



Ausarbeitung

Datenschutzrechtliche Zulässigkeit des WLAN-Trackings

Datenschutzrechtliche Zulässigkeit des WLAN-Trackings

Aktenzeichen: WD 3 - 3000 - 206/17
Abschluss der Arbeit: 20.11.2017
Fachbereich: WD 3: Verfassung und Verwaltung

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

1. Fragestellung

Die Ausarbeitung thematisiert verschiedene Rechtsfragen zum sog. WLAN-Tracking. Dabei soll insbesondere geprüft werden, ob die Erfassung und zeitweise anonymisierte Speicherung von MAC-Adressen datenschutzrechtlich erlaubt ist.

Bei MAC-Adressen (Media-Access-Control) handelt es sich um physikalische Adressen für Netzwerkschnittstellen. Sie bestehen aus 48 Bit und werden oftmals als 12stellige Hexadezimalzahl dargestellt. Die jeweilige MAC-Adresse ist einzigartig und lässt damit eine konkrete Zuordnung zur Netzwerkkarte zu.¹ Dennoch wird sie, anders als etwa IP-Adressen, nicht generell von einem Internetzugangsanbieter oder einer anderen Stelle erfasst.² Die bloße Kenntnis der MAC-Adresse reicht daher regelmäßig noch nicht aus, Rückschlüsse auf den Verwender herzustellen. Für solche sind andere Informationen erforderlich, wie etwa das Bekanntsein eines konkreten Geräts und seines Verwenders. Dennoch ist es nicht ausgeschlossen, dass solche Rückschlüsse etwa durch vorhandene Informationen zum Gerät, das Erstellen von Bewegungsprofilen oder eine gleichzeitige Kameraaufzeichnung hergestellt werden können.³

Die Fragestellung hat Fälle des sog. WLAN-Trackings zum Hintergrund. Dieses dient der Erfassung von Besucherströmen auf öffentlichen Plätzen. Hierzu werden an verschiedenen Standorten in einer Innenstadt Scanner installiert, die jeweils in einem Radius von 500m die Mobiltelefone von Nutzern erfassen, bei denen die WLAN-Suchfunktion nicht deaktiviert ist. Solche aktivierten Geräte senden dauerhaft Suchsignale an Router aus, die von den aufgestellten Scannern erfasst werden. Um eine Mehrfachzählung zu vermeiden, werden die MAC-Adressen, die in diesen Signalen enthalten sind, erfasst und ausgewertet. Die MAC-Adressen werden hierbei nach Darstellung in der Medienberichterstattung codiert und so anonymisiert. Die erfassten Daten sollen zudem nach wenigen Stunden wieder gelöscht werden.⁴

Die nachfolgenden Ausführungen unterstellen, dass das beschriebene WLAN-Tracking durch nicht staatliche Stellen betrieben wird und diesen zur Erlangung eigener Erkenntnisse dient. Weiterhin wird davon ausgegangen, dass die genannten MAC-Adressen nicht zentral, etwa durch den Hersteller oder Verkäufer registriert werden und dadurch unmittelbar eine Zuordnung des jeweiligen Nutzers ermöglichen.

1 Vgl. <https://www.datenschutzbeauftragter-info.de/mac-adressen-aufbau-funktion-und-gefahren-im-netzwerk/> (letzter Zugriff: 15.11.2017).

2 Vgl. zu diesen: EuGH, Urteil vom 19.10.2016 - C-582/14 (Breyer/Deutschland).

3 Vgl. etwa: Düsseldorfer Kreis (Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich), Orientierungshilfe zu den Datenschutzerfordernungen an App-Entwickler und App-Anbieter, S. 5, abrufbar unter: https://www.lda.bayern.de/media/oh_apps.pdf (letzter Zugriff: 15.11.2017); anschaulich zu möglichen Rückschlüssen aus der MAC-Adresse auf den Nutzer: <https://www.elektronik-kompodium.de/sites/net/1406201.htm> (letzter Zugriff: 15.11.2017).

