ARTIKEL-29-DATENSCHUTZGRUPPE

16/DE
WP 237

Arbeitsunterlage 01/2016 über die Rechtfertigung von Eingriffen in die Grundrechte auf Schutz der Privatsphäre und Datenschutz durch Überwachungsmaßnahmen bei der Übermittlung personenbezogener Daten (wesentliche europäische Garantien)

Angenommen am 13. April 2016

Diese Gruppe wurde mit Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG und Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von der Europäischen Kommission, Generaldirektion Justiz und Verbraucher, Direktion C (Grundrechte und Unionsbürgerschaft), 1049 Brüssel, Belgien, Büro: MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

Inhaltsverzeichnis

1. EINLEITUNG 3

2. EINGRIFFE IN GRUNDRECHTE 4

3. DIE WESENTLICHEN EUROPÄISCHEN GARANTIEN 7

4. GARANTIE A – DIE DATENVERARBEITUNG SOLLTE AUF KLAREN, PRÄZISEN UND ZUGÄNGLICHEN VORSCHRIFTEN BERUHEN. 7

5. GARANTIE B – ERFORDERLICHKEIT UND ANGEMESSENHEIT IM HINBLICK AUF DIE VERFOLGTEN LEGITIMEN ZIELE SIND NACHZUWEISEN. 8

6. GARANTIE C – ES SOLLTE EIN UNABHÄNGIGER AUFSICHTSMECHANISMUS BESTEHEN. 10

7. GARANTIE D – DEM BÜRGER MÜSSEN WIRKSAME RECHTSBEHELFE ZUR VERFÜGUNG STEHEN. 12

8. ABSCHLIESSENDE BEMERKUNGEN 14

ANHANG 1 – RECHTSPRECHUNG 16

1. Einleitung

Am 6. Oktober 2015 verkündete der Gerichtshof der Europäischen Union (im Folgenden „EuGH“) sein Grundsatzurteil in der Rechtssache *Maximilian Schrems gegen Data Protection Commissioner*[1]. Aufgrund eines Vorabentscheidungsersuchens des High Court (Irland) erklärte der EuGH die sogenannte Safe-Harbour-Entscheidung für ungültig, da darin nicht hinreichend klar dargelegt war, dass die Rechtsvorschriften der Vereinigten Staaten von Amerika (im Folgenden „USA“) ausreichende Garantien für den Schutz von aus der Europäischen Union (im Folgenden „EU“) stammenden personenbezogenen Daten bieten.

Mit der Ungültigerklärung der Safe-Harbour-Entscheidung wurden zahlreiche Datenübermittlungen in die USA unmittelbar rechtswidrig, da sich eine Vielzahl von Unternehmen bei der Übermittlung von Daten in die USA auf die Bestimmungen einer nicht länger bestehenden Entscheidung stützte. Der EuGH warf die Frage auf, in welchem Umfang möglicherweise aus Gründen der nationalen Sicherheit und der Strafverfolgung in die Grundrechte[2] der Personen eingegriffen wird, deren Daten aus der EU in die USA übermittelt werden. Da sich diese möglichen Eingriffe nicht auf die nach der Safe-Harbour-Entscheidung übermittelten Daten beschränken, wurden zudem Zweifel geäußert, ob andere Instrumente (Ad-hoc-Vertragsklauseln, Standardvertragsklauseln, verbindliche unternehmensinterne Vorschriften und Ausnahmen nach Artikel 26 Absatz 1 der Richtlinie 95/46/EG (im Folgenden „Richtlinie“)) ausreichende Garantien bieten, wenn Daten in die USA übermittelt werden.

Die Artikel-29-Datenschutzgruppe hat daher auf ihrer Sitzung vom 16. Oktober 2015 beschlossen, die Auswirkungen des Schrems-Urteils auf sämtliche Datenübermittlungen in die USA zu bewerten. Zu diesem Zweck hat die Artikel-29-Datenschutzgruppe die Rechtsprechung des EuGH zu den Artikeln 7, 8 und 47 der Charta der Grundrechte (im Folgenden „Charta“) und die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (im Folgenden „EGMR“) zu Artikel 8 der Europäischen Menschenrechtskonvention (im Folgenden „EMRK“), die sich mit Überwachungsfragen in Vertragsstaaten der EMRK befasst, inventarisiert und ausgewertet. Zusammengenommen ergibt sich aus dieser Rechtsprechung eine Orientierungshilfe dazu, was in einer demokratischen Gesellschaft als zu rechtfertigender Eingriff in die Grundrechte angesehen werden kann und was nicht. Das Ergebnis dieser Auswertung wird von der Artikel-29-Datenschutzgruppe als die vier wesentlichen europäischen Garantien bezeichnet (im Folgenden auch „Garantien“).

Diese Garantien sind von dem zu unterscheiden, was der EuGH „ein Schutzniveau der Freiheiten und Grundrechte“ nennt, „das dem in der Union aufgrund der [EU-

[1] Die gesamte Rechtsprechung, die in dieser Analyse zitiert wird, ist in Anhang 1 aufgeführt.

[2] Der in dieser Arbeitsunterlage verwendete Begriff „Grundrechte“ leitet sich aus der Charta der Grundrechte der Europäischen Union ab. Er umfasst jedoch auch die „Menschenrechte“ im Sinne der Europäischen Menschenrechtskonvention. Nach Auffassung der Artikel-29-Datenschutzgruppe sollten beide gleichermaßen geachtet werden.

Datenschutzrichtlinie] im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist.“ „Der Sache nach gleichwertig“ ist der Maßstab des EuGH für einen Angemessenheitsbeschluss nach Artikel 25 Absatz 6 der Datenschutzrichtlinie, während die wesentlichen europäischen Garantien als Orientierungshilfe bei der Prüfung dienen, ob ein Grundrechtseingriff gerechtfertigt und auf alle Datenverarbeitungsvorgänge angewandt werden kann, einschließlich Datenübermittlungen auf der Grundlage der Artikel 25 und 26 der Richtlinie.

