von **Dr. Sebastian Kraska**

Flash-Cookies: Zombies im Datenschutzrecht?

Diverse Blogs im Internet haben letzte Woche über den Start eines höchst interessanten Prozesses in den USA berichtet. Am 23. Juli 2010 wurden die Internetseiten MTV, ESPN, MySpace, Hulu, ABC, NBC und Scribd vor dem United States District Court (Central District of California) verklagt. Die Beklagten hatten – so lautet die Klageschrift – Flash Cookies gesetzt, welche die von den Nutzern gelöschten Cookies wiederherstellten. Daraufhin wurde das Verhalten der Nutzer auf den Webseiten getrackt. Dieser Artikel soll die technischen Hintergründe der Flash Cookies vor dem Hintergrund des deutschen Datenschutzrechts erläutern.

Diverse Online-Studien haben herausgefunden, dass insgesamt etwa 30% der Internetbenutzer nach etwa einem Monat ihre Cookies löschen. Das in der Marktanalyse sehr beliebte Webtracking verliert damit an Aussagegehalt. Da Webtracking Programme oftmals auf Cookies aufbauen, können diejenigen User, welche die Cookies löschen, nicht über einen längeren Zeitraum beobachtet werden. Eine technische Neuerung war aus Sicht der Online-Marketing-Provider damit nötig. Ein Feature für den Adobe Flash Player wurde entwickelt, der sog. Flash Cookie. Die Wissenschaftler der Universität Berkeley haben herausgefunden, dass mehr als 50 der dort untersuchten Top-Webseiten Flash Cookies verwenden.

Was sind Flash Cookies?

Flash Cookies werden auch Local Shared Objects (LSO), Super-Cookies oder teilweise einfach “Zombie-Cookies” genannt. Die Cookies werden via Flash Plug-in auf zentralen Ordnern des Computers gespeichert und sind nicht über das zentrale Browsermenü zu erreichen.

Was ist das Besondere an Flash Cookies?

Grundsätzlich hat ein Flash Cookie die gleichen Eigenschaften wie ein gewöhnlicher Cookie, hat aber weitergehende Vorteile für den Webseiten-Betreiber: Ein Flash Cookie kann insgesamt 100 kb Informationen speichern, während gewöhnliche Cookies nur bis zu 4 kb speichern können. Über diese erhöhte Komplexität können sie insgesamt stabiler gesetzt werden. Flash Cookies werden nicht in dem gleichen Ordner wie gewöhnliche Cookies abgelegt. Internetbenutzer, die noch nicht über die Existenz der Flash Cookies Bescheid wissen, werden diese dementsprechend kaum löschen, da sich diese nicht einfach über den Browser löschen lassen.

Vorteil der Flash Cookies für Webseiten-Betreiber

Flash Cookies können unter anderem so programmiert werden, dass Cookies, die vom Nutzer im Browser gelöscht wurden, beim nächsten Besuch der Webseite wieder aktiviert werden. Diese Praxis wird im Englischen als “re-spawning” (zu Deutsch „wieder erzeugen“) bezeichnet. Die Nutzerverfolgung kann anschließend aufgrund der wieder erzeugten Cookies weitergehen, obwohl der Nutzer diese zuvor ausdrücklich in seinem Browser gelöscht hat.

Cookies: personenbezogene Daten?

Ob Cookies personenbezogene Daten sind oder solche beinhalten, muss natürlich immer am Einzelfall bestimmt werden. Wenn diese, wie etwa beim Webtracking, eine Identifikationsnummer des Webseitenbesuchers beinhalten, sind diese nach wohl vorherrschender Meinung als personenbezogene Daten anzusehen. Flash Cookies, die gerade über einen längeren Zeitraum die Verfolgung der Nutzer bezwecken, können gerade auch über die längere Aufzeichnung des Verhaltens eines Users personenbezogene Daten im Sinne von § 3 Abs. 1 Bundesdatenschutzgesetz („BDSG“) schaffen. Damit sind Cookies in jedem Fall als „potentiell personenbezogene Daten“ zu begreifen und müssen damit unter dem Schutz der datenschutzrechtlichen Vorschriften behandelt werden.

Damit sind die datenschutzrechtlichen Regelungen anwendbar und müssen geprüft werden.

Was stellen sich für datenschutzrechtliche Probleme?

Grundsätzlich ist nach dem System des deutschen Datenschutzrechtes eine Erhebung oder Verarbeitung personenbezogener Daten gestattet, wenn entweder die Einwilligung des Betroffenen vorliegt oder eine Rechtsgrundlage das jeweilige Vorgehen gestattet.

Was fordert die datenschutzrechtliche Einwilligung hinsichtlich Cookies?

Eine Einwilligung im Datenschutzrecht fordert – neben weiteren formalen Voraussetzungen- grundsätzlich die Bereitstellung der nötigen Informationen. Der Träger der personenbezogenen Daten muss schließlich wissen, für was er seine Einwilligung erteilen soll. Vorausgesetzt eine klare Information wird angeboten und die Einwilligung wird auch unter den weiteren Voraussetzungen des § 4a BDSG rechtswirksam erteilt, so ist das Setzen von Flash Cookies grundsätzlich rechtlich wirksam möglich. Die Datenschutzerklärung des verwendenden Unternehmens muss damit angepasst werden. Die Einwilligungserklärung des Nutzers muss den Flash Cookie Gebrauch unbedingt beschreiben. Daneben muss auch eine Widerspruchsmöglichkeit hinsichtlich des Flash Cookies eingeräumt werden.

Rechtsgrundlage für das Setzen von Cookies?

Davon abgesehen kann eine Rechtsgrundlage für das Setzen von Cookies in § 15 Abs. 1 TMG gesehen werden, wenn diese zur Inanspruchnahme von Telemedien notwendig sind. Die sog. „Session Cookies“ können insoweit also durch das Gesetz gerechtfertigt werden. Nach dem Ende der Browser-Session müssen die Cookies jedoch automatisch gelöscht werden. Eine ledigliche Erleichterung des Betriebs einer Internetseite reicht zur Begründung des Erforderlichkeitskriteriums insoweit nicht aus.

Dauerhaft platzierte Cookies sind damit keinesfalls als „notwendig“ im Sinne von § 15 Abs. 1 TMG zu begreifen und insofern nicht unter die Rechtsgrundlage zu subsumieren. Für permanente Cookies muss daher grundsätzlich die Einwilligung des Nutzers eingeholt werden. Dies gilt dann gerade auch für Flash Cookies, da diese eben dauerhaft auf dem Computer gespeichert werden.

Was ändert sich mit der Richtlinie 2009/136/EG?

Zum 15. Mai des nächsten Jahres muss die Richtlinie 2009/136/EG (so genannte „Cookie-Richtlinie“) auch in das deutsche Recht umgesetzt sein. Nach Art. 5 Absatz 3 der Richtlinie 2002/58/EG (ePrivacy-Richtlinie), welche durch die Cookie-Richtlinie verändert wird, ist das Setzen von Cookies dann grundsätzlich nur noch mit Einwilligung des Betroffenen erlaubt.

Fazit

Mit dem Setzen von Flash Cookies können sich neben rechtlichen Konsequenzen aus dem Strafrecht auch datenschutzrechtliche Schwierigkeiten stellen. Nach dem deutschen Datenschutzrecht dürfen diese grundsätzlich nur nach einer Einwilligung des Nutzers gesetzt werden. Es ist insbesondere darauf zu achten, dass Webseitenbetreiber ihre Datenschutzerklärungen entsprechend anpassen und wirksame Widerspruchsmöglichkeiten schaffen.

Autor:
Dr. Sebastian Kraska
Rechtsanwalt