Nutzung zur Verfügung. Beispiele für ihre Verwendung im Bereich der Online- und Mobilfunkdienste umfassen soziale Netzwerke und Smartphones.

Die Artikel-29-Datenschutzgruppe (WP29) hat sich bereits im Arbeitspapier über Biometrie (WP80) und in der kürzlich veröffentlichten Stellungnahme 03/2012 (WP193) zu den Entwicklungen im Bereich der biometrischen Technologien mit der Fähigkeit, Daten automatisch zu erfassen und ein Gesicht von einem digitalen Bild zu erkennen, befasst. Die Gesichtserkennung wird als der Biometrie zugehörig betrachtet, da sie in vielen Fällen genügend Informationen enthält, um die eindeutige Identifizierung einer Person zu ermöglichen.

In der Stellungnahme 03/2012 wurde Folgendes festgestellt:

> *„[biometrics] allow for automated tracking, tracing or profiling of persons and as such their potential impact on the privacy and the right to data protection of individuals is high". (Biometrie ermöglicht die automatisierte Verfolgung und Aufspürung von Personen sowie die Profilerstellung und kann sich folglich erheblich auf die Privatsphäre und auf das Recht des Einzelnen auf Datenschutz auswirken).*

Diese Aussage trifft insbesondere im Fall der Gesichtserkennung bei Online- und Mobilfunkdiensten zu, wenn Bilder von Einzelpersonen erfasst (mit und ohne Kenntnis der jeweiligen Person) und dann für die Weiterverarbeitung an einen Remote-Server übermittelt werden. Online-Dienste, die sich häufig im Besitz von privaten Organisationen befinden und von diesen betrieben werden, haben immense Bildersammlungen angelegt, die von den betroffenen Personen selbst hochgeladen wurden. In einigen Fällen wurden diese Bilder möglicherweise auch rechtswidrig durch das automatische Auslesen aus anderen öffentlichen Webseiten wie Suchmaschinencaches erworben. Kleine mobile Geräte mit hochauflösenden Kameras ermöglichen es den Nutzern, Bilder aufzunehmen und in Echtzeit über ständig bestehende Datenverbindungen eine Verbindung zu Online-Diensten herzustellen. Dadurch können die Nutzer diese Bilder mit anderen teilen oder eine Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung durchführen, um zusätzliche Informationen über die bekannte oder unbekannte, vor ihnen stehende Person zu erhalten.

Da die Verwendung dieser Technologie viele verschiedene Datenschutzbedenken hervorruft, erfordert die Gesichtserkennung in Online- und Mobilfunkdiensten die besondere Aufmerksamkeit der WP29.

Der Zweck dieser Stellungnahme ist es, den Rechtsrahmen zu prüfen und angemessene Empfehlungen zu geben, die auf die Technologie zur Gesichtserkennung anzuwenden sind, wenn diese im Zusammenhang mit Online- und Mobilfunkdiensten genutzt wird. Diese Stellungnahme richtet sich an europäische und nationale Rechtsetzungsbehörden, für die Datenverarbeitung Verantwortliche und die Nutzer solcher Technologien. Die Stellungnahme möchte nicht die Grundsätze wiederholen, auf die in Stellungnahme 03/2012 verwiesen wurde, sondern baut auf diese im Bereich der Online- und Mobilfunkdienste auf.

2. Definitionen

Die Technologie der Gesichtserkennung ist nicht neu und für die einschlägigen Begriffe liegen eine Reihe von Definitionen und Auslegungen vor. Deshalb ist es hilfreich, die Technologie, wie sie in dieser Stellungnahme angesprochen ist, klar zu definieren.

Digitales Bild: Ein digitales Bild ist die Darstellung eines zweidimensionalen Bildes in digitaler Form. Die neuesten Entwicklungen in der Technologie zur Gesichtserkennung machen es jedoch erforderlich, dass dreidimensionale Bilder zusätzlich zu den statischen und den bewegten Bildern hinzugefügt werden (d. h. Fotos, aufgezeichnete Videos und Life-Videos).