In dieser Arbeitsunterlage wird der Hintergrund der vier wesentlichen europäischen Garantien erläutert. Die Artikel-29-Datenschutzgruppe weist darauf hin, dass diese Garantien in erster Linie auf der Rechtsprechung des EuGH und des EGMR beruhen. Sie sollten jedoch in Verbindung mit der Auslegung verschiedener Elemente des Rechtsrahmens der EU für den Datenschutz gesehen werden, die die Artikel-29-Datenschutzgruppe in früheren Stellungnahmen vorgenommen hat. Hinsichtlich der Datenübermittlungen in die USA verweist die Artikel-29-Datenschutzgruppe auf ihre Stellungnahme 01/2016 zum Schutzniveau des EU-US-Datenschutzschilds, die eine Bewertung der wesentlichen europäischen Garantien für Datenübermittlungen in die USA enthält.

2. Eingriffe in Grundrechte

Die Grundrechte auf Achtung des Privat- und Familienlebens sowie auf Schutz personenbezogener Daten sind in den Artikeln 7 und 8 der Charta festgelegt und gelten für jeden. Artikel 8 bietet darüber hinaus grundlegende Orientierungshilfen für die Datenverarbeitung, darunter die Zweckbindung, die unabhängige Überwachung durch eine Aufsichtsbehörde und die Notwendigkeit einer gesetzlich geregelten Rechtsgrundlage sowie das Auskunfts- und das Berichtigungsrecht. Im Schrems-Urteil bekräftigt der EuGH, „dass eine Unionsregelung, die einen Eingriff in die durch die Art. 7 und 8 der Charta garantierten Grundrechte enthält, nach ständiger Rechtsprechung des Gerichtshofs klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme vorsehen und Mindestanforderungen aufstellen muss, sodass die Personen, deren personenbezogene Daten betroffen sind, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen.“[3] Dieses Niveau des Schutzes der Grundrechte vor willkürlichen Eingriffen sollte gewährleistet sein, wenn Daten in ein Land übermittelt werden, dessen Schutzniveau auf der Grundlage des Artikels 25 der Richtlinie als angemessen angesehen wird. Eine ähnliche Regelung sollte auf Datenübermittlungen nach Artikel 26 der Richtlinie Anwendung finden, schon allein deshalb, weil Grundrechte nicht nur je nach der Rechtsgrundlage für eine Datenübermittlung, sondern allgemein gelten. Zudem ist darauf hinzuweisen, dass die Datenschutzbehörden nach Artikel 4 der Standardvertragsklauseln in Verbindung mit Artikel 26 Absatz 4 der Richtlinie verpflichtet sind zu prüfen, ob der Datenimporteur nach den Rechtsvorschriften eines Drittlands gezwungen ist, „vom anwendbaren Datenschutzrecht in einem Maß abzuweichen, das über die Beschränkungen

[3] Schrems, Rn. 91.

hinausgeht, die … für eine demokratische Gesellschaft erforderlich sind“[4]. Die Prüfung, ob die Grundrechte geachtet werden, kann jedoch in einem Einzelfall anders ausfallen als im Zusammenhang mit der allgemeinen Genehmigung von Datenübermittlungen in ein Drittland.

Der Grundrechtsschutz für personenbezogene Daten in Europa beruht nicht nur auf dem Unionsrecht, sondern auch auf der EMRK.[5] Unlängst hat der EGMR in der Rechtssache Zakharov seinen Standpunkt zu Eingriffen in das Grundrecht auf Achtung des Privatlebens bekräftigt. Diese können nur dann gerechtfertigt sein, wenn sie mit dem Gesetz im Einklang stehen, ein legitimes Ziel verfolgen und in einer demokratischen Gesellschaft erforderlich sind, um ein solches Ziel zu erreichen.[6]

Sowohl die Charta als auch die EMRK sehen zur Begrenzung von Einschränkungen der durch sie geschützten Rechte eine Erforderlichkeits- und Angemessenheitsprüfung vor[7]. In Artikel 52 Absatz 1 der Charta ist der Umfang möglicher Einschränkungen der Artikel 7 und 8 festgelegt: „Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.“

Gleichzeitig wird in der Einschränkungsklausel des Artikels 8 Absatz 2 EMRK präzisiert: „Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.“

Nach Auffassung beider Gerichtshöfe können Einschränkungen der Grundrechte auf Schutz der Privatsphäre und Datenschutz sowie Eingriffe in diese Grundrechte (d. h. Erhebung, Speicherung, Zugriff, Verwendung und Verbreitung in Bezug auf personenbezogene Daten nicht für die Zwecke, für sie ursprünglich übermittelt wurden, sondern aus Gründen der nationalen Sicherheit oder zu nachrichtendienstlichen Zwecken) nur dann gerechtfertigt werden, wenn sie „in einer demokratischen Gesellschaft unbedingt erforderlich“[8] sind. In ihren Urteilen haben die Gerichtshöfe recht detailliert ausgeführt, was nach ihrem Verständnis

---

[4] Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (2010/87/EU).

[5] Die Artikel-29-Datenschutzgruppe erinnert in diesem Zusammenhang an Artikel 6 Absatz 3 des Vertrags über die Europäische Union: „Die Grundrechte, wie sie in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, sind als allgemeine Grundsätze Teil des Unionsrechts.“

[6] EGMR, Zakharov, Rn. 227.

[7] Nähere Informationen unter http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15%281997%29.pdf.

