«DEIN SMART-TV SCHAUT ZURÜCK UND ERKENNT DICH»: EINE DATENSCHUTZRECHTLICHE PERSPEKTIVE

Žiga Škorjanc

Mag. Žiga Škorjanc, Universitätsassistent, Universität Wien, Institut für Innovation und Digitalisierung im Recht,
Schenkenstraße 4/ 2. Stock, 1010 Wien, AT,
ziga.skorjanc@univie.ac.at; https://id.univie.ac.at/

Schlagworte: ***Internet der Dinge, Smart-TV, Gesichtserkennung, Bildverarbeitung, Rechtmäßigkeit der Verarbeitung, ausdrückliche Einwilligung***

Abstract: *Ein Smart-TV kann mit seiner (eingebetteten oder externen) Kamera digitale Bilder von Einzelpersonen aufzeichnen. Im Rahmen der Smart-TV-Dienste werden die aufgenommenen Gesichtsbilder oft zur Identifizierung oder Authentifizierung natürlicher Personen verarbeitet. Dieser Beitrag befasst sich mit diesem Spezialfall der Bildverarbeitung und geht vor allem auf die Frage der möglichen Rechtsgrundlagen ein.*

1. Einleitende Bemerkungen zum Smart-TV

1.1. Als Teil des Internets der Dinge

Das «Internet der Dinge»[1] ist längst nicht mehr auf Smart Factories und Connected Cars beschränkt, sondern entwickelt sich unaufhaltsam in Richtung Smart Home und Smart Living, wo es zur Vernetzung von Alltagsgegenständen kommt, die zuvor auch ohne kommunikative Anbindung funktioniert haben.[2]

Das Paradebeispiel für diese Entwicklung ist das omnipräsente Verbraucherprodukt TV bzw. nunmehr Smart-TV, auch intelligenter Fernseher oder Hybrid-TV genannt. Diese Bezeichnung wird für Fernsehgeräte verwendet, die mit (eingebetteten) **Sensoren** und Computer-Zusatzfunktionen, insbesondere **Internet-Fähigkeit**, ausgestattet sind. Neben der TV-Funktion verfügen diese Geräte u.a. über Zusatzschnittstellen wie z.B. USB, Bluetooth und WLAN und meist über eine Hybrid Broadcasting Broadband TV («HbbTV»)-Funktionalität. Diese Konnektivität macht das Smart-TV zu einem wichtigen Element im Internet der Dinge.[3]

1.2. Als datenschutzrechtlich relevanten Vorgang

Das Internet der Dinge bringt in der Regel mit sich, dass Daten verarbeitet werden, die bestimmte oder bestimmbare natürliche Personen betreffen und somit als personenbezogene Daten i.S.v. Art. 4 Z. 1 Datenschutz-Grundverordnung (DSGVO)[4] gelten.[5] Auch Smart-TVs erfassen mit ihren Sensoren (z.B. Kameras, Mikrofone und Bewegungssensoren) Daten (Bilder, Geräusche, Bewegung), die für eine Reihe von datenschutzrecht-

---

1 Zum Begriff «Internet der Dinge» vgl. etwa Artikel-29-Datenschutzgruppe, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223 (angenommen am 16. September 2014), S. 4.

2 Grünwald/Nüssing, Machine-to-Machine (M2M)-Kommunikation – Regulatorische Fragen bei der Kommunikation im Internet der Dinge, MMR 2015, 378.

3 Düsseldorfer Kreis, Orientierungshilfe- Datenschutzanforderungen an Smart-TV-Dienste, 15-16 September 2015, S. 5, 7: HbbTV bedeutet, dass sowohl das Rundfunksignal (Broadcasting) als auch das Breitbandinternet (Broadband) genutzt werden, um dem Fernsehzuschauer neben der Rundfunksendung auch zahlreiche weitere Zusatzinformationen anzubieten; Cappello M. (Hrsg.), Smart-TV und Datenschutz, IRIS Spezial 2015-2, Europäische Audiovisuelle Informationsstelle, Straßburg, 2016, S. 12.

4 Verordnung (EU) 2016/679, ABl. L 119/1, 1.

5 Artikel-29-Datenschutzgruppe, Internet der Dinge, WP 223, S. 4.

lich relevanten **Funktionen wie Gesichtserkennung**, Spracherkennung und Bewegungssteuerung genützt werden.[6]

Die Nutzung eines Smart-TVs setzt mitunter ein Zusammenwirken mehrerer Akteure, welche unterschiedliche datenschutzrechtliche Rollen innehaben können, voraus. Bei unterschiedlichen Smart-TV-Diensten können Gerätehersteller, HbbTV-Anbieter, Portalbetreiber, App-Store-Betreiber, App-Anbieter oder Betreiber von Personalisierungsdiensten (Empfehlungsdienste) als datenschutzrechtliche **Verantwortliche** die von Smart-TV erhobenen Daten verarbeiten.[7] Dies ist im Einzelfall zu prüfen (vgl. Punkt 2.1.1.).