4 Vgl. etwa exemplarisch die Berichterstattung zur Situation in Pinneberg: <https://www.abendblatt.de/region/article212200759/Wie-Pinneberg-Handy-Besitzer-ortet.html> (letzter Zugriff: 15.11.2017).

2. MAC-Adressen als personenbezogene Daten nach § 3 Abs. 1 BDSG

Um den Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) zu eröffnen, müsste es sich bei den genannten MAC-Adressen zunächst um personenbezogene Daten nach § 1 Abs. 2 BDSG handeln. Nach der Legaldefinition des § 3 Abs. 1 BDSG sind dies Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Der Begriff der Einzelangaben deckt sich dabei mit dem der Information.⁵ Einzelangaben beziehen sich immer auf eine bestimmte einzelne natürliche Person.⁶ Einen Bezug zu persönlichen oder sachlichen Verhältnissen weisen diese auf, wenn sie Informationen über den Betroffenen selbst oder über einen auf ihn beziehbaren Sachverhalt enthalten.⁷ Für das Erfassen einer aus einem Handysignal stammenden MAC-Adresse lässt sich zumindest der Sachbezug herstellen, dass sich die jeweilige erfasste Person zu einem bestimmten Zeitpunkt an einem bestimmten Ort befand. Zusätzlich zu dieser Sachinformation müsste sich noch ein hinreichender Personenbezug herstellen lassen. Dieser liegt nach der genannten Legaldefinition vor, wenn die betroffene Person bestimmt oder bestimmbar ist.

2.1. Zuordnung zu einer bestimmten Person

Daten können einer bestimmten Person zugeordnet werden, wenn sich aus ihnen der Name eines Betroffenen ergibt oder sich dieser aus anderen Umständen unmittelbar ermitteln lässt.⁸ Bei der massenweisen Erfassung von MAC-Adressen dürfte ein solcher unmittelbarer Rückschluss bereits aufgrund der Datenmenge ausgeschlossen sein. Aus der MAC-Adresse selbst lässt sich zudem, wie bereits aufgezeigt, kein konkreter Name einer Person ablesen.

2.2. Zuordnung zu einer bestimmbaren Person

Um als personenbezogen zu gelten, reicht es jedoch auch aus, wenn die betroffene Person bestimmbar ist. Welchen Anforderungen die Bestimmbarkeit unterliegt, ist in der juristischen Literatur umstritten. Vertreten werden hierzu zwei Grundansätze:

Nach einem **absoluten Ansatz** reicht es für die Bestimmbarkeit aus, wenn sich der Personenbezug objektiv irgendwie und durch irgendwen herstellen lässt. Es kommt hierbei nicht auf die Möglichkeiten des konkreten Datenverarbeiters an, sondern lediglich auf objektive Möglichkeiten. Dieser

5 Schild, in: Wolff/Brink, 21. Edition, Stand: 01.08.2017, § 3 BDSG Rn. 9.

6 Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 3 BDSG Rn. 3.

7 Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 3 BDSG Rn. 5.

8 Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 3 BDSG Rn. 10.

Ansatz führt zu einer enormen Ausdehnung des Anwendungsbereichs des Datenschutzes.⁹ Im Ergebnis muss das gesamte „Weltwissen“ einbezogen werden.¹⁰ Legt man diesen weiten Ansatz der rechtlichen Beurteilung des oben beschriebenen WLAN-Trackings zugrunde, erscheint es jedenfalls nicht ausgeschlossen, dass sich technische Möglichkeiten zur Herstellung eines konkreten Personenbezugs ergeben. Eine abschließende Bewertung hierzu ist jedoch dem Einzelfall vorbehalten, der sämtliche technische Ausgestaltungen und Möglichkeiten beleuchten müsste.

