führt wird, nicht verhindert, dass die Informationen auf der Webseite des Content-Providers veröffentlicht bleiben und daher weiterhin aufgerufen und von anderen Suchmaschinen indexiert werden können.

■ **Anerkennung eines „Rechts auf Vergessen":** Fraglich ist in diesem Fall, ob die Persönlichkeitsrechte das Recht auf Löschung derjenigen Daten beinhalten, die rechtmäßig und korrekt an der Quelle sind und durch die Suchmaschine indexiert werden (ARTEMI RALLO LOMBARTE, „El derecho al olvido y su protección", Revista TELOS, n° 85, 2010, pp. 1-5; CECILE DE TERWANGNE, „Privacidad en Internet y el derecho a ser olvidado", Revista de Internet, Derecho y Política, n° 13, 2012, pp. 53-66). Das Problem ist die Persistenz von Informationen im Netzwerk im Laufe der Zeit und ihre einfache Zugänglichkeit und Auffindbarkeit. Daher stellt sich die Frage, ob der Bürger verlangen kann, dass bestimmte persönliche Nachrichten und Informationen, die seine Identifizierung erlauben, von Suchmaschinen nicht indiziert werden dürfen. Dadurch würde die Entscheidung, welche persönlichen Informationen im Internet verbreitet werden dürfen, letztendlich beim Bürger selbst liegen. Problematisch könnte sein, dass dadurch die Zuverlässigkeit und Objektivität der Informationen abgeschwächt werden könnte und das „Recht auf Vergessen" als eine Art von Zensur wirken könnte.

3. Zeitliche Übereinstimmung mit den Vorschlägen für eine neue DS-GVO

Der am 25.1.2012 veröffentlichte Vorschlag für eine neue Datenschutz-Grundverordnung (DS-GVO, KOM(2012)10 endg. v. 25.1.2012) über die Verarbeitung personenbezogener Daten könnte die Vorlagefragen inhaltlich überholen. Auf der einen Seite besagt die neue Verordnung, dass EU-Rechtsvorschriften über den Schutz personenbezogener Daten nicht nur für Unternehmen gelten, die in der Europäischen Union ihren Sitz haben, sondern auch für diejenigen Unternehmen, die für europäische Bürger Waren oder Dienstleistungen anbieten und diesbezüglich eine Verarbeitung persönlicher Daten ausführen. Auf der anderen Seite erkennt die vorgeschlagene neue DS-GVO in Art. 17 ausdrücklich das „Recht auf Vergessen" an. Die Vorschrift bestimmt auch die Verpflichtung des Verarbeitenden, auf Antrag des Betroffenen alle Links auf seine persönlichen Informationen zu entfernen.

4. Fazit

Die Beantwortung der vielen aufgeworfenen Fragen ist keine triviale Angelegenheit. Die Entscheidung des *EuGH* wird eine Veränderung im Verhältnis des Bürgers zu Suchmaschinen wie *Google* nach sich ziehen.

Die Aussagen von EU-Justizkommissarin *Viviane Reding* basieren in diesem Fall auf dem Glauben, dass Service-Provider oder Suchmaschinen gewisse Mindestanforderungen beim Sammeln von Nutzerdaten erfüllen müssen, um eine größere Transparenz in ihrer Funktionsweise zu erreichen. Sie müssen den Anforderungen von Art. 8 der Charta der Grundrechte der Europäischen Union gerecht werden.

Es bleibt weiterhin spannend, ob der *EuGH* sich nur zur Frage äußert, ob ein Bürger die Löschung seiner Daten im Internet verlangen kann. Ferner sollte geklärt werden, wer diese Informationen zu löschen oder den Link zu entfernen hat: die Suchmaschinenbetreiber oder der für die Quelle der Informationen Verantwortliche. Vielleicht wird letztendlich alles von der neuen DS-GVO abhängen, in der Hoffnung, dass sie für die hier aufgeworfenen Fragen eine endgültige und langfristige Lösung bietet.

■ Vgl. hierzu auch *Reding*, ZD 2012, 195 – in diesem Heft.

Prof. Monica Arenas Ramiro
ist Professorin an der Juristischen Fakultät der Universität von Alcalá, Spanien.

RAin Silviya Yankova
ist wissenschaftliche Mitarbeiterin am Institut für Informations-, Telekommunikations- und Medienrecht – zivilrechtl. Abt. (Prof. Hoeren) – an der Wilhelms-Universität Münster.

Axel Spies USA: Neue Datenschutzrichtlinien zur Bekämpfung des Terrorismus

ZD-Aktuell 2012, 02793

Am 23.3.2012 veröffentlichten die „Behörde für nationale Nachrichtendienste" (*Office of the Director of National Intelligence – ODNI*) und das Justizministerium der USA (*US Department of Justice*) die neu überarbeiteten Richtlinien, die der Bekämpfung des Terrorismus dienen sollen.