Gesichtserkennung: Gesichtserkennung ist die automatische Verarbeitung digitaler Bilder, die Gesichter von natürlichen Personen enthalten, um bei diesen eine Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung[1] durchzuführen. Der Prozess der Gesichtserkennung besteht seinerseits aus einer Reihe eigenständiger Teilprozesse:

a) Bilderfassung: Der Prozess der Erfassung des Gesichts einer Person und der Umwandlung in eine digitale Form (das digitale Bild). Im Falle eines Online- oder Mobilfunkdienstes kann das Bild von einem anderen System erworben worden sein, z. B. wenn ein Foto mit einer digitalen Kamera aufgenommen und dann an einen Online-Dienst übermittelt wurde.

b) Gesichtserkennung: Der Prozess, mit dem ein Gesicht auf einem digitalen Bild erkannt und der Bereich markiert wird.

c) Bildnormung: Mit dem Prozess werden Abweichungen innerhalb der entdeckten Gesichtsregionen ausgeglichen. Dazu gehört beispielsweise die Umwandlung in eine Standardgröße, das Drehen oder Angleichen der Farbverteilung.

d) Merkmalsextraktion: Der Vorgang der Isolierung und Bestimmung wiederholbarer und unverwechselbarer Messwerte vom digitalen Bild einer Person. Die Merkmalsextraktion kann holistisch[2], merkmalsbasiert[3] oder eine Kombination aus beiden Methoden[4] sein. Der Satz der Hauptmerkmale kann für einen späteren Vergleich in einem Referenz-Template[5] gespeichert werden.

e) Enrolment: Beim ersten Kontakt einer Person mit dem Gesichtserkennungssystem können Bild und/oder Referenz-Template für einen späteren Vergleich als Datensatz gespeichert werden.

f) Vergleich: Der Prozess des Messens der Ähnlichkeit zwischen einem Satz an Merkmalen (Sample) mit einem bereits im System registrierten Satz. Die Hauptzwecke des Vergleichs sind Identifizierung und Authentifizierung/Verifizierung. Ein dritter Zweck des Vergleichs ist die

---

1 Identifizierung, Authentifizierung/Verifizierung und Kategorisierung sind in 03/2012 definiert.

2 Holistische Merkmalsextraktion: eine mathematische Darstellung des gesamten Bildes, wie ein sich aus einer Hauptkomponentenanalyse ergebendes Bild.

3 Merkmalsbasierte Merkmalsextraktion: Lokalisierung bestimmter Gesichtsmerkmale wie Augen, Nase und Mund.

4 Auch als hybride Methode der Merkmalsextraktion bekannt.

5 Template ist in 03/2012 definiert als „Hauptmerkmale, die der Rohform der biometrischen Daten entnommen werden (z. B. Gesichtsmaße von einem Bild) und anstelle der Rohdaten selbst für die spätere Verarbeitung gespeichert werden“.

Kategorisierung. Darunter versteht man den Prozess der Extraktion von Merkmalen aus dem Bild einer Person, um diese Person in einer oder mehreren breiter angelegten Kategorien zu klassifizieren (z. B. Alter, Geschlecht, Farbe der Kleidung usw.). Ein Kategorisierungssystem erfordert nicht unbedingt einen Enrolment-Prozess.

3. Beispiele für die Gesichtserkennung bei Online- und Mobilfunkdiensten

Die Gesichtserkennung kann auf verschiedenen Arten und aus einer Vielzahl von Gründen in Online- und Mobilfunkdienste integriert werden. Im Zusammenhang mit dieser Stellungnahme konzentriert sich die WP29 auf eine Reihe verschiedener Beispiele, die als Hintergrund der Rechtsanalyse dienen und in denen die Gesichtserkennung für die Zwecke der Identifizierung, Authentifizierung/Verifizierung und Kategorisierung verwendet wird.

3.1. Gesichtserkennung als Mittel der Identifizierung

Beispiel 1: Ein sozialer Netzwerkdienst (SNS)[6] erlaubt es den Nutzern, ihrem Profil ein digitales Bild hinzuzufügen. Außerdem können sie Bilder hochladen, um diese mit anderen registrierten oder nicht registrierten Nutzern zu teilen. Registrierte Nutzer können andere Personen (die nicht unbedingt registrierte Nutzer sind) auf den von ihnen hochgeladenen Bildern manuell identifizieren und markieren. Solche Tags (Markierungen) können von der Person gesehen werden, die den Tag angelegt hat und mit einer größeren Gruppe von Freunden oder mit allen registrierten oder nicht registrierten Nutzern geteilt werden. Der SNS kann markierte Bilder nutzen, um einen Referenz-Template für jeden registrierten Nutzer anzufertigen, und durch die Verwendung von Gesichtserkennungssystemen automatisch Tags für neue Bilder vorschlagen, wenn sie hochgeladen werden.