Der **relative Ansatz** stellt für die Bestimmbarkeit einer betroffenen Person hingegen auf die Kenntnisse, Mittel und Möglichkeiten des jeweiligen Datenverarbeiters ab. Diesem muss es mit verhältnismäßigem Aufwand im Rahmen seiner Mittel möglich sein, den Personenbezug herzustellen.¹¹ Bei der Würdigung der oben beschriebenen Konstellation würde dieser Ansatz eher gegen einen bestimmbareren Personenbezug sprechen. Aufgrund der Codierung der Daten und der nur kurzen Speicherzeit dürfte es einem Verantwortlichen kaum möglich sein, die erfassten MAC-Adressen einer Person zuzuordnen. Selbst bei längerer Speicherdauer dürfte dies wegen der oben beschriebenen fehlenden persönlichen Zuordnung einer MAC-Adresse wenn überhaupt nur mit erheblichem Aufwand gelingen. Dennoch wäre auch hier eine abschließende Beurteilung nur im jeweiligen Einzelfall unter Berücksichtigung aller technischen Möglichkeiten möglich.

Der **Europäische Gerichtshof** (EuGH) vertritt im Rahmen der Auslegung der Datenschutzrichtlinie (RL 95/46/EG) zur Bestimmung des Personenbezugs eine eher **vermittelnde Position**, die auf den relativen Ansatz abstellt, diesen aber um einen möglichen Zugriff auf Zusatzinformationen Dritter erweitert.¹² Der EuGH hatte den Personenbezug sog. dynamischer IP-Adressen zu beurteilen. Diese werden bei jeder neuen Internetverbindung einem Rechner (und Nutzer) vom Internetanbieter zugewiesen, können von einem außenstehenden Dritten aber nicht einer konkreten Person zugeordnet werden. Ein Rückschluss auf eine Person ist letztlich nur mit den Informationen des Netzanbieters möglich.¹³ Bei der Beurteilung des Personenbezugs dieser dynamischen IP-Adressen stellte der EuGH zunächst fest, dass diese selbst keine Information über die Identität der natürlichen Person enthalten, die den Computer benutzt.¹⁴ Dennoch sei für die Einstufung als personenbezogenes Datum nicht erforderlich, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer Person befinden.¹⁵ Es reiche vielmehr aus,

9 Vgl. Schantz, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 277, unter Verweis auf: Düsseldorf Kreis, Beschluss vom 26./27.11.2009, Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten, S. 2, abrufbar unter: <https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschiessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.html> (letzter Zugriff: 15.11.2017); Schild, in: Wolff/Brink, 21. Edition, Stand: 01.08.2017, § 3 BDSG Rn. 20.

10 LG Berlin, Urteil vom 31. Januar 2013 – 57 S 87/08 –, juris Rn. 62.

11 Vgl. Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 3 BDSG Rn. 10 m.w.N.

12 Matz, Urteilsanmerkung zu: EuGH, Urteil vom 19.10.2016 - C-582/14 (Breyer/Deutschland), NJW 2016, 3582 f.

13 Zum Ganzen: Kühling/Seidel/Sivridis, Datenschutzrecht 3. Aufl. 2015, Rn. 222.

14 EuGH, Urteil vom 19. Oktober 2016 – C-582/14 –, juris Rn. 38.

15 EuGH, Urteil vom 19. Oktober 2016 – C-582/14 –, juris Rn. 43.

dass der Datenverarbeiter über Mittel verfüge, ggf. über Zusatzinformationen Dritter, die Identität einer Person zu bestimmen.¹⁶ Folgt man dem vermittelnden Ansatz des EuGH, so spricht auch hier zunächst wenig für einen Personenbezug der erfassten MAC-Adressen. Auch bei der Zuhilfenahme von Drittinformationen drängen sich jedenfalls keine offensichtlichen Möglichkeiten zur Herstellung eines solchen auf. Anders als bei den dynamischen IP-Adressen werden die MAC-Adressen grundsätzlich nicht von einem Netzanbieter erfasst. Dennoch kann ein mittelbarer Rückschluss auf die Identität der Nutzer im Rahmen aller denkbaren technischen Möglichkeiten auch nicht völlig ausgeschlossen werden. Eine abschließende Beurteilung wird sich auch hier nur im Einzelfall erreichen lassen.