Im Folgenden wird untersucht, auf welche Rechtsgrundlage sich der Verantwortliche bei der Verarbeitung von Bilddaten zum Zwecke der Gesichtserkennung und dieser zeitlich vorgelagerten Bildaufnahmen stützen kann.

2. Bildaufnahmen und Gesichtserkennung durch das Smart-TV

Ein Smart-TV kann mit (externer oder eingebauter) Kamera **digitale Bilder von Einzelpersonen aufzeichnen und** diese Bilddaten **zur Gesichtserkennung verwenden**. Dadurch kann nicht nur ein Rückschluss auf die Zahl der Zuschauer bei bestimmten Angeboten gezogen werden, vielmehr ermöglicht die Gesichtserkennung in vielen Fällen auch die eindeutige Identifizierung einer Person und ist daher als ein biometrisches System zu betrachten. Ferner ermöglicht die Gesichtserkennung auch etwa die Erstellung von Nutzerprofilen auf der Grundlage von Sehgewohnheiten,[8] die sich erheblich auf die Privatsphäre und auf das Recht des Einzelnen auf Datenschutz auswirken kann.[9]

2.1. Zulässigkeit der biometrischen Gesichtserkennung nach der DSGVO

2.1.1. Verarbeitung biometrischer Daten

Wie nach der Datenschutzrichtlinie (DSRL)[10] können Bilddaten auch nach der Konzeption der DSGVO personenbezogene Daten sein. Dies ist der Fall, wenn auf einem (digitalen) Bild «*ein klar sichtbares Gesicht einer Person abgebildet ist, das es ermöglicht, diese Person zu identifizieren*».[11] Bilder können auch personenbezogene Daten von mehr als einer Person enthalten.[12]

Die DSGVO hat zusätzlich den Begriff der biometrischen Daten eingeführt[13] und definiert diese als «*mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie* ***Gesichtsbilder*** *oder daktyloskopische Daten*».[14] Die Verarbeitung

---

6 Cappello M., Smart-TV und Datenschutz, 2016, S. 15.

7 Düsseldorfer Kreis, Smart-TV-Dienste, S. 9ff; Artikel-29-Datenschutzgruppe, Internet der Dinge, WP 223, S. 12ff (15): Nutzer der Smart-TV-Dienste (und oft auch Nicht-Nutzer, wie etwa mit dem Nutzer zusammenwohnende Personen), insbesondere auch der Inhaber des Geräts, sind betroffene Personen und keine Verantwortlichen eines Smart-TV-Dienstes.

8 **Bei der Gesichtserkennung selbst handelt es sich nicht um Profiling** gem. Art. 4 Z. 4 DSGVO, weil weder «*persönliche Aspekte*» der betroffenen Personen, wie etwa persönliche Vorlieben oder Interessen, bewertet noch die betroffenen Personen selbst klassifiziert werden; Klabunde in Ehmann/Selmayr, DS-GVO[2] Art 4 Rz 30.

9 Cappello M., Smart-TV und Datenschutz, 2016, S. 16, 62; Artikel-29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192 (angenommen am 22. März 2012), S. 1; Artikel-29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, WP 193 (angenommen am 27. April 2012), S. 3ff.

10 ErwGr 14 Richtlinie 1995/46/EG, ABl. L 1995/281, 31 i.d.F. ABl. L 2003/284, 1: «*In Anbetracht der Bedeutung der gegenwärtigen Entwicklung im Zusammenhang mit der Informationsgesellschaft bezüglich Techniken der Erfassung, Übermittlung, Veränderung, Speicherung, Aufbewahrung oder Weitergabe von personenbezogenen Ton- und* ***Bilddaten*** *muß diese Richtlinie auch auf die Verarbeitung dieser Daten Anwendung finden*».

11 Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 4.

12 Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 4.

13 Schwaiger, Biometrische Gesichtserkennung in Jahnel, Jahrbuch Datenschutzrecht 2016, 193 (200).

14 Art. 4 Z. 14 DSGVO; vgl. bereits Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff «personenbezogene Daten», WP 136 (angenommen am 20. Juni 2007), S. 9f.

von «*biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person*» ist als Verarbeitung besonderer Kategorien personenbezogener Daten anzusehen und daher nur unter den strengen Voraussetzungen des Art. 9 Abs. 2 DSGVO nicht untersagt (*abgestuftes Schutzkonzept*).