Internet-Suchmaschinen könnten dann Zugriff auf diese Bilder von natürlichen Personen nehmen, die durch die Nutzer öffentlich verfügbar gemacht werden und sie zwischenspeichern. Die Suchmaschine möchte ihre Suchfunktion möglicherweise verbessern, indem sie es Nutzern ermöglicht, das Bild einer Person zu übermitteln und eine Liste von Bildern mit sehr ähnlichen Merkmalen zu erhalten und diese wieder mit der Profilseite des SNS zu verlinken. Das für die Abfrage genutzte Bild kann direkt mit einer Smartphone-Kamera aufgenommen worden sein.

3.2. Gesichtserkennung als Mittel der Authentifizierung/Verifizierung

Beispiel 2: Ein Gesichtserkennungssystem wird genutzt, um einen Nutzernamen/ein Passwort zu ersetzen, mit dem der Zugang zu einem Online- oder Mobilfunkdienst oder -gerät kontrolliert wird. Beim Enrolment wird mit Hilfe einer Kamera an dem Gerät ein Bild des authorisierten Nutzers des Geräts aufgenommen und ein Referenz-Template erstellt, das in dem Gerät oder entfernt durch den Onlinedienst gespeichert werden kann. Um auf den Dienst oder das Gerät zugreifen zu können, wird ein neues Bild der betreffenden Person aufgenommen, das mit dem Referenzbild verglichen wird. Wenn das System einen positiven Abgleich meldet, wird der Zugang gewährt.

[6] In der Stellungnahme 05/2009 zu sozialen Online-Netzwerken werden soziale Online-Netzwerke allgemein definiert *„als Kommunikationsplattformen im Online-Bereich, die es dem Einzelnen ermöglichen, sich Netzwerken von gleich gesinnten Nutzern anzuschließen bzw. solche zu schaffen“*.

3.3. Gesichtserkennung als Mittel der Kategorisierung

Beispiel 3: Der in Beispiel 1 beschriebene SNS kann einem Dritten, der einen Online-Gesichtserkennungsdienst betreibt, den Zugang zu der Bilderdatei gewähren. Der Dienst ermöglicht es den Kunden, Gesichtserkennungstechnologie in andere Produkte zu integrieren. Die Funktion ermöglicht es diesen anderen Produkten, Bilder von Personen hinzufügen, um Gesichter zu ermitteln und in eine Gruppe zu ordnen oder nach vordefinierten Kriterien zu kategorisieren, z.B. wahrscheinliches Alter, Geschlecht und Laune.

Beispiel 4: Der Nutzer einer Spielekonsole verwendet ein Gestensteuerungssystem, bei dem Bewegungen des Nutzers zur Steuerung des Spiels erkannt werden. Die Kamera(s), die für das Gestensteuerungssystem verwendet wird, gibt/geben die Bilder der Personen an ein Gesichtserkennungssystem weiter, das das wahrscheinliche Alter, das Geschlecht und die Stimmung der Spieler zu erkennen versucht. Daten, einschließlich der Daten aus anderen multimodalen Faktoren ändern dann möglicherweise das Spiel, um das Spielerlebnis des Nutzers zu verbessern, oder ändern die Umgebung, um das bevorzugte Profil des Nutzers wiederzugeben. Auf ähnliche Weise könnte das System Nutzer klassifizieren, um den Zugang zu altersbezogenen Inhalten zu erlauben/zu verweigern oder um im Spiel gezielte Werbung zu schalten.

4. Rechtsrahmen

Der einschlägige Rechtsrahmen für die Gesichtserkennung ist die Datenschutzrichtlinie (95/46/EG), die in dieser Hinsicht bereits in der Stellungnahme 03/2012 diskutiert wurde. In diesem Abschnitt soll nur, basierend auf den Beispielen aus Abschnitt 3, eine Zusammenfassung des Rechtsrahmens im Kontext der Gesichtserkennung in Online- und Mobilfunkdiensten gegeben werden. In der Stellungnahme 03/2012 werden weitere Beispiele der Gesichtserkennung betrachtet.

4.1. Digitale Bilder als personenbezogene Daten

Wenn auf einem digitalen Bild ein klar sichtbares Gesicht einer Person abgebildet ist, das es ermöglicht, diese Person zu identifizieren, gehört das Bild in die Gruppe der personenbezogenen Daten. Das hängt von einer Reihe von Parametern ab, wie der Bildqualität und der jeweiligen Perspektive. Bilder von Szenen, die in der Ferne Personen zeigen oder bei denen die Gesichter unscharf sind, werden in den wenigsten Fällen als personenbezogene Daten gelten. Es muss jedoch angemerkt werden, dass digitale Bilder personenbezogene Daten von mehr als einer Person enthalten können (in Beispiel 4 können z. B. mehr Spieler im Blickfeld sein) und das Vorhandensein Anderer auf einem Foto kann auf eine bestehende Beziehung hinweisen.