Für die nachfolgenden Ausführungen soll daher grundsätzlich unterstellt werden, dass die beschriebenen MAC-Adressen einen hinreichenden Personenbezug aufweisen können, indem sie eine konkrete Person bestimmbar machen.

3. Zulässigkeit der Datenerhebung bzw. der Datenverarbeitung gem. § 4 Abs. 1 BDSG

Ordnet man die MAC-Adressen den personenbezogenen Daten zu, so richtet sich deren zulässige Erhebung bzw. Verarbeitung und Nutzung zunächst nach § 4 Abs. 1 BDSG. Die Vorschrift stellt den Grundtatbestand für alle Datenverwendungen dar und ist sowohl auf öffentliche als auch auf nicht-öffentliche Stellen anwendbar, soweit letztere jedenfalls Daten i.S.d. § 1 Abs. 2 Nr. 3 BDSG erheben oder verarbeiten.¹⁷ Nicht öffentliche Stellen fallen demnach in den Anwendungsbereich des Bundesdatenschutzgesetzes, wenn sie automatisiert Daten verarbeiten.¹⁸ Dies dürfte bei der oben beschriebenen Erfassung der MAC-Adressen der Fall sein. Daher kommt es für die weitere Prüfung darauf an, ob es sich bei der Speicherung der MAC-Adressen um eine Erhebung bzw. Verarbeitung oder Nutzung von personenbezogenen Daten handelt.

3.1. Erhebung von Daten über den Betroffenen i.S.d. § 3 Abs. 3 BDSG

Nach der Legaldefinition in § 3 Abs. 3 BDSG versteht man unter einer Erhebung das Beschaffen von Daten über den Betroffenen. Soweit der Gesetzestext von „Daten über den Betroffenen“ spricht, sind diese in der Bedeutung den personenbezogenen Daten gleichzusetzen.¹⁹ In der Literatur wird daraus geschlussfolgert, dass eine Bestimmbarkeit der Person und damit auch ein Erheben von personenbezogenen Daten ausscheidet, wenn die beschaffende Stelle einschließlich der für sie handelnden Personen zu keinem Zeitpunkt in der Lage ist, den Betroffenen zu bestimmen.²⁰ Angewendet auf den oben beschriebenen Sachverhalt könnte dieser Ansatz dazu führen, die Speicherung der MAC-Adressen als nicht personenbezogen und folglich auch nicht als Erhebung

16 EuGH, Urteil vom 19. Oktober 2016 – C-582/14 –, juris Rn. 49.

17 Bäcker, in: Wolff/Brink, 21. Edition, Stand: 01.08.2017, § 4 BDSG Rn. 2.

18 Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 1 BDSG Rn. 20.

19 Schild, in: Wolff/Brink, 21. Edition, Stand: 01.08.2017, § 3 BDSG Rn. 54.

20 Dammann, in: Simitis, 8. Aufl. 2014, § 3 BDSG Rn. 108; so auch: Schild, in: Wolff/Brink, 21. Edition, Stand: 01.08.2017, § 3 BDSG Rn. 54; ähnlich: Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 3 BDSG Rn. 43.

personenbezogener Daten anzusehen. Dazu müsste jedoch wie beschrieben jede Zugriffsmöglichkeit des Datenverarbeiters auf Informationen zum Betroffenen ausgeschlossen sein. Dafür spricht hier die sofortige Codierung der Daten sowie die kurze Speicherdauer. Dennoch wird sich auch an dieser Stelle nur im Einzelfall abschließend klären lassen, welche Zugriffsmöglichkeiten tatsächlich bestehen und ob der Datenverarbeiter zumindest die Möglichkeit hat, die Daten einer konkreten Person zuzuordnen.