Die Verarbeitung von Bilddaten ist allerdings «***nur** dann von der Definition des Begriffs «biometrische Daten» erfasst […], **wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen**»,* und eine entsprechende Auswertungsabsicht besteht.[15] Erfasst ist unter anderem die digitale bzw. automatisierte Datengewinnung durch eine **Gesichtserkennungssoftware**, welche die Identifizierung von abgebildeten Personen ermöglicht.[16] Solche Gesichtserkennungssoftwares werden **auch bei Smart-TV-Diensten** eingesetzt.[17]

Der für die Datenverarbeitung Verantwortliche ist in der Regel der Anbieter des jeweiligen Smart-TV-Dienstes, der die Gesichtserkennungssoftware einsetzt (vgl. Punkt 1.2.).[18] Oft handelt es sich dabei um den App-Anbieter.

2.1.2. Rechtsgrundlage und Handlungsmöglichkeiten der Mitgliedstaaten

Der normative Mehrwert der Einstufung von biometrischen Daten als besondere Kategorie personenbezogener Daten liegt in der Nichtanwendbarkeit des Art. 6 Abs. 1 DSGVO, insbesondere der Interessenabwägung mit berechtigten Interessen des Verantwortlichen oder eines Dritten (lit. f).[19] Des Weiteren ist die Verarbeitung auf vertraglicher Basis (lit. b) grundsätzlich ausgeschlossen.[20]

Da weder die Interessenabwägung noch die Vertragserfüllung als Rechtsgrundlage der Verarbeitung von biometrischen Daten im Rahmen der Smart-TV-Dienste in Frage kommen, kann die Gesichtserkennung durch ein Smart-TV in der Praxis – wie auch sonst die Verarbeitung von besonderen Datenkategorien im Internet der Dinge – nur auf die **ausdrückliche** (also nicht bloß konkludente) **Einwilligung der betroffenen Person** gem. Art. 9 Abs. 2 lit. a DSGVO gestützt werden.[21]

Die Mitgliedstaaten sind zwar nicht berechtigt, weitere Ausnahmen vom Verarbeitungsverbot gem. Art. 9 Abs. 1 DSGVO zu schaffen, dürfen hingegen aber «*zusätzliche Bedingungen, einschließlich Beschränkungen*» für die Verarbeitung von biometrischen Daten in spezifizierten Konstellationen «*einführen oder aufrechterhalten*».[22] Die Regelung der Art. 9 DSGVO stellt daher ein europarechtliches **Mindestschutzniveau** dar, **das durch nationales Recht nicht unterschritten werden darf**.[23]

Zu prüfen ist im nächsten Schritt, ob das österreichische Datenschutzrecht weitere Verschärfungen enthält, die sich auf die Gesichtserkennung im Rahmen der Smart-TV-Dienste auswirken (können).

---

15 ErwGr 51 Satz 3 DSGVO; Art. 9 Abs. 1 DSGVO; Schulz in Gola, DS-GVO^2 Art 9 Rz 14.

16 Kampert in Sydow, Europäische Datenschutzgrundverordnung^2 (2018) Art 4 Rz 184; Schiff in Ehmann/Selmayr, Datenschutz-Grundverordnung^2 (2018) Art 9 Rz 27; Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 5.

17 Cappello M., Smart-TV und Datenschutz, 2016, S. 16.

18 Vgl. auch Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 5.

19 Schiff in Ehmann/Selmayr, DS-GVO^2 Art 9 Rz 27.

20 Art. 6 Abs. 1 lit. b DSGVO; Schulz in Gola, DS-GVO^2 Art 9 Rz 6: Eine Verarbeitung von sensiblen Daten auf vertraglichen Basis ist nur bei Subsumtion unter einen spezifischen Erlaubnistatbestand des Art. 9 Abs. 2 DSGVO möglich (z.B. aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs nach lit. h).

21 Artikel-29-Datenschutzgruppe, Internet der Dinge, WP 223, S. 17, 20; zur Big Data mit gleichem Ergebnis Schiff in Ehmann/Selmayr, DS-GVO^2 Art 9 Rz 68.