Die Stellungnahme 04/2007 zum Begriff „personenbezogene Daten“ bekräftigt, dass Daten, *„die Merkmale oder das Verhalten dieser Person betreffen oder wenn sie verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt wird“* als personenbezogene Daten gelten.

Definitionsgemäß gilt ein Referenz-Template, das von dem Bild einer Person geschaffen wurde, auch als personenbezogene Daten, da es einen Satz unverwechselbarer Merkmale des Gesichts einer Person enthält, der dann mit einer bestimmten Person verlinkt wird und als Referenz für spätere Vergleiche zur Identifizierung und Authentifizierung/Verifizierung gespeichert wird.

Ein Template oder ein Satz unverwechselbarer Merkmale, die nur in einem Kategorisierungssystem verwendet werden, enthalten im Allgemeinen nicht ausreichend Informationen, um eine Person zu identifizieren. Es sollten nur genügend Informationen darauf enthalten sein, um die Kategorisierung vornehmen zu können (z. B. männlich oder weiblich). In dem Fall würde es sich nicht um personenbezogene Daten handeln, vorausgesetzt, dass das Template (oder das Ergebnis) nicht mit der Akte einer Person, mit ihrem Profil oder mit dem Originalbild (das weiterhin als personenbezogene Daten gilt) in Verbindung gebracht wird.

Da sich digitale Bilder von Personen auf „*biologische Eigenschaften, auf Verhaltensaspekte, physiologische Merkmale, Gesichtszüge oder reproduzierbare Handlungen [beziehen], wobei diese Merkmale und/oder Handlungen für die betreffende Person spezifisch und messbar sind*[7]“, sollten sie als biometrische Daten gelten.

4.2. Digitale Bilder als besondere Kategorie personenbezogener Daten

Digitale Bilder von Personen können in bestimmten Fällen als besondere Kategorie personenbezogener Daten[8] angesehen werden. Insbesondere, wenn digitale Bilder von Personen oder Templates weiterverarbeitet werden, um bestimmte Kategorien von Daten zu erhalten, gehören sie ganz bestimmt zu dieser Kategorie. Ein Beispiel hierfür ist, wenn die Daten dazu genutzt werden, Informationen über die ethnische Herkunft, die Religion oder die Gesundheit zu erhalten.

4.3. Verarbeitung personenbezogener Daten im Zusammenhang mit einem Gesichtserkennungssystem

Wie bereits beschrieben, basiert die Gesichtserkennung auf einer Reihe automatisierter Verarbeitungsschritte. Deshalb stellt die Gesichtserkennung eine automatisierte Form der Verarbeitung personenbezogener Daten, einschließlich biometrischer Daten, dar.

Durch die Verwendung biometrischer Daten können Gesichtserkennungssysteme in einzelnen Mitgliedstaaten zusätzlichen Kontrollen oder anderen Rechtsvorschriften wie einer vorherigen Genehmigung oder dem Arbeitsrecht unterliegen. Auf die Verwendung von Biometrie im Beschäftigungskontext wird in Stellungnahme 03/2012 näher eingegangen.

4.4. Für die Datenverarbeitung Verantwortlicher

Die vorstehenden Beispiele zeigen, dass die für die Datenverarbeitung Verantwortlichen üblicherweise Eigentümer der Website und/oder Online-Service-Provider sowie Betreiber mobiler Applikationen, die Gesichtserkennungsdienste anbieten, sind, da sie den Zweck und/oder die Mittel der Verarbeitung[9] festlegen. Das entspricht auch der Schlussfolgerung aus Stellungsnahme 05/2009 ein, die lautet: „Die Anbieter sozialer Netzwerkdienste sind die ’für die Verarbeitung von Benutzerdaten Verantwortlichen’ im Sinne der Datenschutzrichtlinie.“

4.5. Berechtigter Grund

Richtlinie 95/46/EG legt die Bedingungen fest, die bei der Verarbeitung personenbezogener Daten eingehalten werden müssen. Das heißt, dass die Verarbeitung zuerst die Anforderungen hinsichtlich der Datenqualität (Artikel 6) erfüllen muss. In diesem Fall muss die Verarbeitung der digitalen Bilder der Personen und der entsprechenden Templates für die