[8] EGMR, Klass, Rn. 42, 48; EGMR, Malone, Rn. 81 und andere.

in einer demokratischen Gesellschaft erforderlich ist, einschließlich der Voraussetzung, dass Maßnahmen im Einklang mit den Gesetzen getroffen werden müssen und „einen Mindestschutz vor Missbrauch“[9] bieten sollten.

Darüber hinaus erkennt der EGMR bei der Prüfung der Erforderlichkeit von Maßnahmen in ständiger Rechtsprechung an, dass die Vertragsstaaten „bei der Wahl der Mittel zum Erreichen des legitimen Ziels des Schutzes der nationalen Sicherheit einen großen Ermessensspielraum haben“[10]. Dieses Recht der Länder, Rechtsvorschriften mit dem Ziel der Aufrechterhaltung der nationalen Sicherheit oder der Erhebung von Daten zu nachrichtendienstlichen Zwecken zu erlassen, wird natürlich auch von der Artikel-29-Datenschutzgruppe anerkannt. Zudem kann die nachrichtendienstliche Gewinnung von Erkenntnissen ein vollkommen legitimes Ziel sein, das eine Datenverarbeitung rechtfertigt, wie auch der EGMR, zuletzt in der Rechtssache Szabó, hervorgehoben hat.[11] Sie kann sogar geheime Überwachungsmaßnahmen umfassen, solange angemessene und wirksame Garantien gegen Missbrauch bestehen, um zu verhindern, dass die Überwachung die Demokratie unter dem Deckmantel ihrer Verteidigung untergräbt oder sogar zerstört[12].

Grundsätzlich stellen alle Datenverarbeitungsvorgänge, auch Überwachungsmaßnahmen[13], einen Eingriff dar, insbesondere wenn Daten über das Privatleben einer Person von einer Behörde gespeichert werden[14] und/oder wenn den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste und den Betreibern eines öffentlichen Kommunikationsnetzes die Pflicht auferlegt wird, Daten über das Privatleben einer Person und ihre Kommunikationsvorgänge auf Vorrat zu speichern[15]. Der Zugriff einer (für die Strafverfolgung) zuständigen Behörde auf die Daten stellt einen zusätzlichen Eingriff dar.[16] Für die Feststellung eines Eingriffs „kommt es nicht darauf an, ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten“[17].

Der EuGH und der EGMR haben in ihren Urteilen klargestellt, dass die Entscheidung darüber, ob ein gerechtfertigter Eingriff in ein Grundrecht vorliegt oder nicht, letztlich bei ihnen liegt. Wenn jedoch kein einschlägiges Urteil vorliegt, sind die Datenschutzbehörden nach ständiger Rechtsprechung befugt, Einzelfälle von Amts wegen oder aufgrund einer Beschwerde zu prüfen, um zu entscheiden, ob eine Datenübermittlung (weiter) erfolgen darf, wenn sie einen Eingriff in die Grundrechte auf Schutz der Privatsphäre und Datenschutz festgestellt haben.

---

[9] EuGH, Schrems, Rn. 91 sowie die dort angeführte Rechtsprechung.
[10] EGMR, Weber und Saravia, Rn. 106.
[11] EGMR, Szabó, Rn. 57.
[12] EGMR, Szabó, Rn. 57: „undermine or even destroy democracy under the cloak of defending it“.
[13]EGMR, Malone, Rn. 64.
[14] EGMR, Amman, Rn. 70.
[15] EuGH, Digital Rights Ireland, Rn. 34.
[16] EGMR, Leander, Rn. 48; EGMR, Rotaru, Rn. 46; EuGH, Digital Rights Ireland, Rn. 35.
[17] EuGH, Schrems, Rn. 87 sowie die dort angeführte Rechtsprechung.

3. Die wesentlichen europäischen Garantien

Die Artikel-29-Datenschutzgruppe hat die Rechtsprechung ausgewertet, um die „wesentlichen europäischen Garantien“ zu ermitteln, die vorhanden sein sollten, damit gewährleistet ist, dass Eingriffe nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist. Die wesentlichen europäischen Garantien gehen in erster Linie auf die Rechtsprechung des EuGH und des EGMR in Rechtssachen zurück, in denen es um die Anwendung der Rechte auf Schutz der Privatsphäre und Datenschutz in Europa ging. Die Garantien finden daher vor allem in den und auf die Mitgliedsstaaten der Europäischen Union und des Europarats Anwendung, wenn diese europäische oder nationale Rechtsvorschriften anwenden, die in diese Rechte eingreifen. Da Daten, die in Länder außerhalb der EU übermittelt werden, durchgehend vor willkürlichen Eingriffen geschützt werden sollten, werden die wesentlichen europäischen Garantien auch bei allen Datenübermittlungen in Drittländer gebührend zu berücksichtigen sein.

Die Artikel-29-Datenschutzgruppe weist darauf hin, dass die Garantien auf den Grundrechten beruhen, die für jeden unabhängig von seiner Staatsangehörigkeit gelten.

Nach Auswertung der Rechtsprechung ist die Artikel-29-Datenschutzgruppe zu dem Ergebnis gelangt, dass sich die Anforderungen in vier wesentlichen europäischen Garantien zusammenfassen lassen:

A. Die Datenverarbeitung sollte auf klaren, präzisen und zugänglichen Vorschriften beruhen.
B. Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele sind nachzuweisen.
C. Es sollte ein unabhängiger Aufsichtsmechanismus bestehen.
D. Dem Bürger müssen wirksame Rechtsbehelfe zur Verfügung stehen.