22 Art. 9 Abs. 4 DSGVO; ErwGr 53 Satz 4 DSGVO; Schiff in Ehmann/Selmayr, DS-GVO^2 (2018) Art 9 Rz 64.

23 Kampert in Sydow, EU-DSGVO^2 Art 9 Rz 60.

2.2. Zulässigkeit der Bildverarbeitung nach österreichischem Datenschutzgesetz

2.2.1. Allgemeines

Die DSGVO enthält keine besonderen Bestimmungen zur Zulässigkeit der Verarbeitung von Bilddaten, die nicht als biometrische Daten zu qualifizieren sind, bot allerdings den Anlass für den nationalen Gesetzgeber die Bestimmungen über die Bildverarbeitung (vormals Videoüberwachung) grundlegend zu überarbeiten.[24]

Nach der Einschätzung des österreichischen Gesetzgebers hat sich die Regelung zur Videoüberwachung im DSG 2000 grundsätzlich bewährt. Im DSG ist die «*Bildaufnahme*» daher weiterhin als **besondere Datenverarbeitung** geregelt, wobei sich der Gesetzgeber bei der Erlassung bzw. Aufrechterhaltung der Regelung, die nunmehr in §§ 12 f DSG enthalten ist, auf Art. 6 Abs. 2 und 3 sowie Art. 23 DSGVO und Kap IX DSGVO iVm ErwGr 10 gestützt hat.[25] Da in der DSGVO keine spezifische Öffnungsklausel für Bildverarbeitung vorgesehen ist, ist bereits fraglich, ob die Mitgliedstaaten überhaupt befugt sind, eine nationale Norm zur Videoüberwachung für private, nicht hoheitliche Zwecke zu erlassen.[26]

Die Bilderfassung ist **Grundvoraussetzung für die Gesichtserkennung**.[27] Die Zulässigkeit der Aufnahme digitaler Bilder von Einzelpersonen durch einen Smart-TV wird daher im Folgenden aus der Sicht der neuen Regelungen der Bildverarbeitung beleuchtet. Vor allem wird untersucht, ob sich daraus weitere Einschränkungen für die Gesichtserkennung ergeben.

Es ist darauf hinzuweisen, dass Smart-TV-Dienste auch zu anderen Zwecken als der Gesichtserkennung Bilder aufnehmen und daher die nachstehenden Ausführungen auch bei sonstigen Bildverarbeitungen zu beachten sind (z.B. Erkennung der Anzahl der Zuschauer bei bestimmten Angeboten zum Zweck der Optimierung des Empfehlungsdienstes).

2.2.2. Bildaufnahme durch Smart-TV

Anders als noch bei der Regelung der Videoüberwachung nach DSG 2000, erfasst die neue Regelung «*grundsätzlich alle **Bildaufnahmen durch Verantwortliche des privaten Bereichs***» und hat somit einen deutlich breiteren Anwendungsbereich.[28] Umfasst sind daher nicht nur eine systematische oder fortlaufende Feststellung von Ereignissen, sondern auch Einzelaufnahmen, die bspw. mit einem Smartphone gemacht werden.[29] Nicht umfasst sind hingegen Bildaufnahmen zur Vollziehung hoheitlicher Aufgaben.[30]

Das DSG definiert eine Bildaufnahme als «***die durch Verwendung technischer Einrichtungen zur Bildverarbeitung** vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken. Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen*».[31] Der Begriff Bildaufnahme soll weit ausgelegt werden.[32]

Da diese Tatbestandsmerkmale bei der Aufnahme der digitalen Bilder von Einzelpersonen durch die Kamera des Smart-TVs erfüllt sind,[33] ist im nächsten Schritt zu prüfen, auf welche Rechtsgrundlage die Bildverarbeitung durch ein Smart-TV gestützt werden darf.

---

24 Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl, Datenschutzgesetz (2018) § 12 Anm 6.

25 ErIAB zu den §§ 12 und 13 idF des Datenschutz-Anpassungsgesetzes 2018, 1761 BIgNR 25. GP 8f.

26 Kastelitz/Hötzendorfer/Tschohl in Knyrim, DatKomm Art 6 DSGVO (Stand 1.10.2018, rdb.at) Rz 79 mwN (vgl. FN 268f); Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl, DSG § 12 Anm 20.

27 Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 2.

28 ErIAB zu den §§ 12 und 13 idF des Datenschutz-Anpassungsgesetzes 2018, 1761 BIgNR 25. GP 8f; Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl, DSG § 12 Anm 7f.

29 Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl, DSG § 12 Anm 9.

30 ErIAB zu den §§ 12 und 13 idF des Datenschutz-Anpassungsgesetzes 2018, 1761 BIgNR 25. GP 8f.

31 § 12 Abs. 1 DSG.

32 ErIAB zu den §§ 12 und 13 idF des Datenschutz-Anpassungsgesetzes 2018, 1761 BIgNR 25. GP 8f.

33 Dies dürfte bei Einsatz von Machine Vision Systems («*MVS*») generell der Fall sein, wenn u.a. natürliche Personen abgelichtet werden, zum Begriff MVS vgl. etwa https://www.techopedia.com/definition/30414/machine-vision-system-mvs.