3.2. Verarbeitung bzw. Nutzung von personenbezogenen Daten

Stuft man die Erfassung der MAC-Adressen als Erhebung von personenbezogenen Daten ein, so stellt sich für die weitere Verwendung dieser Daten die Frage, ob auch eine Verarbeitung bzw. Nutzung von personenbezogenen Daten vorliegt. Nach dem oben beschriebenen Sachverhalt sollen die MAC-Adressen vorübergehend gespeichert werden, um diese ggf. zur Verhinderung von Mehrfachzählungen mit anderen abzugleichen. Da jede Phase der Datenverwendung einer gesonderten Erlaubnisprüfung nach § 4 Abs. 1 BDSG bedarf,²¹ müsste diese Abgleichung, sofern es sich bei den verwendeten Informationen um personenbezogene Daten handelt, ebenfalls einer Zulässigkeitsprüfung unterzogen werden. Wie oben beschrieben wurde, sollen die erfassten MAC-Adressen unmittelbar mit der Erhebung codiert und damit anonymisiert werden. Die **Anonymisierung** stellt eine dem Datenschutzrecht bekannte Kategorie dar. Nach der Legaldefinition in § 3 Abs. 6 BDSG liegt eine solche vor, wenn personenbezogene Daten derart verändert werden, dass Einzelangaben über persönliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Liegt eine Anonymisierung in diesem Sinne vor, so ist von einem neuen Datensatz auszugehen, der keinen Personenbezug mehr aufweist.²² Dementsprechend wäre der Abgleich der Daten auch nicht als weitere Verarbeitung oder Nutzung von personenbezogenen Daten anzusehen. Auch an dieser Stelle ist jedoch eine Einzelfallprüfung erforderlich, ob die strengen Voraussetzungen einer Anonymisierung auch tatsächlich eingehalten werden. Ist es der verantwortlichen Stelle ohne großen Aufwand möglich, die Betroffenen wieder zu bestimmen oder bestimmbar zu machen, kann nicht von einer Anonymisierung ausgegangen werden.²³

4. Mögliche Zulässigkeit bei Bejahung des Personenbezugs

Bejaht man einen Personenbezug der erhobenen Daten, müssten die Anforderungen des § 4 Abs. 1 BDSG eingehalten werden. Demnach ist jede Verwendung von Daten unzulässig, solange sie nicht von einem Erlaubnistatbestand gedeckt ist.²⁴ Als Erlaubnistatbestände kommen die Einwilligung des Betroffenen sowie eine Zulässigkeit aufgrund einer Rechtsvorschrift in Betracht.

21 Vgl. Kühling/Seidel/Sivridis, Datenschutzrecht 3. Aufl. 2015, Rn. 214.

22 Vgl. Schild, in: Wolff/Brink, 21. Edition, Stand: 01.08.2017, § 3 BDSG Rn. 98; Dammann, in: Simitis, 8. Aufl. 2014, § 3 BDSG Rn. 204.