---

7 Definition von Biometrie aus Stellungnahme 03/2012

8 In bestimmten Ländern hat die Rechtsprechung digitale Bilder von Gesichtern als besondere Kategorie von Daten eingestuft - LJN BK6331 Oberster Gerichtshof der Niederlande vom 23. März 2010

9 Siehe Stellungnahme 01/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“.

Zwecke der Verarbeitung zur Gesichtserkennung „relevant“ sein und darf „nicht darüber hinausgehen“. Außerdem darf nur dann eine Verarbeitung stattfinden, wenn eine der in Artikel 7 niedergelegten Voraussetzungen erfüllt ist.

Aufgrund der besonderen Risiken, die mit biometrischen Daten einhergehen, muss folglich vor dem Beginn der Verarbeitung von digitalen Bildern für die Gesichtserkennung die in Kenntnis der Sachlage erteilte Einwilligung der betroffenen Person eingeholt werden. In einigen Fällen kann es jedoch erforderlich sein, dass der für die Datenverarbeitung Verantwortliche vorübergehend einige Verarbeitungsschritte zur Gesichtserkennung durchführen muss, um zu bewerten, ob der Nutzer seine Einwilligung in die Verarbeitung erteilt hat oder nicht und ob somit eine Rechtsgrundlage vorhanden ist. In dem Fall kann diese anfängliche Verarbeitung (d. h. Bilderfassung, Gesichtserkennung, Vergleich usw.) eine andere Rechtsgrundlage haben und zwar insbesondere das rechtmäßige Interesse des für die Datenverarbeitung Verantwortlichen an der Einhaltung der Datenschutzbestimmungen. Daten, die während dieser Schritte verarbeitet werden, sollten ausschließlich für die Feststellung genutzt werden, ob der Nutzer seine Einwilligung erteilt hat, und sollten folglich sofort danach gelöscht werden.

Im ersten Beispiel hat der für die Datenverarbeitung Verantwortliche festgestellt, dass an allen hochgeladenen, neuen Bildern von registrierten Nutzern des SNS die Schritte der Gesichtserkennung, der Merkmalsextraktion und des Vergleichs durchgeführt werden sollen. Nur bei registrierten Nutzern, von denen sich ein Referenz-Template in der Datenbank befindet, wird eine Entsprechung mit diesen neuen Bildern festgestellt und folglich automatisch eine Markierung vorgeschlagen. Wenn die Einwilligung der Einzelperson als einziger berechtigter Grund für die gesamte Verarbeitung anzusehen ist, muss der vollständige Dienst blockiert werden, da beispielsweise keine Möglichkeit besteht, die Einwilligung von nicht registrierten Nutzern einzuholen, deren personenbezogene Daten möglicherweise während der Gesichtserkennung und Merkmalsextraktion verarbeitet werden. Außerdem wäre es nicht möglich, die Gesichter der registrierten Nutzer, die ihre Einwilligung erteilt haben, von denen zu unterscheiden, die keine Einwilligung erteilt haben, ohne zuerst eine Gesichtserkennung durchzuführen. Erst nachdem eine Identifizierung stattgefunden hat (oder diese nicht möglich war), könnte ein für die Datenverarbeitung Verantwortlicher feststellen, ob ihm die erforderliche Einwilligung in die jeweilige Verarbeitung erteilt wurde.

Bevor ein registrierter Nutzer ein Bild auf einen SNS hochlädt, muss er in klarer Weise darüber informiert werden, dass diese Bilder durch ein Gesichtserkennungssystem laufen. Noch wichtiger ist, dass die registrierten Nutzer darüber hinaus entscheiden können, ob sie der Aufnahme ihres Referenz-Templates in die Identifizierungs-Datenbank zustimmen. Bei nicht registrierten Nutzern und bei registrierten Nutzern, die ihre Einwilligung nicht erteilt haben, wird folglich ihr Name nicht automatisch für eine Markierung vorgeschlagen, da Bilder, auf denen sie abgebildet sind, das Ergebnis „keine Übereinstimmung“ ergeben.