2.2.3. Rechtsgrundlage

Das DSG sieht eine Liste von **Erlaubnistatbeständen** vor. Danach ist eine Bildaufnahme zulässig, wenn (Z 1) sie im lebenswichtigen Interesse einer Person erforderlich ist, (Z 2) die (ausdrückliche oder konkludente) Einwilligung der betroffenen Person vorliegt, (Z 3) sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder (Z 4) im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.[34] In sämtlichen Fällen sind besondere Vorgaben nach § 13 DSG (Protokollierung, Löschungspflicht, Kennzeichnungspflicht und Auskunftspflicht) zu berücksichtigen.

Wie die Vorgängerregelung in § 50a Abs. 5 und 7 DSG 2000 enthält auch § 12 DSG im Abs. 4 eine Liste an **Verarbeitungsverboten**, die teilweise bei der Bildverarbeitung im Rahmen der Erbringung von Smart-TV-Diensten einschlägig sind. In diesem Zusammenhang ist wiederum fraglich, ob aus der DSGVO die Befugnis des nationalen Gesetzgebers, solche Einschränkungen vorzunehmen, abgeleitet werden kann.[35] Für die Zwecke dieses Beitrags wird von der Anwendbarkeit der geltenden nationalen Bestimmungen ausgegangen und deren Einfluss auf die Smart-TV-Dienste untersucht.

Gänzlich verboten hat der österreichische Gesetzgeber «*die Auswertung von mittels Bildaufnahmen gewonnenen personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) als Auswahlkriterium*».[36] Diese Bestimmung ist dem § 50a Abs. 7 DSG 2000[37] nachgebildet und soll die betroffenen Personen vor Gefahr einer Diskriminierung schützen.[38] Die Suche innerhalb der Bilddaten nach besonderen Kategorien der personenbezogenen Daten (z.B. Hautfarbe oder gesundheitlichen Einschränkungen)[39] wäre bei einer Zuordnung der (identifizierten) betroffenen Personen zu bestimmten Nutzerkategorien, etwa zum Zwecke der (diskriminierenden) personalisierten Werbung, denkbar (z.B. zusätzliche Werbespots für Subprime-Kredite oder Korrekturbrillen). Hingegen birgt die Durchsuchung von Bilddaten nach einer bestimmten Person im Rahmen der Gesichtserkennung, wenn auch unter Verwendung von biometrischen Daten, (an sich) nicht die Gefahr der Diskriminierung und fällt nicht unter diesen Tatbestand, (zumindest) wenn damit kein verpöntes Motiv verfolgt wird. So sind ausweislich der Materialien auch die «*Zutrittskontrollen auf der Basis eines Abgleichs biometrischer Bilddaten*» zulässig (siehe dazu sogleich).[40]

Unzulässig ist weiters «*der automationsunterstützte Abgleich von mittels Bildaufnahmen gewonnenen personenbezogenen Daten ohne ausdrückliche Einwilligung und für das Erstellen von Persönlichkeitsprofilen mit anderen personenbezogenen Daten*».[41] Einerseits ist daher der **Vergleich von Bilddaten mit anderen personenbezogenen Daten** (nicht nur anderen Bilddaten) **für das Erstellen von Persönlichkeitsprofilen** – gemeint ist m.E. Profiling i.S.d. Art. 4 Z. 4 DSGVO – **generell ausgeschlossen**.[42] Anderseits ist ein Vergleich von Bilddaten zu einem anderen Zweck, etwa bei «*Zutrittskontrollen auf der Basis eines Abgleichs biometrischer Bilddaten»,* nur mit ausdrücklicher Einwilligung der betroffenen Person zulässig.[43] Somit dürfen Bilddaten nicht durch die Bewertung der auf den Bildaufnahmen ersichtlichen persönlichen Aspekten (z.B. wahrscheinliches Alter, Geschlecht, Körpergröße, Gewicht, ethnische Herkunft oder sogar Stimmung/Laune

---

34 § 12 Abs. 2 DSG; Letzter Erlaubnistatbestand wird durch drei Fallgruppen beispielhaft konkretisiert, vgl. § 12 Abs. 3 DSG; Kastelitz/Hötzendorfer/Tschohl in Knyrim, DatKomm Art 6 DSGVO Rz 84.

35 Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl, DSG § 12 Anm 21: Unstrittig ist hingegen, dass der nationale Gesetzgeber die Bildaufnahme zum Zwecke der Kontrolle von Arbeitnehmern (Z. 4) untersagen darf.

36 § 12 Abs. 4 Z. 4 DSG.

