I. AUFSÄTZE

GEOLOKALISATION UND GLÜCKSSPIELRECHT

(TEIL 1)

VON PROF. DR. THOMAS HOEREN, MÜNSTER

Einleitung

Im Glücksspielrecht stellt sich immer die Frage, inwieweit es möglich ist, geographisch Nutzer und Geräte im Internet anhand von IP-Adressen innerhalb der BRD zu lokalisieren. Der Begriff Geolokalisation (Geo-Targeting, Geo-Location) beschreibt den technischen Vorgang der geographischen Lokalisation von Nutzern und Geräten im Internet. Es existieren verschiedene Verfahren zur Geolokalisation, die im Folgenden näher betrachtet werden. Dabei wird grundlegend von der Tatsache Gebrauch gemacht, dass jeder Rechner im Internet zu einem Zeitpunkt durch eine eindeutige Adresse, der sog. IP-Adresse, identifiziert wird (vgl. Kapitel 1.1). Anhand der IP-Adresse und dem Weg, den ein Datenpaket zurücklegt (vgl. Kapitel 1.3), um vom Sender zum Empfänger zu gelangen, lassen sich Rückschlüsse auf den geographischen Ursprung eines Nutzers oder Gerätes im Internet ziehen.

Geolokalisationsverfahren werden zur Zeit in verschiedenen Anwendungsbereichen eingesetzt. Durch Geolokalisation lässt sich z.B. zielgerichtetes Marketing betreiben, digitale Inhalte lassen sich gegen unberechtigten Zugriff schützen, Spam-Nachrichten können erkannt werden und Kreditkartenbetrug lässt sich verhindern.

Dabei stellt sich zum einen die Frage nach der Genauigkeit und Zuverlässigkeit der Verfahren. Zum anderen stellt sich die Frage inwiefern es Methoden gibt, die Verschleierungsversuche der Herkunft einer IP-Adresse erkennen und verhindern können.

Es wird gezeigt, dass eine solche Zuordnung technisch möglich ist. Des Weiteren werden konkrete Methoden aufgezeigt, die es ermöglichen, Verschleierungsversuche bezüglich der Herkunft einer IP-Adresse aufzudecken. Ferner wird eine Übersicht über zur Zeit existente Anbieter von Geolokalisationstechnologie gegeben. Abschließend wird auf die Bedeutung von Geolokalisationstechnologie in Bezug auf Online-Glücksspiel und Online-Wetten eingegangen.[1]

1. Grundlagen der Geolokalisation

Die Grundlage aller Geolokalisationsverfahren bildet die IP-Adresse. Die Vergabe von IP-Adressen erfolgt zentralisiert durch ein hierarchisch organisiertes Netzwerk von Institutionen (vgl. Kapitel 1.2). Anhand der fest vergebenen IP-Adressbereiche lassen sich erste Rückschlüsse auf die geographische Herkunft einer IP-Adresse ziehen. Darüber hinaus werden zusätzliche Methoden, wie z. B. das Routing/Tracing (vgl. Kapitel 1.3) oder die Auswertung von Antwortzeiten / Pings (vgl. Kapitel 1.4) zur Optimierung des Lokalisationsergebnisses angewandt.[2]

1.1 IP-Adressen

Die IP-Adresse (Internet-Protocol-Adresse) dient zur eindeutigen Adressierung von Rechnern im Internet. Sie ist eine Binärzahl, die aus 32 Bit (Version IPv4) bzw. aus 128 Bit (Version IPv6) besteht. Die zurzeit meistverwendete Version ist Version 4 (IPv4).

Der IPv4 Adressraum umfasst 2^{32}, also 4.294.967.296 verschiedene Adressen. Aufgrund des steigenden Bedarfs an IP-Adressen wurde mit der Version IPv6 der Adressraum auf 2^{128} Adressen erweitert. IPv6 befindet sich bereits in der Einführungsphase und wird schrittweise die Version IPv4 ablösen.