Die Einwilligung der Person, die das Bild hochlädt, darf nicht verwechselt werden mit der Anforderung eines berechtigten Grunds für die Verarbeitung der personenbezogenen Daten anderer Personen, die möglicherweise auch auf dem Bild sind. Aus diesem Grund möchte der für die Datenverarbeitung Verantwortliche möglicherweise auf einen anderen berechtigten Grund für die Verarbeitung in den Zwischenschritten (Gesichtserkennung, Bildnormierung und Vergleich) zurückgreifen, wie beispielsweise, dass die Verarbeitung im berechtigten Interesse des für die Datenverarbeitung Verantwortlichen liegt, sofern genügend Einschränkungen und Kontrollen vorhanden sind, die die Grundrechte und -freiheiten der betroffenen Personen schützen, die nicht das Bild selbst hochgeladen haben. Zu diesen

Kontrollen würde unter anderem die Sicherstellung gehören, dass keine Daten aus der Verarbeitung aufbewahrt werden, wenn als Ergebnis „keine Übereinstimmung“ erhalten wurde (d. h. alle Templates und damit verbundenen Daten werden auf sichere Weise gelöscht). Der für die Datenverarbeitung Verantwortliche könnte auch die Bereitstellung von Werkzeugen in Erwägung ziehen, die es der das Bild hochladenden Person ermöglichen, die Gesichter derjenigen Personen unkenntlich zu machen, für die es in der Referenzdatenbank kein übereinstimmendes Template gibt. Das Enrolment des Templates einer Person in eine Identifizierungsdatenbank (und damit die Möglichkeit, eine Übereinstimmung festzustellen und Markierungsvorschläge zu unterbreiten) wäre nur mit der in Kenntnis der Sachlage erteilten Einwilligung der betroffenen Person möglich.

Im zweiten Beispiel gibt es während des Enrolment-Prozesses eindeutig die Möglichkeit, die Einwilligung der Person einzuholen, die während des Enrolment-Prozesses zum Zugang zum Gerät befugt ist. Damit die Einwilligung gültig ist, muss ein alternatives und gleichermaßen sicheres Zugangskontrollsystem vorhanden sein (wie ein sicheres Passwort). Diese alternative, privatsphärenschutzfreundliche Option sollte der Standard sein. Wenn ein einzelner Nutzer sich unter eine mit dem Gerät verbundene Kamera stellt und damit der ausdrückliche Zweck verbunden ist, Zugang zu erhalten, kann davon ausgegangen werden, dass diese Person ihre Einwilligung in die daraus resultierende Gesichtserkennung erteilt hat, die für die Authentifizierung erforderlich ist, selbst wenn es sich bei dieser Person nicht um einen befugten Nutzer des Geräts handelt. Der Umfang der erteilten Informationen muss ausreichend sein, um sicherzustellen, dass die Einwilligung gültig ist.

Die im dritten Beispiel beschriebene weitere Verbesserung der SNS-Fotobibliothek wäre eine eindeutige Verletzung der Zweckbindung. Deshalb muss vor der Einführung einer solchen Funktion die gültige Einwilligung der Person eingeholt werden und eindeutig angegeben werden, dass eine solche Bilderverarbeitung stattfindet. Das gilt auch für die in Beispiel 1 beschriebene Suchmaschine. Die von der Suchmaschine bezogenen Bilder wurden nicht für die Erfassung durch Gesichtserkennungssysteme eingestellt, sondern mit der Absicht, dass sie gesehen werden. Der Suchmaschinenbetreiber müsste die Einwilligung der betroffenen Personen für die Registrierung in dem zweiten Gesichtserkennungssystem einholen.

Das wäre auch in dem vierten Beispiel der Fall, da der Nutzer nicht davon ausgehen kann, dass Bilder, die für die Gestensteuerung bestimmt waren, weiter verarbeitet werden. Wenn der für die Datenverarbeitung Verantwortliche die Einwilligung für eine längerfristige Verarbeitung (d. h. zeitlich oder für mehrere Spiele) einholen will, muss er die Nutzer in regelmäßigen Abständen daran erinnern, dass das System in Betrieb ist und standardmäßig ausgeschaltet wird.

Stellungnahme 15/2011 zur Definition von Einwilligung betrachtet die Qualität, die Zugänglichkeit und die Sichtbarkeit von Informationen zur Verarbeitung von personenbezogenen Daten. Die Stellungnahme stellt fest:

> *„Informationen müssen den Personen direkt gegeben werden. Es reicht nicht aus, dass die Informationen irgendwo ’verfügbar’ sind.“*

Informationen zur Funktion der Gesichtserkennung in Online- oder Mobilfunkdiensten dürfen also nicht irgendwo versteckt sein, sondern müssen auf eine leicht zugängliche und verständliche Weise verfügbar sein. Dazu gehört auch, dass die Kameras selbst nicht verborgen sind. Die für die Datenverarbeitung Verantwortlichen sollten die berechtigten Erwartungen der Öffentlichkeit in Bezug auf die Privatsphäre berücksichtigen, wenn sie eine

Gesichtserkennungstechnologie einsetzen. Sie sollten auf diese Bedenken in angemessener Weise eingehen.