37 *«Mit einer Videoüberwachung gewonnene Daten von Betroffenen dürfen […] nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden.»*

38 ErläutRV 472 BlgNR 24. GP 19:*«eine automationsunterstützte Suche nach «unerwünschten Personen»».*

39 König in Jelinek/Schmidl/Spanberger, Datenschutzgesetz (2018) § 12 Anm 16.

40 ErlAB zu § 12 Abs. 4 Z. 3 DSG i.d.F. des Datenschutz-Deregulierungs-Gesetzes 2018, 98 BlgNR 26. GP 4.

41 § 12 Abs. 4 Z. 3 DSG.

42 König in Jelinek/Schmidl/Spanberger, Datenschutzgesetz (2018) § 12 Anm 15; zum Profiling vgl. FN 9.

43 König in Jelinek/Schmidl/Spanberger, Datenschutzgesetz (2018) § 12 Anm 15.

der abgebildeten Person) in die Profilbildung einfließen; hingegen ist m.E. die Verwendung von Bilddaten zur Authentifizierung bzw. Verifizierung (anstelle eines Passworts) vom Profilinhaber zulässig.[44]

Ferner sind ohne deren ausdrückliche Einwilligung Bildaufnahmen der betroffenen Person in deren höchstpersönlichen Lebensbereich verboten.[45] Nach der Judikatur des OGH stellt der höchstpersönliche Lebensbereich «*den Kernbereich der geschützten Privatsphäre […]. Dieser höchstpersönliche Kernbereich ist nicht immer eindeutig abgrenzbar, es ist aber davon auszugehen, dass jedenfalls die Gesundheit, das Sexualleben und das Leben in und mit der Familie dazu gehören*».[46] Zum höchstpersönlichen Lebensbereich gehört jedenfalls die Privatwohnung der betroffenen Person, wo ein Smart-TV in der Regel genutzt wird.[47]

Im Ergebnis erfordert die Bildaufnahme durch ein Smart-TV in der Regel eine **ausdrückliche Einwilligung der betroffenen Person** gem. Art. 9 Abs. 2 lit. a DSGVO.

Werden die Bilddaten nach deren Erhebung nicht ausschließlich im Smart-TV-Gerät verarbeitet, sondern anschließend in einem zweiten Schritt übermittelt (z.B. Speicherung auf dem Cloud Server; Bildverarbeitung durch eine webbasierte Software) ist ferner zu beachten, dass auf diese Übermittlung wiederum die Erlaubnis- und Verbotstatbestände des § 12 Abs. 2 und 4 DSG anzuwenden sind.[48] Für die Übermittlung von im Wege einer zulässigen Bildaufnahme ermittelten Bilddaten ist daher eine (weitere) ausdrückliche Einwilligung notwendig. Sollten diese Bilddaten in ein Drittland übermittelt werden, ist zusätzlich Kapitel 5 der DSGVO («*Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen*») zu beachten.

2.3. Ausdrückliche Einwilligung bei Smart-TV-Diensten

Die Materialien zu § 12 DSG verweisen hinsichtlich des Begriffs der ausdrücklichen Einwilligung auf Art. 9 Abs. 2 lit. a DSGVO und beschreiben diese als «*jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass die mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist*».[49] Damit wiederholt der Gesetzgeber die Definition der Einwilligung nach Art. 4 Z. 11 DSGVO, die allerdings auch konkludente Einwilligung umfasst.

Der Begriff «*ausdrücklich*» bezieht sich darauf, wie die betroffene Person ihre Einwilligung zum Ausdruck bringt.[50] Eine ausdrückliche Einwilligung muss unmittelbar auf die Verarbeitung besonderer Kategorien personenbezogener Daten (hier biometrischen Daten) und Bilddaten Bezug nehmen.[51] Da eine bestimmte Form der Einwilligung nicht vorgeschrieben wird, kann nach der DSGVO eine ausdrückliche Einwilligung nicht nur durch eine schriftliche (und unterschriebene) Erklärungen, sondern auch etwa durch eine **elektronische Erklärung** eingeholt werden.[52] **Im digitalen oder Online-Kontext** kann eine betroffene Person die erforderliche Erklärung bspw. durch Ausfüllen eines elektronischen Formulars, Senden einer E-Mail, Hochladen eines eingescannten Dokuments, das von der betroffenen Person unterzeichnet wurde oder durch Verwenden einer

---

44 Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 3f: Datenverarbeitungen im Beispiel 4 und wohl auch Beispiel 3 sind nach § 12 Abs 4 Z 3 DSG unzulässig; ErlAB zu § 12 Abs. 4 Z. 3 DSG i.d.F. des Datenschutz-Deregulierungs-Gesetzes 2018, 98 BlgNR 26. GP 4.