23 Dammann, in: Simitis, 8. Aufl. 2014, § 3 BDSG Rn. 200.

24 Bäcker, in: Wolff/Brink, 21. Edition, Stand: 01.08.2017, § 4 BDSG Rn. 1.

4.1. Einwilligung

Die Anforderungen an eine Einwilligung enthält § 4a BDSG. Demnach ist eine Einwilligung nur wirksam, wenn sie auf einer freien Entscheidung des Betroffenen beruht. Die Vorschrift verlangt zudem für den Regelfall die Schriftform sowie eine Hinweispflicht des Datenverarbeiters.²⁵ Eine konkludente Einwilligung wird in der Literatur teilweise abgelehnt oder nur unter engen Voraussetzungen für zulässig erachtet.²⁶ Bei der oben beschriebenen Erfassung der MAC-Adressen auf öffentlichen Plätzen dürfte in der Regel keine Einwilligung nach § 4a BDSG vorliegen. Hierfür spricht bereits die regelmäßige Unkenntnis der Besucher von der Erfassung ihrer Handysignale. Die beschriebene Datenerfassung erfolgt massenhaft und dementsprechend ohne vorherigen Hinweis. Die erfassten Personen werden daher kaum ein Bewusstsein darüber entwickeln, dass die MAC-Adressen ihres mitgeführten Handys erfasst werden. Bei diesem fehlenden Bewusstsein kann im bloßen Betreten eines Platzes keine konkludente Einwilligung erblickt werden.

4.2. Zulässigkeit aufgrund einer Rechtsvorschrift

Fehlt es an einer Einwilligung, bedarf es für die zulässige Verwendung personenbezogener Daten der Erlaubnis aufgrund einer Rechtsvorschrift. Vorschriften für die Datenverwendung nicht öffentlicher Stellen finden sich in den §§ 27 ff. BDSG. Dabei gilt es zunächst, eine Datenverarbeitung für eigene Geschäftszwecke nach § 28 BDSG von einer Datenverarbeitung zum Zwecke der Übermittlung nach § 29 BDSG abzugrenzen. Eine Datenverarbeitung für eigene Geschäftszwecke beinhaltet dabei sämtliche Datenverarbeitungsvorgänge, die für eigene private Zwecke getätigt werden. Die Bezeichnung als (Geschäfts)zweck ist insoweit missverständlich. Ein unmittelbarer wirtschaftlicher Bezug ist nicht erforderlich.²⁷ Sollen die Daten hingegen geschäftsmäßig an Dritte vermarktet werden, greift die Regelung des § 29 BDSG.²⁸ In der oben beschriebenen Konstellation dürfte der Anwendungsbereich des § 28 BDSG eröffnet sein, da die erfassten MAC-Adressen der eigenen Kenntniserlangung dienen. Sollen hingegen im Rahmen des WLAN-Trackings Daten geschäftsmäßig erhoben werden, um diese an Dritte weiterzuleiten, käme es auf die Anforderungen des § 29 BDSG und in der Konstellation zum Zwecke der Marktforschung wohl auch auf § 30 BDSG an.²⁹

4.2.1. Voraussetzungen des § 28 BDSG

§ 28 Abs. 1 BDSG lässt das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung zur Erfüllung eigener Geschäftszwecke insbesondere in drei Konstellationen

25 Vgl. Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 4a BDSG Rn. 26, ders. zum Schriftformerfordernis: Rn. 29 ff.

26 Ablehnend: Dammann, in: Simitis, 8. Aufl. 2014, § 4a BDSG Rn. 43 ff.; unter engen Voraussetzungen bejahend, etwa bei fortdauernder stillschweigender Einwilligung: Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 4a BDSG Rn. 29a; Kühling, in: Wolff/Brink, 21. Edition, Stand: 01.08.2017, § 4a BDSG Rn. 50.

27 Wolff, in: Wolff/Brink, 21. Edition, Stand: 01.08.2017, § 28, Rn. 10; Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 28 BDSG Rn. 4.

28 Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 28 BDSG Rn. 4.

29 Vgl. umfassend zu dessen Voraussetzungen: Kühling/Seidel/Sivridis, Datenschutzrecht 3. Aufl. 2015, Rn. 438 ff.

zu. Da der oben beschriebenen Erfassung der MAC-Adressen weder ein Schuldverhältnis zugrunde liegt, noch eine Datenerhebung aus allgemein zugänglichen Quellen erfolgt, wäre die Zulässigkeit im Rahmen einer **Interessenabwägung** zu bestimmen, wie sie in § 28 Abs. 1 Nr. 2 BDSG geregelt ist. Danach liegt eine zulässige Datenverwendung vor, soweit sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