In diesem Zusammenhang kann die Einwilligung in das Enrolment nicht davon abgeleitet werden, dass der Nutzer die allgemeinen Geschäftsbedingungen der zugrunde liegenden Dienste generell angenommen hat, es sein denn, dass bei dem vorrangigen Ziel des Dienstes die Verwendung von Gesichtserkennung zu erwarten ist. Das liegt daran, dass Enrolment in den meisten Fällen eine zusätzliche Funktion ist und nicht in direktem Zusammenhang mit dem Betreiben des Online- oder Mobilfunkdienstes steht. Die Nutzer müssen nicht unbedingt davon ausgehen, dass eine solche Funktion aktiviert ist, wenn sie den Dienst nutzen. Daher sollten Nutzer abhängig vom Zeitpunkt der Einführung der Funktion entweder während der Registrierung oder zu einem späteren Zeitpunkt ausdrücklich die Möglichkeit haben, ihre Einwilligung in diese Funktion zu erteilen.

Damit die Einwilligung gültig ist, müssen angemessene Informationen über die Datenverarbeitung gegeben worden sein. Nutzer sollten immer die Möglichkeit haben, ihre Einwilligung auf einfache Weise zurückzuziehen. Sobald die Einwilligung in die Verarbeitung für Zwecke der Gesichtserkennung zurückgezogen wurde, ist diese unverzüglich zu beenden.

5. Spezifische Risiken und Empfehlungen

Das Risiko eines Gesichtserkennungssystems für die Privatsphäre hängt vollständig von der Art der verwendeten Verarbeitung und dem/den Zweck(en) ihrer Verwendung ab. Es gibt jedoch bestimmte Risiken, die während bestimmter Phasen der Gesichtserkennung eine größere Bedeutung haben. Der folgende Abschnitt beleuchtet die hauptsächlichen Risiken und gibt Empfehlungen für bewährte Verfahren.

5.1. Rechtswidrige Verarbeitung zu Zwecken der Gesichtserkennung

Im Online-Bereich können die für die Datenverarbeitung Verantwortlichen auf viele Arten Bilder erhalten, beispielsweise, indem sie von den Nutzern der Online- oder Mobilfunkdienste, von deren Freunden oder Kollegen oder von Dritten bereitgestellt werden. Auf den Bildern können die Gesichter der Nutzer selbst abgebildet sein und/oder die Gesichter von anderen registrierten oder nicht registrierten Nutzern oder sie können ohne die Kenntnis der betroffenen Person beschafft worden sein. Unabhängig davon, auf welche Weise diese Bilder beschafft wurden, muss für ihre Verarbeitung eine Rechtsgrundlage vorliegen.

Empfehlung 1: Wenn der für die Datenverarbeitung Verantwortliche das Bild direkt erhält (wie z. B. in den Beispielen 2 und 4), muss er sicherstellen, dass die gültige Einwilligung der betroffenen Personen bereits vor der Erfassung vorliegt, und ausreichende Informationen bereitstellen, wenn eine Kamera für die Zwecke der Gesichtserkennung genutzt wird.

Empfehlung 2: Wenn Einzelpersonen digitale Bilder haben und diese bei Online- oder Mobilfunkdiensten für Zwecke der Gesichtserkennung hochladen, müssen die für die Datenverarbeitung Verantwortlichen sicherstellen, dass die die Bilder hochladenden Personen in die Verarbeitung der Bilder eingewilligt haben, die möglicherweise für Zwecke der Gesichtserkennung durchgeführt wird.

Empfehlung 3: Wenn für die Datenverarbeitung Verantwortliche digitale Bilder von Personen von Dritten erhalten (z. B. wenn sie diese von einer Website kopieren oder von einem anderen für die Datenverarbeitung Verantwortlichen kaufen), müssen sie die Quelle der Bilder und den Kontext, in dem die Originalbilder erworben und verarbeitet werden, sorgfältig prüfen und auch, ob die betroffenen Personen einer solchen Verarbeitung zugestimmt hatten.