45 § 12 Abs. 4 Z. 1 DSG.

46 RIS RS0122148.

47 Vgl. König in Jelinek/Schmidl/Spanberger, Datenschutzgesetz (2018) § 12 Anm 13: diese ist für den Verantwortlichen eine fremde Privatwohnung; Kastelitz/Hötzendorfer/Tschohl in Knyrim, DatKomm Art 6 DSGVO Rz 84 (FN 319).

48 Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl, DSG § 12 Anm 22.

49 ErlAB zu § 12 Abs. 4 Z. 3 DSG i.d.F. des Datenschutz-Deregulierungs-Gesetzes 2018, 98 BlgNR 26. GP 4.

50 Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01 (zuletzt überarbeitet und angenommen am 10. April 2018), S. 22.

51 Kampert in Sydow, EU-DSGVO^2 Art 9 Rz 14.

52 Artikel-29-Datenschutzgruppe, Einwilligung, WP 259 rev.01, S, 22; Kampert in Sydow, EU-DSGVO^2 Art 9 Rz 14.

elektronischen Signatur erteilen.[53] Ferner kann ein Verantwortlicher von den Nutzern einer App oder eines Portals auch «*eine ausdrückliche Einwilligung erhalten, indem er einen Bildschirm mit «Ja»- oder «Nein»-Auswahlkästchen für das Erteilen einer ausdrücklichen Einwilligung anbietet, vorausgesetzt, in dem Text wird die Einwilligung deutlich gezeigt*».[54]

Diese Möglichkeiten stehen auch zur Einholung einer ausdrücklichen Einwilligung in die Verarbeitung von Bilddaten zum Zwecke der Gesichtserkennung und sonstige Bildverarbeitung im Rahmen der Smart-TV-Dienste zur Verfügung. Der Verantwortliche muss dabei sicherstellen, dass ausreichende Informationen bereitstellt werden und die gültige Einwilligung der betroffenen Personen bereits vor der Verarbeitung von Bilddaten vorliegt.[55]

Die ausdrückliche Einwilligung ist **von sämtlichen Personen**, deren biometrische Daten möglicherweise während der Gesichtserkennung oder sonstigen Bildverarbeitung im Rahmen der Smart-TV-Dienste verarbeitet werden, einzuholen. Dabei handelt es sich nicht nur um registrierte Nutzer, sondern auch um allfällige nicht registrierte Nutzer und Nicht-Nutzer, deren Bilddaten verarbeitet werden (z.B. Personen, die mit dem registrierten Nutzer im gemeinsamen Haushalt leben und Besucher).[56]

Wegen des Verbotes der Bildaufnahmen der betroffenen Person in deren höchstpersönlichen Lebensbereich und des Vergleichs von Bilddaten zu einem anderen Zweck als für das Erstellen von Persönlichkeitsprofilen ohne deren ausdrückliche Einwilligung, können die Verarbeitungsschritte, die notwendig sind, um zu bewerten, ob eine Person (als registrierter Nutzer oder auf andere Weise) seine Einwilligung in die Verarbeitung der Bilddaten erteilt hat oder nicht (Bilderfassung, Gesichtserkennung, Vergleich usw.) und ob somit eine Rechtsgrundlage vorhanden ist («*anfängliche Verarbeitung*»), anders als nach DSGVO nicht auf die Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (z.B. eines registrierten Nutzers) gestützt werden.[57]

Besteht bei einem Smart-TV-Dienst keine Möglichkeit, die ausdrückliche Einwilligung von sämtlichen möglicherweise betroffenen Personen (vorab) einzuholen, muss der vollständige Dienst blockiert werden.[58] Daraus ergibt sich eine nicht unwesentliche (und vom Gesetzgeber wohl unbeabsichtigte) Einschränkung der Zulässigkeit von Smart-TV-Diensten im Vergleich zur Rechtslage nach DSGVO.

3. Schlussfolgerungen

Smart-TVs können mit Kameras digitale Bilder von Einzelpersonen aufzeichnen. Im Rahmen der Smart-TV-Dienste werden die aufgenommenen Gesichtsbilder oft mit Gesichtserkennungssoftware verarbeitet, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Die verarbeiteten Bilddaten, die Gesichtsbilder enthalten, sind daher als biometrische Daten zu qualifizieren und dürfen als besondere Kategorie personenbezogener Daten nur mit ausdrücklichen Einwilligung der betroffenen Person verarbeitet werden.[59]

---

53 Artikel-29-Datenschutzgruppe, Einwilligung, WP 259 rev.01, S, 22.

54 Artikel-29-Datenschutzgruppe, Einwilligung, WP 259 rev.01, S, 22 (Beispiel 17); vgl. auch ErwGr 32 Satz 2, 3 und 6 DSGVO.

55 Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 6; zur Problematik der «geringwertigen» Einwilligungen, vgl. Artikel-29-Datenschutzgruppe, Internet der Dinge, WP 223, S. 8.

56 Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 6 und 9 (Empfehlung 5); Artikel-29-Datenschutzgruppe, Internet der Dinge, WP 223, S. 15.

57 Zur Zulässigkeit der anfänglichen Verarbeitung Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 6 und 9 (Empfehlung 5).

58 Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 6 und 9 (Empfehlung 5).

59 ErwGr 51 Satz 3 DSGVO; Art. 9 Abs. 1 DSGVO; Artikel-29-Datenschutzgruppe, Internet der Dinge, WP 223, S. 17, 20; Cappello M., Smart-TV und Datenschutz, 2016, S. 16.

Die Grundvoraussetzung der Gesichtserkennung ist die Bilderfassung.[60] Die neue Regelung der Bildverarbeitung nach DSG ist bei der Aufnahme der digitalen Bilder von Einzelpersonen durch die Kamera des Smart-TVs anzuwenden. Das DSG enthält allerdings auch mehrere Verarbeitungsverbote, die bei der Erbringung von Smart-TV-Diensten zu beachten sind. So ist der Vergleich von Bilddaten mit anderen personenbezogenen Daten für das Erstellen von Persönlichkeitsprofilen generell unzulässig. Hingegen ist der Vergleich von Bilddaten mit anderen personenbezogenen Daten für andere Zwecke, etwa zur Authentifizierung bzw. Verifizierung der betroffenen Person, bei Einholung der ausdrücklichen Einwilligung zulässig. Diese ist ferner für Bildaufnahme der betroffenen Person in deren höchstpersönlichen Lebensbereich erforderlich.

Die ausdrückliche Einwilligung in die Verarbeitung von Bilddaten zum Zwecke der Gesichtserkennung und sonstige Bildverarbeitung im Rahmen der Smart-TV-Dienste muss unmittelbar auf die Verarbeitung dieser Bilddaten Bezug nehmen. Sie ist von jeder möglicherweise betroffenen Person einzuholen, ansonsten muss der vollständige Dienst blockiert werden.

4. Literatur

Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff «personenbezogene Daten», WP 136 (angenommen am 20. Juni 2007).

Artikel-29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192 (angenommen am 22. März 2012).

Artikel-29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, WP 193 (angenommen am 27. April 2012).

Artikel-29-Datenschutzgruppe, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223 (angenommen am 16. September 2014).

Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01 (zuletzt überarbeitet und angenommen am 10. April 2018).

Bresich, Ronald/Dopplinger, Lorenz/Dörnhöfer, Stefanie/Kunnert, Gerhard/Riedl, Eckhard, Datenschutzgesetz, Linde Verlag, Wien 2018.

Cappello, Maja (Hrsg.), Smart-TV und Datenschutz, IRIS Spezial 2015-2, Europäische Audiovisuelle Informationsstelle, Straßburg, 2016.

Düsseldorfer Kreis, Orientierungshilfe- Datenschutzanforderungen an Smart-TV-Dienste, 15-16 September 2015.

Ehmann, Eugen/Selmayr, Martin, Datenschutz-Grundverordnung, 2. Auflage, C. H. Beck, München 2018.

Gola, Peter, Datenschutz-Grundverordnung, 2. Auflage, C. H. Beck, München 2018. Grünwald, Andreas/Nüssing, Christoph, Machine-to-Machine (M2M)-Kommunikation – Regulatorische Fragen bei der Kommunikation im Internet der Dinge, MMR 2015, 378.

Jelinek, Andrea/Schmidl, Matthias/Spanberger, Barbara, Datenschutzgesetz, Sigmund Freud University Press, Wien 2018.

Knyrim, Rainer, DatKomm, Praxiskommentar zum Datenschutzrecht, DSGVO und DSG, Manz Verlag, Wien 2018.

Schwaiger, Christina Maria, Biometrische Gesichtserkennung. In Jahnel, Dietmar (Hrsg.), Jahrbuch Datenschutzrecht 2016, NWV Verlag, Wien 2016, S. 193.

Sydow, Gernot, Europäische Datenschutzgrundverordnung, 2. Auflage, MANZ Verlag Wien, Nomos, Dike Verlag Zürich 2018.

[60] Artikel-29-Datenschutzgruppe, Gesichtserkennung bei Online- und Mobilfunkdiensten, WP 192, S. 2.