Nach diesen Richtlinien wird der „Nationalen Terrorismusbekämpfungsbehörde" (*National Counterterrorism Center – NCTC*) die Befugnis eingeräumt, Daten, die in einer Verbindung mit terroristischen Handlungen stehen, bis zu fünf Jahre zu speichern. Allerdings beziehen sich die neuen Richtlinien nur auf solche Daten, die bereits von anderen Behörden der *US-Regierung* zuvor gesammelt wurden und in deren Datenbank gespeichert sind. Sofern diese Daten Informationen über Terrorismusaktionen enthalten und der Zugriff auf diese Daten einen bestimmten Zweck verfolgt, wird dem *NCTC* der Zugang, die Speicherung, die Benutzung und die Übermittlung dieser Daten eingeräumt.

Bei der *NCTC* handelt es sich um eine Behörde, die nach den Anschlägen des 11. September 2001 gegründet wurde und die als zentrale Regierungsbehörde zur nachrichtendienstlichen Analyse und Terrorismusbekämpfung fungiert. Als Institution untersteht das *NCTC* dem *ODNI* und koordiniert die nachrichtendienstlichen Aktivitäten diverser US-Behörden bei der Bekämpfung des Terrorismus, wie z.B. der *Central Intelligence Agency* (*CIA*), dem *Department of Justice/Federal Bureau of Investigation* (*FBI*), den *Departments of State, Defense, Homeland Security* sowie in beratender Funktion den *Departments of Energy, Treasury, Agriculture, Transportation, Health and Human Services*, der *Nuclear Regulatory Commission* und der *US-Capitol Police*. Dem *NCTC* gehören mehr als 500 Mitarbeiter von 16 Ministerien und Agenturen an, wobei jedoch lediglich 60% von diesen allein dem *NCTC* zugeteilt sind. Das *NCTC* ist auch eine wichtige Anlaufstelle für ausländische Regierungsstellen bei der Terrorismusbekämpfung.

Nach den neuen Richtlinien beträgt die Höchstzeit dieser Art von Vorratsdatenspeicherung durch das *NCTC* fünf Jahre, wobei jedoch die Zeit vom Datentyp, der Sensibilität der Daten, bestehenden gesetzlichen Bestimmungen und weiteren

Umständen abhängt. Jedoch dürfen diese Richtlinien nicht mit der vielfach diskutierten Vorratsdatenspeicherung in Deutschland verwechselt werden. In den USA handelt es sich bei diesen Richtlinien nämlich lediglich um Daten, die bereits durch Behörden der *Regierung* unter bestehendem Datenschutzrecht gesammelt wurden und in deren Datenbanken gespeichert sind. Die Daten werden auch nicht von TK-Anbietern oder Internetdienstleistern gespeichert.

Der Zugriff des *NCTC* beschränkt sich dabei auf solche Daten, die über Terrorismusbestrebungen informieren oder die speziell inländischen Terrorismus betreffen. Doch auch Informationen, die keine Verbindung zu einer Terrorgruppe oder -aktion enthalten, können unter bestimmten Bedingungen gespeichert werden. Als Begründung dafür gibt *Robert Kitt*, Leiter der Rechtsabteilung der ODNI an, dass Informationen oft zunächst als unwichtig erscheinen und erst später für die Ermittlung relevant werden.

Kritiker dieser Richtlinien, wie der Direktor des Electronic Privacy Information Center (EPIC), *Marc Rotenberg*, befürchten allerdings eine zu starke Erweiterung der Kontrollbefugnisse der *US-Regierung* und eine Einschränkung des Federal Privacy Act. Laut *Alexander Joel*, der bei der *ODNI* für die Einhaltung der Freiheitsrechte zuständig ist, stehen der Speicherung von Daten durch das *NCTC* hohe Anforderungen entgegen, die sicherstellen, dass die Daten einen mit hoher Wahrscheinlichkeit terroristischen Inhalt enthalten und nur potenziell bedeutsame Informationen gesammelt werden.

Diese neuen Richtlinien basieren auf älteren Richtlinien vom November 2008. Nach den alten Richtlinien musste das *NCTC* jedoch erhobene Daten innerhalb von 180 Tagen löschen, die bereits in Datenbanken anderer Regierungsbehörden gesammelt waren, sofern keine Verbindung mit Terrornetzwerken hergestellt werden konnte. Allerdings reichten der *Regierung* laut einigen Kongressabgeordneten diese Speicherbefugnisse nicht aus, was sich insbesondere bei den Ermittlungsarbeiten der *NCTC* nach dem Amoklauf in Fort Hood und dem Flugzeugattentat in Detroit im Jahr 2009 herausgestellt habe. Nach dem Attentat in Detroit habe sich herausgestellt, dass US-Behörden Gespräche der *Al-Qaida* auf der Arabischen Halbinsel abgehört hatten und dass zugleich ein korrespondierender Bericht eines US-Konsulats aus Nigeria vorlag. Mittels beider Informationen und erweiterten Speicherfristen hätte das Attentat möglicherweise verhindert werden können, sofern diese Informationen zusammengefügt worden wären.

Nach Aussage von *James Clapper*, dem Direktor des ODNI, soll mit den neuen Richtlinien die Aufgabe der *NCTC* realisierbarer und effektiver werden. Durch den Zugriff auf die Informationen vieler US-Institutionen soll das *NCTC* in der Lage sein, Verknüpfungen zwischen den einzelnen Informationen finden und dadurch erfolgreicher ermitteln zu können.

Dr. Axel Spies
ist Rechtsanwalt bei Bingham McCutchen in Washington DC und Mitherausgeber der Zeitschrift ZD.

Tim Wybitul Aktuelle Gesetzesinitiativen zum Schutz von Hinweisgebern

ZD-Aktuell 2012, 02794

Hinweisgeber sind ausgesprochen wichtig für eine funktionierende Compliance-Kultur in Unternehmen. Die strukturierte Entgegennahme von Hinweisen über mögliche Fehlentwicklungen und deren angemessene Auswertung sind wesentliche Elemente eines funktionierenden internen Kontrollsystems. Die Praxis zeigt, dass Hinweisgeber eine Vielzahl von Schäden und Gefährdungen aufdecken. Es ist daher ausgesprochen wichtig, Personen zu schützen, die auf bestehende Missstände oder Verletzungen von Vorschriften und unternehmensinternen Verhaltensregeln hinweisen. Der vorliegende Überblick beruht auf einer Stellungnahme, die der Verfasser als Einzelsachverständiger vor dem *Deutschen Bundestag* abgegeben hat. Er zeigt einige für die Praxis maßgebliche Probleme der derzeit diskutierten Regelungen bzw. des Antrags der *LINKEN*-Fraktion, BT-Drs. 17/6492 (nachstehend: Antrag) und des Gesetzentwurfs der *SPD*-Fraktion, BT-Drs. 17/8567, (nachstehend: Entwurf) auf und gibt Empfehlungen für sachgerechte Lösungen. Der Schwerpunkt der Betrachtung liegt dabei auf den für Unternehmen besonders kritischen Fragen des Datenschutzes.

I. Bedeutung von Hinweisgebersystemen in der Unternehmenspraxis

Vor allem in großen und mittelgroßen Unternehmen sind Hinweisgebersysteme ausgesprochen wichtig, um interne Fehlentwicklungen und insbesondere Gesetzesverstöße aufzudecken und zu vermeiden (vgl. zum Rechtsrahmen beim Betrieb von Hinweisgebersystemen *Wybitul*, ZD 2011, 118 ff.). Gerade in größeren Unternehmensstrukturen sind interne Abläufe und der Geschäftsbetrieb in der Regel so komplex, dass Wirtschaftsdelikte und andere Regelverstöße schwer zu bemerken und leicht zu verschleiern sind. In der betrieblichen Praxis sind es häufig Beschäftigte oder Geschäftspartner, deren Hinweise diese Missstände oder gar Straftaten aufdecken. Dies führt dazu, dass vor allem große und international tätige Unternehmen zunehmend Hinweisgebersysteme einrichten.

Ein wichtiger Punkt ist beim Umgang mit Hinweisen auf Fehlentwicklungen oder Fehlverhalten besonders zu beachten: Beim Whistleblowing geht es in der Sache nicht um Denunziation oder gar ein „Verpfeifen", sondern um das grundrechtlich geschützte Informieren über Regelverstöße (*EGMR*, U. v. 21.7.2011 – 28274/08; vgl. zu der Entscheidung auch *Wybitul*, ZD-Aktuell 2011, 9). Allerdings zeigen die gegen Hinweisgeber geäußerten Vorbehalte eine wichtige Voraussetzung von Hinweisgebersystemen auf – sie müssen so ausgestaltet sein, dass sie nicht missbraucht werden. Außerdem müssen gutgläubige Hinweisgeber vor Nachteilen geschützt werden (*BVerfG*, B. v. 2.7.2001 – 1 BvR 2049/00, Rdnr. 10). Denn andernfalls würden gutgläubige Hinweisgeber in ihren Grundrechten aus Art. 2 Abs. 1 GG i.V.m. dem Rechtsstaatsprinzip verletzt (*BVerfG*, a.a.O., Rdnr. 20). Generell ist die aktuelle Entwicklung in Deutschland hin zu Hinweisgebersystemen uneingeschränkt zu begrüßen.

II. Verhältnis von unternehmensinternen Hinweisgebersystemen und Meldungen gegenüber Behörden

Unternehmen sollten Strukturen schaffen, die es Hinweisgebern erlauben, ge-