Empfehlung 4: **Die f**ür die Datenverarbeitung Verantwortlichen müssen sicherstellen, dass digitale Bilder und Templates nur für den angegebenen Zweck genutzt werden, für den sie zur Verfügung gestellt wurden. Die für die Datenverarbeitung Verantwortlichen sollten technische Kontrollen einführen, um das Risiko zu reduzieren, dass digitale Bilder durch Dritte für Zwecke weiterverarbeitet werden, für die der Nutzer keine Einwilligung erteilt hat. Sie sollten für die Nutzer auch Werkzeuge bereitstellen, mit denen diese die Sichtbarkeit der von ihnen hochgeladenen Bilder überprüfen können, wenn die Verfügbarkeit für Dritte standardmäßig eingeschränkt ist.

Empfehlung 5: **Die f**ür die Datenverarbeitung Verantwortlichen müssen sicherstellen, dass die Bilder von Personen, die keine registrierten Nutzer des Dienstes sind und die in eine solche Verarbeitung nicht auf eine andere Weise eingewilligt haben, nur soweit verarbeitet werden, wie es im begründeten Interesse des für die Datenverarbeitung Verantwortlichen liegt. Beim ersten Beispiel würde das das Einstellen der Verarbeitung und Löschen aller Daten im Falle des Ergebnisses „keine Übereinstimmung“ bedeuten.

Sicherheitsverletzung während der Übermittlung
Im Fall von Online- und Mobilfunkdiensten ist es wahrscheinlich, dass zwischen dem Erwerb des Bildes und den weiteren Verarbeitungsschritten (z. B. dem Hochladen des Bildes von einer Kamera auf eine Website für die Merkmalsextraktion und den Vergleich) eine Datenübermittlung stattfindet.

Empfehlung 6: Der für die Datenverarbeitung Verantwortliche muss geeignete Schritte unternehmen, um die Sicherheit der Datenübermittlung sicherzustellen. Dazu können eine Verschlüsselung der Kommunikationskanäle oder des erworbenen Bildes selbst zählen. Sofern möglich, und insbesondere im Bereich der Authentifizierung/Verifizierung, sollte die Verarbeitung vor Ort vorgezogen werden.

5.2. Gesichtserkennung, Bildnormierung, Merkmalsextraktion

Datenminimierung
Von Systemen zur Gesichtserkennung erstellte Templates enthalten möglicherweise mehr Daten, als für den/die angegebenen Zweck(e) benötigt werden.

Empfehlung 7: **Die f**ür die Datenverarbeitung Verantwortlichen müssen sicherstellen, dass die aus einem digitalen Bild für die Erstellung eines Templates extrahierten Daten nur die Informationen enthalten, die für den angegebenen Zweck erforderlich sind, und so eine weitere Verarbeitung verhüten. Templates sollten nicht zwischen Gesichtserkennungssystemen übertragbar sein.

Sicherheitsverletzungen während der Datenaufbewahrung
Die Identifizierung und Authentifizierung/Verifizierung erfordern wahrscheinlich die Speicherung des Templates für die Verwendung bei einem späteren Vergleich.

Empfehlung 8: Der für die Datenverarbeitung Verantwortliche muss überlegen, wo die Daten am besten gespeichert werden. Das kann auch im Gerät des Nutzers oder im System des für die Datenverarbeitung Verantwortlichen geschehen. Der für die Datenverarbeitung Verantwortliche muss geeignete Schritte unternehmen, um die Sicherheit der gespeicherten Daten sicherzustellen. Dazu kann die Verschlüsselung des Templates gehören. Ein unbefugter Zugang zu dem Template oder dem Speicherort sollte nicht möglich sein. Insbesondere im Fall der Gesichtserkennung für Zwecke der Verifizierung können biometrische Verschlüsselungstechniken verwendet werden. Bei diesen Techniken ist der kryptographische Schlüssel direkt an die biometrischen Daten geknüpft und wird nur dann erneut erstellt, wenn das richtige, biometrische Daten einer Person zur Verifizierung vorgelegt wird. Es wird kein Bild oder Template gespeichert (folglich eine Art „nicht verfolgbarer Biometrie“).

Zugang durch die betroffene Person

Empfehlung 9: Der für die Datenverarbeitung Verantwortliche sollte den betroffenen Personen geeignete Mechanismen zur Verfügung stellen, damit sie gegebenenfalls ihr Zugangsrecht sowohl auf die Originalbilder als auch auf die im Zusammenhang mit der Gesichtserkennung generierten Templates ausüben können.

Brüssel, den 22. März 2012

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM