

Stellungnahme des ECCHR vor dem belgischen Verfassungsgericht - Zusammenfassung -

Das European Center for Constitutional and Human Rights (ECCHR) reichte letzte Woche eine Stellungnahme als Nebenintervenient im Fall des belgischen Verfassungsgerichts gegen das Übereinkommen zwischen der EU und der USA zur Registrierung von Namen von Fluggästen (Passenger Name Record/ PNR) und dem Massenüberwachungssystem ein.

Hintergrund

Im Juli 2007 unterzeichnete die EU ein Abkommen mit dem US Department of Homeland Security, um den USA für die Bekämpfung von Terrorismus und schweren transnationalen Verbrechen den Zugriff auf Europäische PNR-Daten zu erleichtern. Das Übereinkommen, das von Institutionen wie dem Europäische Parlament, dem Europäischen Datenschutzbeauftragten, der Agentur der Europäischen Union für Grundrechte, sowie Bürgerrechts-, Datenschutz- und Anti-Rassismus-Aktivisten stark kritisiert wurde, erlaubt den US-Strafverfolgungsbehörden europäische personenbezogene Daten zu sammeln und für wenigstens 15 Jahre zu speichern. Damit setzt es alle Passagiere ausgedehnter Überwachung aus, unabhängig davon, ob sie eines Verbrechens beschuldigt werden. Das Übereinkommen macht es US-Behörden möglich, eine so genanntes *data profiling* vorzunehmen, also unschuldige Passagiere mit „verdächtigen“ Passagieren auf Basis harmloser Faktoren wie Reiseverhalten oder Kreditkartengebrauch und (möglicherweise) religiöser und ethnischer Hintergründe in Verbindung zu bringen.

Am 1. März 2010 reichte die belgische Sektion der Ligue des Droits de L’Homme (Liga der Menschenrechte) beim belgischen Verfassungsgericht Klage gegen das nationale Gesetz vom 30 November 2009, das das PNR-Übereinkommen zwischen EU und USA ins belgische Recht überträgt, ein. Am 21. Mai 2010 reichte das ECCHR eine Stellungnahme zur Unterstützung der belgischen Klage ein mit dem Ersuchen dem Verfahren als weitere Partei beitreten zu können.

Rechtliches Vorbringen

Das ECCHR erörtert in seiner Stellungnahme, dass das PNR-Übereinkommen gegen drei Kerngrundrechte verstößt: das *Recht auf Achtung des Privatlebens* (nach Artikel 8 der Europäischen Menschenrechtskonvention und Artikel 7 der Grundrechtscharta der Europäischen Union), das *Recht auf Datenschutz* gemäß Artikel 8 der Grundrechtscharta in Verbindung mit der Datenschutzrichtlinie 95/46/EC und das *Recht auf Nichtdiskriminierung* (nach Artikel 21 der Grundrechtscharta und Artikel 14 der Europäischen Menschenrechtskonvention).

Die Hauptargumente des ECCHR sind folgende:

- Im Übereinkommen fehlen angemessene Mechanismen, mit denen Bürger ihre Rechte im Falle der Verletzung durchsetzen können, ein Verstoß gegen den *Vorbehalt des Gesetzes*, den Artikel 8 der Menschenrechtskonvention erfordert.

- Das Übereinkommen verstößt gegen Grundrechte, indem es den nach Artikel 8 erforderlichen Grad an *rechtlicher Bestimmtheit* nicht aufbringt. Es fehlt an Bestimmtheit hinsichtlich der Ermessensausübung von staatlichen Behörden zum Zugang zu „sensiblen Daten“, die Informationen über Rasse, Religion, politische oder sexuelle Einstellung des Einzelnen preisgeben. Darüber hinaus ist es, da das Übereinkommen nicht aufzeigt, wie genau das *data profiling* eigentlich funktioniert, für den Einzelnen unmöglich zu wissen, welcher Gebrauch von seinen persönlichen Daten gemacht wird.
- Das Übereinkommen beeinträchtigt *unverhältnismäßig* die Rechte des Einzelnen aus Artikel 8. Es ist nicht offensichtlich, dass die Massenüberwachung, die durch das Übereinkommen erleichtert wird, eine effektive (und damit erforderliche) Maßnahme zur Bekämpfung des Terrorismus ist. Es sind weniger einschneidende Maßnahmen denkbar – beispielsweise haben die ähnlichen EU-PNR-Abkommen mit Australien und Kanada vergleichbare Ziele, erlauben aber die Speicherung von Passagierdaten nur für signifikant kürzere Zeit. Außerdem mangelt es dem derzeitigen Übereinkommen an angemessenen prozessualen Schutzmaßnahmen und Möglichkeiten zur Entschädigung. Der Schutz, der durch den US Privacy Act von 1974 gewährleistet wird, erreicht jedenfalls in der Praxis nicht den Umfang, den die Europäer sich zur Durchsetzung ihrer Individualrechte gegenüber den US-Behörden wünschen.
- Das PNR-Überwachungssystem wird bereits von den US-Behörden zu Zwecken genutzt, die *über den Anwendungsbereich des Übereinkommens hinausgehen* und damit gegen Artikel 6(1)(b) der Datenschutzrichtlinie verstoßen. Kürzliche Überprüfungen des Systems durch die EU zum Beispiel ergaben, dass persönliche PNR-Daten von den US-Behörden zu Zwecken der Immigrations- und der Grenzschutzkontrolle missbraucht werden, anstatt zur Bekämpfung von Terrorismus und transnationalen Verbrechen.
- Das Übereinkommen erlaubt den US-Behörden persönliche Daten für eine übermäßige - möglicherweise unbegrenzte - Zeit zu speichern. Nach vorigen PNR-Übereinkommen konnten Daten für 3,5 Jahre gesichert werden. Nach dem jetzigen Übereinkommen werden die Daten in allen Fällen für mindestens 15 Jahre gespeichert. Darüber hinaus haben die USA weder eine verbindliche Zusage getroffen die Daten wirklich nach 15 Jahren zu vernichten, noch die Zerstörung bei anderen Behörden, die das US Department of Homeland Security an den PNR-Informationen teilhaben lässt, sicherzustellen. Dies ist eindeutig unvereinbar mit Artikel 6 der Datenschutzrichtlinie, der verlangt, dass für einen bestimmten Zweck *die persönlichen Daten nicht länger als erforderlich gespeichert* werden.
- Das derzeitige PNR-Übereinkommen erlaubt die umfassende Sammlung und Speicherung von Daten von unschuldigen Menschen durch die Strafverfolgungsbehörden. Diese Daten werden dann weiter verwendet für anschließende Analyse, Kreuzvergleiche, Abgleich mit unbekanntem Kriterien über eine möglicherweise unbestimmte Zeit, um „Risiko -“ oder „Verdächtigen-Profile“ zu erstellen. Diese *unterschiedslose* Art des Massenüberwachungssystems verstößt

gegen die Anforderungen an die Verhältnismäßigkeit nach Artikel 6(1)(c) der Datenschutzrichtlinie.

- Trotz des Gebrauchs von automatischer Filterung, erlaubt das Übereinkommen den US-Behörden noch Zugang zu sensiblen Daten (sowohl in „Ausnahmefällen“ als auch zum Beispiel durch Analyse von einfacher PNR-Information bezüglich diätischen/medizinischen Bedarfs und/oder Fluggastnamen). Diese Daten ermöglichen die Konstruktion von Datenprofilen, die auf nicht überprüften Verallgemeinerungen oder stereotypen Annahmen, dass Personen einer bestimmten Rasse, ethnischen Herkunft oder religiösen Hintergrunds besonders wahrscheinlich an terroristischen Angriffen beteiligt sind, basieren. Das Übereinkommen erleichtert den diskriminierenden Effekt von rassischem oder ethnischem Profiling ohne ausreichende Schutzmechanismen zu enthalten. Die Konsequenz könnte ein *Verstoß gegen Vorschriften zur Nichtdiskriminierung* gemäß Artikel 21 der Grundrechtscharta und Artikel 14 der Menschenrechtskonvention sein.

Ergebnis und weiteres Vorgehen

Das ECCHR erwartet momentan die Entscheidung des Gerichtshofs über unseren Antrag in dieser wichtigen Sache. Wir rechnen damit, detaillierter in dieser Sache Stellung nehmen zu können, bevor der Verhandlungstermin durch das Gericht für Ende 2010 anberaumt wird.