4.2.2. Interessenabwägung im Einzelfall

Nach dem Wortlaut des § 28 Abs. 1 Nr. 2 BDSG darf kein Grund zur Annahme dafür bestehen, dass das schutzwürdige Interesse des Betroffenen den berechtigten Interessen der verantwortlichen Stelle überwiegt. Die geforderte Interessenabwägung lässt sich nur im Einzelfall durchführen. Sie hat dabei alle spezifischen Umstände der konkreten Datenverwendung zu berücksichtigen. Als berechnete Interessen der verantwortlichen Stelle kommen in Rahmen dieser Abwägung alle von der Rechtsordnung gebilligten Interessen in Betracht, seien sie **ideeller** oder auch **wirtschaftlicher Natur**.³⁰ Die Erfassung von MAC-Adressen zur Feststellung von Besucherzahlen in Innenstädten und damit zur besseren Bewirtschaftung und Vermarktung derselben dürfte ein hinreichendes wirtschaftliches Interesse zugrunde liegen. Die Schutzwürdigkeit der Interessen von Betroffenen ergibt sich bereits aus deren Bezug zum informationellen Selbstbestimmungsrecht.³¹ Eine abschließende Abwägung lässt sich an dieser Stelle wie ausgeführt nicht durchführen. Allgemein lässt sich zur hiesigen Konstellation jedoch sagen, dass die schutzwürdigen Interessen der Betroffenen jedenfalls solange nicht erheblich beeinträchtigt sein dürften, wie die Datenerfassung im beschriebenen eingeschränkten Umfang erfolgt und solange die sofortige Anonymisierung und begrenzte Speicherdauer gewährleistet wäre. Anders würde sich die Abwägung jedoch gestalten, wenn Bewegungsprofile erstellt würden oder etwa eine umfassende Erfassung der Anwohner möglich wäre.

5. Benachrichtigungspflichten nach § 33 Abs. 1 BDSG

Nach § 33 Abs. 1 BDSG ist ein Betroffener, dessen personenbezogene Daten ohne seine Kenntnis erhoben wurden, zu benachrichtigen. Die verantwortliche Stelle muss den Betroffenen dabei über die Speicherung, die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und ihre Identität in Kenntnis setzen. Von der Benachrichtigungspflicht bestehen nach § 33 Abs. 2 BDSG umfassende Ausnahmen. Im Einzelfall wäre daher zu prüfen, ob ein Ausnahmetatbestand einer Benachrichtigungspflicht entgegensteht.

6. Fazit

Eine allgemeine Aussage über die Zulässigkeit des WLAN-Trackings zur Feststellung von Besucherzahlen mittels einer Erfassung von MAC-Adressen ist nicht möglich. Nach derzeitigem Kenntnisstand spricht einiges dafür, MAC-Adressen, die im Rahmen der beschriebenen Verfahrensweise

30 Kühling/Seidel/Sivridis, Datenschutzrecht 3. Aufl. 2015, Rn. 379; Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 28 BDSG Rn. 24.

31 Gola/Klug/Körffler, in: Gola/Schomerus, 12. Auflage 2015, § 28 BDSG Rn. 26.

erfasst werden, nicht als personenbezogene Daten anzusehen, bzw. bei sofortiger Anonymisierung nicht von einer Erhebung personenbezogener Daten auszugehen. Unterstellt man dennoch einen Personenbezug, richtet sich die Zulässigkeit der Datenerhebung nach § 28 BDSG. Im Rahmen der im Einzelfall durchzuführenden Interessenabwägung spricht zumindest einiges dafür, dass die Interessen der Betroffenen jedenfalls nicht in erheblicher Weise beeinträchtigt wären. Dennoch ist für jeden Einzelfall eine gesonderte Interessenabwägung durchzuführen, in deren Rahmen man je nach Gewichtung der Abwägungsgüter auch zu anderen Ergebnissen gelangen kann.