4. Garantie A – Die Datenverarbeitung sollte auf klaren, präzisen und zugänglichen Vorschriften beruhen.

Ein zu rechtfertigender Eingriff muss zunächst mit dem Gesetz im Einklang stehen. Der Eingriff muss hinsichtlich seiner Auswirkungen auf den Bürger vorhersehbar sein, um diesem angemessenen Schutz vor willkürlichen Eingriffen zu bieten. Die Datenverarbeitung muss deshalb auf einer präzisen, klaren und zugänglichen (d. h. öffentlichen) Rechtsgrundlage erfolgen.[18] Diese Rechtsgrundlage sollte in jedem Fall im Gesetzesrecht festgelegt werden, einschließlich der Art der Straftaten, die zu einer Überwachungsanordnung führen können, einer Definition der Personengruppen, die überwacht werden können, einer zeitlichen Begrenzung der Maßnahme, des Verfahrens für die Prüfung, Verwendung und Speicherung der gewonnenen Daten sowie der bei der Übermittlung der Daten an Dritte zu treffenden Vorkehrungen.[19] Sie muss auch die Umstände sowie die materiell- und verfahrensrechtlichen

[18] EGMR, Malone, Rn. 65, 66, 70.
[19] EGMR, Weber und Saravia, Rn. 95.

Voraussetzungen für den Zugriff der zuständigen Behörden umfassen.[20] Und schließlich gibt es nach Auffassung des Gerichtshofs keinen Grund, auf die Zugänglichkeit und Klarheit der Vorschriften für die Überwachung der Kommunikation Einzelner einerseits und für allgemeinere Überwachungsprogramme andererseits unterschiedliche Grundsätze anzuwenden.[21]

Der EGMR hat in der Rechtssache Zakharov daran erinnert, dass „Vorhersehbarkeit" im Zusammenhang mit der Überwachung des Kommunikationsverkehrs nicht dasselbe sein kann wie in vielen anderen Bereichen. Er präzisiert, dass im Falle geheimer Überwachungsmaßnahmen wie der Überwachung des Kommunikationsverkehrs Vorhersehbarkeit nicht bedeuten kann, dass der Bürger vorhersehen können sollte, wann die Behörden wahrscheinlich Maßnahmen zur Überwachung seiner Kommunikation treffen werden, sodass er sein Verhalten entsprechend anpassen kann. Da jedoch unter solchen Umständen die Gefahr von Willkür offensichtlich ist, sind klare, ausführliche Vorschriften für das Abhören von Telefongesprächen unerlässlich, insbesondere da sich die hierfür zur Verfügung stehende Technologie ständig weiterentwickelt. Die innerstaatlichen Rechtsvorschriften müssen so klar sein, dass sie den Bürgern einen angemessenen Hinweis auf die Umstände und Voraussetzungen an die Hand geben, unter denen Behörden ermächtigt sind, auf solche Maßnahmen zurückzugreifen.[22]

5. Garantie B – Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele sind nachzuweisen.

Jede Verarbeitung von Daten durch staatliche Behörden ist per definitionem ein Eingriff in die Rechte auf Schutz der Privatsphäre und Datenschutz.[23] Dies gilt auch für die Datenverarbeitung durch staatliche Behörden zu nachrichtendienstlichen Zwecken, die zwar zu rechtfertigen sein kann, jedoch nur, wenn sie im Hinblick auf ein legitimes Ziel erforderlich und angemessen ist.

Im Schrems-Urteil hat der EuGH hierzu Folgendes festgestellt: „Nicht auf das absolut Notwendige beschränkt ist eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium

[20] EuGH, Digital Rights Ireland, Rn. 61.

[21] EGMR, Liberty, Rn. 63: „The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other."

[22] EGMR, Zakharov, Rn. 229: „[T]he reference to ‚foreseeability' in the context of interception of communications cannot be the same as in many other fields. Foreseeability … cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. … It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures".

[23] Siehe zum Beispiel EuGH, Digital Rights Ireland, Rn. 36.

vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen“[24].

In der Rechtssache Szabó hat eine Kammer des EGMR darauf hingewiesen, dass der Gerichtshof angesichts dieses Fortschritts prüfen muss, ob gleichzeitig mit der Entwicklung der Überwachungsmethoden, die die Erhebung von Datenmassen zur Folge haben, auch rechtliche Garantien entwickelt wurden, die die Achtung der in der EMRK verankerten Rechte der Bürger gewährleisten. Denn es würde dem Zweck der Anstrengungen des Staates zur Eindämmung des Terrorismus, mit denen ja auch das Vertrauen der Bürger in seine Fähigkeiten zur Aufrechterhaltung der öffentlichen Sicherheit wiederhergestellt werden soll, zuwiderlaufen, wenn an die Stelle der Bedrohung durch den Terrorismus paradoxerweise eine als Bedrohung wahrgenommene uneingeschränkte Exekutivgewalt treten würde, die mithilfe unkontrollierter und zugleich weitreichender Überwachungstechniken und -befugnisse in die Privatsphäre der Bürger eindringt. Diese Bedrohung der Privatsphäre muss sowohl auf innerstaatlicher Ebene als auch nach der EMRK einer sehr genauen Kontrolle unterworfen werden. Auf diese Frage musste im vorliegenden Fall jedoch nicht eingegangen werden.[25]

Der EuGH hat in der Rechtssache Digital Rights Ireland darauf hingewiesen, dass ein Rechtsakt, der sich „auf alle Personen und alle elektronischen Kommunikationsmittel … erstreckt“, eine „Differenzierung, Einschränkung oder Ausnahme“[26] enthalten sollte. Zudem ist es nach Auffassung des EuGH notwendig, dass der Gesetzgeber ein „objektives Kriterium vorsieht, das es ermöglicht, den Zugang … zu den Daten und deren spätere Nutzung … zu beschränken“[27].

Gleichzeitig hat die Große Kammer des EGMR in der Rechtssache Zakharov entschieden, dass das Bestehen eines begründeten Verdachts gegen die betreffende Person[28], die eindeutig durch Namen, Anschriften, Telefonnummern oder sonstige relevante Informationen[29] zu identifizieren ist, überprüfbar sein muss, was darauf schließen lässt, dass nur eine gezielte Datenerhebung zugelassen werden sollte.

---

[24] EuGH, Schrems, Rn. 93.

[25] EGMR, Szabó, Rn. 68 („In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens’ Convention rights. … Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens’ trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens’ private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives.“), 70 („This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. … However, it is not warranted to embark on this matter in the present case“.)

[26] EuGH, Digital Rights Ireland, Rn. 57.

[27] EuGH, Digital Rights Ireland, Rn. 60.

[28] EGMR, Zakharov, Rn. 260: „the existence of a reasonable suspicion against the person concerned“.

[29] EGMR, Zakharov, Rn. 264: „names, addresses, telephone numbers or other relevant information“.

Zur Rechtmäßigkeit der massiven, wahllosen Erhebung (d. h. der nicht zielgerichteten Sammelerhebung) personenbezogener Daten und ihrer späteren Verwendung, einschließlich der Frage, unter welchen Umständen eine solche Erhebung und Verwendung personenbezogener Daten zulässig wäre, scheinen sich die Gerichtshöfe noch nicht abschließend geäußert zu haben. Der EuGH dürfte sich mit dieser Frage – zumindest in gewissem Umfang – im Laufe des Jahres 2016 befassen, und zwar zum einen in den verbundenen Rechtssachen Tele2 Sverige AB/Post- och telestyrelsen und Secretary of State for the Home Department/Davis und andere[30] und zum anderen im Rahmen des Gutachtens zur Gültigkeit des PNR-Abkommens mit Kanada[31].

Zum Inhalt von Kommunikationsdaten bezieht der EuGH klarer Stellung. Im Schrems-Urteil hat er festgestellt, dass es den Behörden nicht erlaubt sein sollte, generell auf den Inhalt elektronischer Kommunikation zuzugreifen.[32] Denn eine Regelung, die den Behörden einen solchen Zugriff gestattet, verletzt nicht nur das Recht, sondern auch „den Wesensgehalt des … Grundrechts auf Achtung des Privatlebens“[33]. Der Gerichtshof definiert jedoch nicht, was er unter „generell“ versteht.

6. Garantie C – Es sollte ein unabhängiger Aufsichtsmechanismus bestehen.

Der EGMR vertritt seit den 1970er Jahren die Auffassung, dass jeder Eingriff in die Rechte auf Schutz der Privatsphäre und Datenschutz der wirksamen, unabhängigen und unparteiischen Aufsicht durch einen Richter oder eine andere unabhängige Stelle (z. B. eine Verwaltungsbehörde oder ein parlamentarisches Gremium) unterliegen muss.[34] Ungeachtet der Form der unabhängigen Aufsicht stellt das Bestehen von Aufsichtsbehörden „ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten“[35] dar. Die Artikel-29-Datenschutzgruppe erinnert daran, dass ein Eingriff sowohl zum Zeitpunkt der Datenerhebung als auch zu dem Zeitpunkt stattfindet, zu dem eine staatliche Behörde auf die Daten zugreift, um sie zu nachrichtendienstlichen Zwecken weiterzuverarbeiten.

Nach Auffassung des EGMR kann die unabhängige Aufsicht in verschiedenen Phasen eines Datenverarbeitungsvorgangs stattfinden: bei der ersten Anordnung der Überwachung, während ihrer Durchführung und/oder nach ihrem Abschluss.[36] Angesichts der Besonderheiten der Datenverarbeitung zu nachrichtendienstlichen Zwecken wird es als zulässig angesehen, dass die betroffene Person – zumindest zu Beginn und während der Überwachung – nicht über die Verarbeitung informiert wird. Der EGMR hat präzisiert, dass es Natur und Logik der geheimen Überwachung in den ersten beiden Phasen gebieten, nicht nur die Überwachung selbst, sondern auch die begleitende Überprüfung ohne Wissen der

[30] EuGH, verbundene Rechtssachen C-203/15 und C-698/15.
[31] EuGH, Gutachten 1/15.
[32] EuGH, Schrems, Rn. 94.
[33] EuGH, Schrems, Rn. 94.
[34] EGMR, Klass, Rn. 17, 51.
[35] EuGH, Kommission/Deutschland, Rn. 23.
[36] EGMR, Klass, Rn. 55 f. EGMR, Zakharov, Rn. 233.

betroffenen Person durchzuführen. In einem Bereich, in dem Missbrauch in Einzelfällen so leicht möglich ist und derart schädliche Folgen für die demokratische Gesellschaft insgesamt haben kann, ist es grundsätzlich wünschenswert, dass ein Richter mit der Aufsicht betraut wird, da die richterliche Aufsicht die beste Gewähr für Unabhängigkeit, Unparteilichkeit und ein ordnungsgemäßes Verfahren bietet.[37]

Wie der EuGH ausführt, sollte „der Zugang … zu den auf Vorrat gespeicherten Daten … [der] vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle [unterliegen], deren Entscheidung den Zugang zu den Daten und ihre Nutzung auf das zur Erreichung des verfolgten Ziels absolut Notwendige beschränken soll und im Anschluss an einen mit Gründen versehenen Antrag der genannten Behörden im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten ergeht.“[38]

Es ist darauf hinzuweisen, dass der EGMR seine Schlussfolgerungen offenbar in Rechtssachen zur Telefonüberwachung gezogen hat, in denen es schwierig gewesen wäre, zwischen der vorherigen Genehmigung der Datenerhebung und dem anschließenden Zugriff auf die Daten zu unterscheiden. Das EuGH-Zitat dagegen stammt aus dem Urteil in der Rechtssache Digital Rights Ireland zur Vorratsdatenspeicherung, bei der nach den betreffenden Rechtsvorschriften die nicht zielgerichtete Erhebung großer Datenmengen erfolgt.

Eine nachträgliche Aufsicht erfolgt hauptsächlich über die dem Bürger zur Verfügung stehenden Rechtsbehelfe. Diese werden im Abschnitt über Garantie D behandelt. Es sei darauf hingewiesen, dass in einigen Fällen eine nachträgliche Kontrolle auch von Amts wegen vorgenommen werden könnte, um zu prüfen, ob die Überwachungsmaßnahmen mit den anwendbaren Rechtsvorschriften im Einklang stehen. Soweit der Artikel-29-Datenschutzgruppe bekannt ist, haben die Gerichtshöfe keine besonderen Kriterien für eine solche nachträgliche Aufsicht von Amts wegen festgelegt.

Mit Blick auf die Unabhängigkeit des Aufsichtsmechanismus für die Überwachung gibt der Straßburger Gerichtshof der Betrauung eines Richters mit der Verantwortung für die Aufsicht den Vorzug. Es ist jedoch nicht ausgeschlossen, dass die Verantwortung einer anderen Stelle übertragen wird, sofern diese über hinreichende Unabhängigkeit von der Exekutive verfügt[39] und auch „von den Behörden, welche die Überwachung durchführen, unabhängig und mit ausreichenden Machtbefugnissen und Kompetenzen ausgestattet [ist], um eine wirksame und ständige Kontrolle ausüben zu können“[40]. Der EGMR fügt hinzu, dass bei der Prüfung der

[37] EGMR, Zakharov, Rn. 233: „As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual’s knowledge. … In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure“.
[38] EuGH, Digital Rights Ireland, Rn. 62. Mit seiner Entscheidung, die Richtlinie über die Vorratsdatenspeicherung, die diese Anforderungen nicht erfüllte, für ungültig zu erklären, hat der Gerichtshof dies klargestellt.
[39] EGMR, Zakharov, Rn. 258: „provided that that authority is sufficiently independent from the executive“.
[40] EGMR, Klass, Rn. 56.

Unabhängigkeit auch die Modalitäten der Ernennung und die Rechtsstellung der Mitglieder des Aufsichtsgremiums[41] zu berücksichtigen sind. Dies schließt Personen mit Befähigung zum Richteramt ein, die entweder vom Parlament oder vom Regierungschef ernannt werden. Dagegen wurde ein Innenminister – der nicht nur ein politisches Amt innehatte und der Exekutive angehörte, sondern auch direkt an der Beschaffung besonderer Überwachungsmittel beteiligt war – für nicht hinreichend unabhängig befunden.[42] Wie der EGMR ferner anmerkt, ist es unerlässlich, dass die Aufsichtsstelle Zugang zu sämtlichen relevanten Schriftstücken hat, unter anderem auch zu Verschlusssachen.[43] Und schließlich berücksichtigt der EGMR, ob die Tätigkeit der Aufsichtsstelle der öffentlichen Kontrolle unterliegt.[44]

Insbesondere mit Blick auf die Datenschutzbehörden hat der EuGH in drei Rechtssachen dargelegt, was nach seiner Auffassung Unabhängigkeit im Sinne der Richtlinie bedeutet. Da einige Datenschutzbehörden auch für die Aufsicht über die Datenverarbeitung zu nachrichtendienstlichen Zwecken zuständig sind, könnte der vom EuGH festgelegte Standard in diesen besonderen Fällen von Bedeutung sein. Dies bedeutet vor allem, dass die Behörde ihre Aufgaben frei von äußeren Einflüssen wahrnehmen sollte. „Unabhängigkeit schließt u. a. jede Anordnung und jede sonstige wie auch immer geartete äußere Einflussnahme aus, sei sie unmittelbar oder mittelbar, an denen ihre Entscheidungen ausgerichtet werden könnten“[45]. Der EuGH erinnert auch daran, dass „funktionelle Unabhängigkeit … für sich allein nicht aus[reicht], um diese Kontrollstelle vor jeder äußeren Einflussnahme zu bewahren.“[46]

7. Garantie D – Dem Bürger müssen wirksame Rechtsbehelfe zur Verfügung stehen.

Die letzte der vier wesentlichen europäischen Garantien betrifft den Rechtsschutz für den Bürger. Ihm muss ein wirksamer Rechtsbehelf zur Wahrung seiner Rechte zur Verfügung stehen, wenn er den Eindruck hat, diese würden nicht geachtet. Im Schrems-Urteil hat der EuGH erläutert, dass „eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz [verletzt]. Nach Art. 47 Abs. 1 der Charta hat nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, nach Maßgabe der in

[41] EGMR, Zakharov, Rn. 278: „the manner of appointment and the legal status of the members of the supervisory body“.
[42] EGMR, Zakharov, Rn. 278: „persons qualified to hold judicial office, appointed either by parliament or by the Prime Minister … In contrast, a Minister of Internal Affairs – who not only was a political appointee and a member of the executive, but was directly involved in the commissioning of special means of surveillance – was found to be insufficiently independent“.
[43] EGMR, Zakharov, Rn. 281: „notes that it is essential that the supervisory body has access to all relevant documents, including closed materials“.
[44] EGMR, Zakharov, Rn. 283: „whether the supervisory body’s activities are open to public scrutiny“.
[45] EuGH, Kommission/Ungarn, Rn. 51 sowie die dort angeführte Rechtsprechung.
[46] EuGH, Kommission/Österreich, Rn. 42.

diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen."[47]

Für den EGMR ist die Frage des wirksamen Rechtsbehelfs untrennbar damit verbunden, dass der Bürger von einer Überwachungsmaßnahme nach deren Beendigung benachrichtigt wird. Der betroffene Bürger hat grundsätzlich kaum Möglichkeiten, den Rechtsweg zu beschreiten, es sei denn, er wird von den ohne sein Wissen durchgeführten Maßnahmen in Kenntnis gesetzt und kann so deren Rechtmäßigkeit im Nachhinein anfechten, oder er kann sich, wenn er den Verdacht hat, dass seine Kommunikation überwacht wurde oder wird, die Gerichte anrufen, sodass die Zuständigkeit der Gerichte nicht von der Benachrichtigung der überwachten Person von der Überwachung ihrer Kommunikation abhängt.[48]

Für den Fall, dass keine Benachrichtigung erfolgt, hat der EGMR in der Rechtssache Kennedy klargestellt, dass ein Gericht seiner Auffassung nach hinreichende Rechtsschutzmöglichkeiten bietet, sofern es eine Reihe von Kriterien erfüllt: Es muss sich um eine unabhängige und unparteiische Stelle handeln, die sich eine Verfahrensordnung gegeben hat und aus Mitgliedern besteht, die ein hohes Richteramt bekleiden oder bekleidet haben oder erfahrene Juristen sein müssen. Bei der Prüfung von Beschwerden Einzelner sollte das Gericht Zugang zu allen relevanten Informationen haben[49], unter anderem auch zu Verschlusssachen. Und schließlich sollte es befugt sein, bei Rechtsverletzungen Abhilfe zu schaffen.[50]

Es stellt sich die Frage, ob ein wirksamer Rechtsbehelf nur bei einem ordentlichen Gericht eingelegt werden kann oder auch bei einer anderen Stelle, die über hinreichende Unabhängigkeit und ausreichende Befugnisse verfügt, um bei Rechtsverletzungen Abhilfe zu schaffen. In der deutschen Sprachfassung der Charta wird in Artikel 47 zwar der Begriff „Gericht" verwendet.[51] Gleichzeitig verpflichtet die EMRK die Mitgliedsstaaten jedoch lediglich zu gewährleisten, dass „[j]ede Person, die in ihren … Rechten oder Freiheiten verletzt worden ist, … das Recht [hat], bei einer innerstaatlichen Instanz eine wirksame Beschwerde zu erheben"[52]. Dies muss nicht unbedingt eine Justizbehörde sein, wie der

[47] EuGH, Schrems, Rn. 95.
[48] EGMR, Zakharov, Rn. 234: „There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively … or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications".
[49] Die Artikel-29-Datenschutzgruppe weist darauf hin, dass nach Auffassung des Menschenrechtskommissars des Europarats die sogenannte Drittenregel – nach der Nachrichtendienste eines Landes, die Nachrichtendiensten eines anderen Landes Daten übermitteln, der Empfängerseite die Verpflichtung auferlegen können, die übermittelten Daten Dritten gegenüber nicht offenzulegen – nicht für Aufsichtsstellen gelten sollte, um die Möglichkeit eines wirksamen Rechtsbehelfs nicht zu beeinträchtigen (Themenpapier „Democratic and effective oversight of national security services").
[50] EGMR, Kennedy, Rn. 167.
[51] Auch in der niederländischen Fassung heißt es „gerecht", in der englischen dagegen „tribunal" und nicht „court".
[52] Artikel 13 EMRK.

EGMR in der Rechtssache Klass klargestellt hat.[53] Der Straßburger Gerichtshof stellt jedoch hohe Anforderungen an die Stelle, bei der der wirksame Rechtsbehelf einzulegen ist, wie er in der Rechtssache Kennedy präzisiert hat.

8. Abschließende Bemerkungen

Die in dieser Stellungnahme beschriebenen vier wesentlichen europäischen Garantien sind keine unbedingten Garantien. In Anbetracht ihrer Formulierung bedürfen sie in gewissem Umfang auch der Auslegung.

Sollte ein Drittland Eingriffe zulassen, die über das hinausgehen, was als in einer demokratischen Gesellschaft unbedingt erforderlich anzusehen ist, so kann sich der Bürger an seine Datenschutzbehörde wenden, um Hilfe bei der Aufklärung und dem Schutz seiner Grundrechte zu erhalten. Die Artikel-29-Datenschutzgruppe weist darauf hin, dass die Datenschutzbehörden eine Prüfung vornehmen werden, um einen Einzelfall zu untersuchen oder um massive, strukturelle oder wiederholte Datenübermittlungen auf der Grundlage eines der dafür vorgesehenen Instrumente zu genehmigen (oder zu evaluieren). Je nach dem Ergebnis der Prüfung könnte als Durchsetzungsmaßnahme unter anderem in Betracht kommen, die Datenübermittlungen im Einzelfall zu verbieten oder auszusetzen.

Die Artikel-29-Datenschutzgruppe weist darauf hin, dass die Auslegung der wesentlichen europäischen Garantie B (Notwendigkeit des Nachweises von Erforderlichkeit und Angemessenheit) im Laufe des Jahres 2016 möglicherweise angepasst werden muss, wenn der EuGH seine Entscheidungen in den Rechtssachen PNR-Abkommen mit Kanada sowie Tele2 Sverige und Davis verkündet hat. Bis dahin erinnert die Artikel-29-Datenschutzgruppe daran, dass nach der von ihr konsequent vertretenen Auffassung eine massive, wahllose Erhebung (d. h. eine nicht zielgerichtete Sammelerhebung) von Daten auf jeden Fall nicht als angemessen angesehen werden kann[54].

Die wesentlichen europäischen Garantien sollten nicht unabhängig voneinander geprüft werden, sondern in ihrer Gesamtheit und unter Berücksichtigung der einschlägigen Rechtsvorschriften zur Datenerhebung zu Überwachungszwecken, zum Mindestmaß an Garantien für den Schutz der Rechte der betroffenen Personen sowie zu den nach dem nationalen Recht des Drittlands zur Verfügung stehenden Rechtsbehelfen. Wie der EGMR in der Rechtssache Kennedy festgestellt hat, hängt die Prüfung von allen Umständen des Falles ab, darunter Art, Umfang und Dauer möglicher Maßnahmen, die für ihre Anordnung erforderlichen Gründe, die für ihre Genehmigung, Durchführung und Aufsicht zuständigen Behörden sowie die Art der im nationalen Recht vorgesehenen Rechtsbehelfe.[55]

---

[53] EGMR, Klass, Rn. 67.

[54] WP 215, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_de.pdf

[55] EGMR, Kennedy, Rn. 153: „The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law“.

Die Artikel-29-Datenschutzgruppe weist darauf hin, dass die Garantien auf den Grundrechten beruhen, die für jeden unabhängig von seiner Staatsangehörigkeit gelten. Zudem ist darauf hinzuweisen, dass die Garantien auf dem rechtlich Gebotenen beruhen und nicht unbedingt auf der derzeitigen Praxis in den EU-Mitgliedsstaaten. Die Artikel-29-Datenschutzgruppe misst nicht mit zweierlei Maß und hat die Mitgliedsstaaten daher schon mehrmals aufgerufen sicherzustellen, dass ihre Überwachungsvorschriften mit der Rechtsprechung des EuGH und des EGMR im Einklang stehen.

Anhang 1 – Rechtsprechung

In dieser Stellungnahme wird auf die Rechtsprechung des Gerichtshofs der Europäischen Union und des Europäischen Gerichtshofs für Menschenrechte Bezug genommen. Der Ausarbeitung dieser Stellungnahme lagen die folgenden Rechtssachen zugrunde, darunter auch einschlägige Rechtssachen, auf die nicht ausdrücklich Bezug genommen wird:

- Amman gegen Schweiz
  Europäischer Gerichtshof für Menschenrechte, 16. Februar 2000
  Individualbeschwerde Nr. 27798/95

- Association for European Integration and Human Rights und Ekimdzhiev gegen Bulgarien
  Europäischer Gerichtshof für Menschenrechte, 28. Juni 2007
  Individualbeschwerde Nr. 62540/00

- Bucur und Toma gegen Rumänien
  Europäischer Gerichtshof für Menschenrechte, 8. Januar 2013
  Individualbeschwerde Nr. 40238/02

- Chalal gegen Vereinigtes Königreich
  Europäischer Gerichtshof für Menschenrechte, 15. November 1996
  Individualbeschwerde Nr. 22414/93

- Kommission/Österreich
  Gerichtshof der Europäischen Union, 16. Oktober 2012
  Rechtssache C-614/10

- Kommission/Deutschland
  Gerichtshof der Europäischen Union, 9. März 2010
  Rechtssache C-518/07

- Kommission/Ungarn
  Gerichtshof der Europäischen Union, 8. April 2014
  Rechtssache C-288/12

- Copland gegen Vereinigtes Königreich
  Europäischer Gerichtshof für Menschenrechte, 3. April 2007
  Individualbeschwerde Nr. 62617/00

- Digital Rights Ireland, Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl u. a./Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irland und The Attorney General
  Gerichtshof der Europäischen Union, 8. April 2012
  Verbundene Rechtssachen C-293/12 und C-594/12

- Gillan und Quinton gegen Vereinigtes Königreich
  Europäischer Gerichtshof für Menschenrechte, 12. Januar 2010
  Individualbeschwerde Nr. 4158/05

- Hokkanen gegen Finnland
  Europäischer Gerichtshof für Menschenrechte, 23. September 1994
  Individualbeschwerde Nr. 19823/92

- Huvig gegen Frankreich
  Europäischer Gerichtshof für Menschenrechte, 24. April 1990
  Individualbeschwerde Nr. 11105/84

- Klass u. a. gegen Deutschland
  Europäischer Gerichtshof für Menschenrechte, 6. September 1978
  Individualbeschwerde Nr. 5029/71

- Leander gegen Schweden
  Europäischer Gerichtshof für Menschenrechte, 26. März 1987
  Individualbeschwerde Nr. 9248/81

- Liberty u. a. gegen Vereinigtes Königreich
  Europäischer Gerichtshof für Menschenrechte, 1. Juli 2008
  Individualbeschwerde Nr. 58243/00

- López Ostra gegen Spanien
  Europäischer Gerichtshof für Menschenrechte, 9. Dezember 1994
  Individualbeschwerde Nr. 16798/90

- Malone gegen Vereinigtes Königreich
  Europäischer Gerichtshof für Menschenrechte, 2. August 1984
  Individualbeschwerde Nr. 8691/79

- Rotaru gegen Rumänien
  Europäischer Gerichtshof für Menschenrechte, 4. Mai 2000
  Individualbeschwerde Nr. 28341/95

- S. und Marper gegen Vereinigtes Königreich
  Europäischer Gerichtshof für Menschenrechte, 4. Dezember 2008
  Individualbeschwerden Nrn. 30562/04 und 30566/04

- Schrems/Data Protection Commissioner of Ireland
  Gerichtshof der Europäischen Union, 6. Oktober 2015
  Rechtssache C-362/14

- Szabó und Vissy gegen Ungarn
  Europäischer Gerichtshof für Menschenrechte, 12. Januar 2016
  Individualbeschwerde Nr. 37138/14

- Weber und Saravia gegen Deutschland
  Europäischer Gerichtshof für Menschenrechte, 29. Juni 2006
  Individualbeschwerde Nr. 54934/00

- Zakharov gegen Russland
  Europäischer Gerichtshof für Menschenrechte, 4. Dezember 2015
  Individualbeschwerde Nr. 47143/06

- ZZ/Secretary of State for the Home Department
  Gerichtshof der Europäischen Union, 4. Juni 2013
  Rechtssache C-300/11