Eine IPv4 Adresse wird i.d.R. als eine 12-stellige Dezimalzahl der Form xxx.xxx.xxx.xxx dargestellt (dotted decimal notation). Das entspricht einem Adressbereich von 0.0.0.0 bis 255.255.255.255. Jede der durch Punkte getrennten Dezimalzahlen repräsentiert genau ein Byte (8 Bit) der IP-Adresse. Die Vergabe der IP-Adressbereiche an Regionen, Länder und Internet Service Anbieter ist global institutionalisiert (vgl. Kapitel 1.2). Darüber hinaus sind ca. 14% aller IP-Adressen reserviert für besondere Funktionen (Für eine Auflistung der reservierten Adressbereiche für besondere Funktionen siehe Anhang A).

Die IP-Adresse stellt die Grundlage für die Kommunikation zweier Rechner im Internet dar. Jedes im Internet verschickte Daten-Paket enthält in den Kopfdaten (Header) sowohl die IP-Adresse des Absenders als auch die des Empfängers. Dadurch kann jedem Paket jederzeit seine Ursprungsadresse und seine Bestimmungsadresse zugeordnet werden. Da im Internet die Kommunikation nur selten direkt, sondern in den meisten Fällen über zwischengeschaltete Server (Router) abläuft (vgl. Kapitel 1.3), sind Absender- und Empfängeradresse für eine erfolgreiche Kommunikation notwendig. Dadurch wird das problemlose Ermitteln der IP-Adresse des Absenders eines Daten-Pakets, also bspw. des Nutzers einer bestimmten Internetseite, möglich.

1 *Hoeren, T.*, Zoning und Geolocation - Technische Ansätze zu einer Reterritorialisierung des Internet, MMR 2007, 3.

2 *Bassett, E., John, J., Anderson, T., Krishnamurthy, A., Chawathe, Y., Wetherall, D.*: Towards IP Geolocation Using Delay and Topology Measurements, in: Proc. of the ACM SIGCOMM/IMC, Rio de Janeiro, Brasilien, 2006; *Gueye, B., Ziviani, A., Crovella, M., Fdida, S.*: Contrained-Based Geolocation of Internet Hosts, in: Proc. of the ACM SIGCOMM/IMC, Taormina, Italien, 2004.

1.2 Vergabe von IP-Adressbereichen

Geolokalisationsverfahren nutzen die Tatsache, dass die Vergabe von IP-Adressen hierarchisch organisiert ist. Jeder Rechner/Nutzer, der sich mit dem Internet verbindet, erhält zu Anfang der Verbindung eine eindeutige und für die Dauer der Verbindung unveränderbare IP-Adresse von einem sog. Internet-Service-Provider (ISP). ISP sind lokale Vergabestellen für IP-Adressen und werden auch Local-Internet-Registries (LIR) genannt. Beispiele für ISP in Deutschland sind T-Online, Arcor oder Versatel.

Jeder ISP besitzt einen vorher festgelegten Bereich von IP-Adressen, die er nach eigenem Ermessen an seine Kunden vergeben kann. Die Vergabe von IP-Adressen kann entweder statisch (Ein Kunde erhält genau eine IP-Adresse, die für alle seine Verbindungen gültig ist) oder dynamisch (Ein Kunde erhält bei jeder Verbindung eine IP-Adresse, die nur für die Dauer einer Sitzung gültig ist und anschließend wieder frei gegeben wird) erfolgen.

Die Vergabe des IP-Adressbereichs an den ISP erfolgt durch Regionale Vergabestellen (Regional-Internet-Registry (RIR)).

RIRs:
- AfriNIC (African Network Information Centre) - Africa Region[3]
- APNIC (Asia Pacific Network Information Centre) - Asia/Pacific Region[4]
- ARIN (American Registry for Internet Numbers) - North America Region[5]
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands[6]
- RIPE NCC (Réseaux IP Européens) - Europe, the Middle East, and Central Asia[7]

Das für Deutschland zuständige RIR ist RIPE NCC. Jeder ISP in Deutschland erhält den ihm zur Verfügung stehenden Adressbereich entweder direkt von RIPE NCC oder von einem dem ISP übergeordneten Local-Internet-Registry. Zu einer bestimmten IP-Adresse lässt sich der zugehörige ISP über eine whois-Abfrage ermitteln. Diese Abfrage kann entweder WWW-gestützt über ein Portal[8] oder über die Kommandozeile mit der Syntax „whois IP-Adresse" durchgeführt werden. Eine whois-Abfrage einer IP-Adresse liefert unter anderem Informationen über Name, Sitz, Land und Kontaktadresse des ISP, der diese IP-Adresse verwaltet.

Die Regionalen-Internet-Register beziehen wiederum ihre Adressbereiche von der non-profit Organisation ICANN[9] (Internet Corporation for Assigned Names and Numbers). Während früher die IANA[10] (Internet Assigned Numbers Authority) IP-Adressbereiche direkt an die Nutzer vergeben hat verteilt ICANN Adressbereiche nun an die RIRs. ICANN ist die höchste globale Autorität für die Vergabe von IP-Adressen.

1.3 Routing/Tracing

Um den geographischen Ursprungsort eines Datenpakets zu ermitteln, ist es von Nutzen, den Weg nachvollziehen zu können, den das Paket im Internet genommen hat. Anhand dieser Information lassen sich anschließend Rückschlüsse auf den Ursprungsort des Paketes ziehen. Das Routing im Zusammenhang mit dem Internet bezeichnet die Vermittlung von Datenpaketen zwischen einem Absender und einem Empfänger. Dabei wird ein Datenpaket in der Regel über eine Reihe von zwischengeschalteten Servern (Routern) vermittelt. Aufgrund des hohen Komplexitätsgrades wird im Internet vorwiegend dynamisches Routing verwendet. Das heißt: Die Route, die ein Paket dabei nimmt ist nicht festgelegt, sondern ergibt sich erst während der Übermittlung.

Ein Router nimmt ein Paket entgegen, ermittelt dessen Bestimmungsort und ermittelt anschließend anhand einer lokal gespeicherten und vorher berechneten Routingtabelle den kürzesten Weg, den das Paket nehmen kann, um zum Empfänger zu gelangen. Das Paket wird daraufhin zu dem nächsten Router weitergeleitet. Die Übertragung zwischen 2 Routern wird auch als Hop bezeichnet. Nach einer endlichen Anzahl Hops erreicht das Paket seinen Empfänger.

Das Tracing bezeichnet die Ermittlung des Weges, den ein Datenpaket genommen hat. Dieser Weg wird auch als Traceroute bezeichnet. Mit dem Tracing lässt sich die IP-Adresse jedes Servers / Routers ermitteln, über den ein Datenpaket vermittelt wurde. Voraussetzung dafür ist, dass ein Server nicht „versteckt" agiert. Unter UNIX lässt sich der Pfad eines Pakets mit dem Befehl „traceroute *domain.de*" ermitteln. Unter Windows lautet der Befehl „tracert *domain.de*".

1.4 Antwortzeiten / Pings

Die Zeit, die ein Datenpaket braucht, um über das Internet von einem Rechner zu einem anderen Rechner zu gelangen, nennt sich Latenz oder Antwortzeit. Um diese Antwortzeiten zu ermitteln existiert das Programm Ping.

Ping sendet ein ICMP-„Echo-Request"-Paket (ping) an die Zieladresse des zu überprüfenden Hosts. Der Empfänger muss, sofern er das Protokoll unterstützt, laut Protokollspezifikation eine Antwort zurücksenden: ICMP „Echo-Reply" (pong). Ist der Zielrechner nicht erreichbar, antwortet der zuständige Router: „Network unreachable" (Netzwerk nicht erreichbar) oder „Host unreachable"(Gegenstelle nicht erreichbar).

Aus einer fehlenden Antwort kann nicht geschlossen werden, dass die Gegenstelle nicht erreichbar wäre, da manche Hosts so konfiguriert sind, dass sie ICMP-Pakete ignorieren und

3 http://www.afrinic.net/
4 http://www.apnic.net/
5 http://www.arin.net/
6 http://lacnic.net/en/index.html
7 http://www.ripe.net/
8 http://www.db.ripe.net/whois
9 http://www.icann.org
10 http://www.iana.org/

verwerfen.[11]

Da die Antwortzeit oft mit der Entfernung korrespondiert, die zwischen zwei Rechnern liegt, lassen sich Antwortzeiten zur Geolokalisation von Internetnutzern heranziehen.

2. Technische Umsetzung der Geolokalisation

Die Methoden zur Geolokalisation lassen sich in drei grundlegende Kategorien unterteilen:

1. Die Auswertung von öffentlichen und zentral in Datenbanken gespeicherten Informationen über die Vergabe von IP-Adressen (vgl. Kapitel 2.1)

2. Die Auswertung von Informationen, die in einer Domain oder in der Bezeichnung eines Routers / Servers mitgeliefert werden (vgl. Kapitel 2.2.)

3. Auswertung von Routing / Tracing Informationen sowie von Antwortzeiten / Pings (vgl. Kapitel 2.3 und 2.4).

Für jede Kategorie existieren mehrere Methoden zur Umsetzung. Zur Zeit am Markt existierende Geolokalisationsanbieter kombinieren i.d.R. mehrere oder alle dieser Ansätze mit selbsterstellten und laufend aktualisierten Datenbanken, in denen Erfahrungswerte und Zusatzinformationen über die geographische Lage von IP-Adressen gehalten werden.

2.1 Auswertung von Adressdatenbanken durch whois-Abfragen

Zu jeder IP-Adresse lässt sich eine Abfrage auf einer öffentlichen whois-Datenbank durchführen. Durch eine solche Abfrage lässt sich der für diese IP-Adresse registrierte „Besitzer" (ISP, Unternehmen, Universität, etc.) bestimmen. Die whois-Abfrage liefert unter anderem Informationen über E-Mail-Adresse, Telefonnummer und Postanschrift des Besitzers. Anhand dieser Informationen lassen sich Rückschlüsse auf die geographische Herkunft einer IP-Adresse ziehen. Der Ländercode *country*: DE gibt an, dass die Adresse aus Deutschland stammt. Als Besitzer der IP-Adresse wird zB die „Universität Münster" angegeben. Mit diesen und weiteren Informationen, wie z.B. anhand der Postleitzahl lassen sich nun mithilfe spezieller Umwandlungs-Programme (z.B. GoogleMaps) Bundesländer sowie ungefähre Längen- und Breitengrade ermitteln. Durch eine whois-Abfrage lassen sich also erste Hinweise auf die Herkunft einer IP-Adresse ermitteln. Da der Standort des Endnutzers jedoch nicht immer zwangsläufig mit dem Standort der in der whois-Datenbank registrierten Organisation übereinstimmen muss, ist die Anwendung weiterer Methoden notwendig, um das Ergebnis zu validieren.

2.2 Auswertung von Domain- und Routerspezifischen Informationen

Falls der zu lokalisierenden IP-Adresse ein Domain-Name hinterlegt ist, lassen sich anhand dieses Domain-Namens zusätzliche Informationen über den Standort der IP-Adresse extrahieren. Von den 264 möglichen Top-Level-Domains (z.B. ".de", ".at", ".com") sind 245 *country code* Top-Level-Domains. Liegt beispielsweise die Domain *uni-muenster.de* vor, so lässt sich anhand der Top-Level-Domain (.de) schon einmal das Ursprungsland der Domain, nämlich Deutschland, feststellen.
Diese Methode lässt sich auch auf den „normalen" Internetnutzer anwenden, dessen IP i.d.R. keine Domain hinterlegt ist. Dabei lässt sich die Tatsache nutzen, dass viele ISP in den Domain-Namen ihrer Router geographische Codes verwenden. Zum Bespiel kann der Traffic eines Versatel-Nutzers über den Router *10g-7-4.ber023isp005.versatel.de* geleitet werden. Die Buchstabenfolge „ber" zeigt in diesem Fall an, dass der Router in Berlin steht.

Die Benennung der Router steht jedem ISP frei. Es ist also im Vorhinein abzuklären ob ein ISP Benennungskonventionen einhält und in welcher Form diese vorliegen. Diese Informationen können in Datenbanken gesammelt abgespeichert und anschließend automatisiert in Echtzeit abgefragt werden.

2.3 Auswertung von Routing/Tracing Informationen

Das Auswerten von Routing-Informationen eines Datenpaketes stellt eine weitere Möglichkeit dar, den geographischen Ursprung eines Internetnutzers herauszufinden. Mit traceroute lässt sich der Weg ermitteln, den ein Datenpaket genommen hat (vgl. Kapitel 1.3). Es wird angenommen, dass ein Router, der nur wenige Hops von dem Ziel entfernt ist auch geographisch in der Nähe des Ziels liegt. Anhand der nächstgelegen Router-Namen lassen sich, wie schon in Kapitel 2.2 beschrieben, Informationen über die geographische Herkunft ableiten.

Anhand dieser Informationen lässt sich wiederum mithilfe zugrundeliegender Datenbanken das Lokalisationsergebnis verbessern bzw. validieren.

2.4 Auswertung von Antwortzeiten

Entgegen der allgemeinen Ansicht ist es möglich, Standorte von Routern oder Internetnutzern anhand dessen Antwortzeit (vgl. Kapitel 1.4) bei einem Ping zu bestimmen. Da im Internet ein Paket nicht immer denselben Weg zurücklegt und ein Router eine Anfrage nicht immer gleich schnell bearbeitet, variieren die Antwortzeiten eines Routers. Es existiert jedoch ein absolutes Antwortzeit-Minimum, über das ein Router nicht hinauskommt. Um dieses Minimum näherungsweise zu ermitteln wird ein Router mehrmals (z.B. 10-15 Mal) gepingt. Der kleinste Wert wird dann zur Bestimmung Antwortzeit genutzt.

Es wird bei der Geolokalisation mit Antwortzeiten zwischen zwei grundlegenden Methoden unterschieden. Die erste Methode basiert auf der Beobachtung, dass Maschinen, die

11 Vgl. http://de.wikipedia.org/wiki/Ping_%28Daten%C3%BCbertragung%29 – Stand: 21.03.2008

ähnliche Antwortzeiten zu anderen festgelegten Maschinen besitzen, sich auch geographisch nahe sind.

Diese auch als GeoPing[12] bezeichnete Methode misst zuerst die Antwortzeiten zwischen einer Menge von Routern/Hosts, die als Prüfmaschinen agieren (im Beispiel P1-P3) und einer anderen Menge von Maschinen, die als fixe Landmarken agieren (L1-L5). Die geographische Position dieser Landmarken wird im Vorhinein ermittelt. Die minimalen Antwortzeiten zwischen jeweils einer Menge von Prüfmaschinen und einer Landmarke werden zu Vektoren zusammengefasst. Anschließend wird ein Vektor aus den Antwortzeiten des unbekannten Ziels und der Menge der Prüfmaschinen erstellt. Das Ziel wird nun derjenigen Landmarke zugeordnet, deren Antwortzeitenvektor dem Zielvektor am ähnlichsten ist. Dabei wird ein vorher festgelegtes Ähnlichkeitsmaß angelegt (z.B. Euklidische Distanz, City-Block-Distanz).

Die zweite Methode, auch Contrained-Based Geolocation[13] genannt, bestimmt den geographischen Ursprung eines Ziels durch systematisches Eingrenzen des Zielbereichs. Auch für diese Methode werden Landmarken-Hosts benötigt, deren geographische Position im Vorhinein bekannt ist. Anschließend werden Antwortzeiten in Entfernungen umgewandelt, indem die Antwortzeiten zwischen jeder Landmarke mit allen anderen gemessen werden. Das Ziel wird nun einem geographischen Bereich zugeordnet, der ihm anhand des Abstands zu den Landmarken am besten entspricht.

Die Genauigkeit dieser Verfahren hängt proportional von der Anzahl Landmarken ab. Je mehr Landmarken definiert sind, desto genauer ist das Lokalisationsergebnis. Landmarken-Hosts müssen dabei nicht zwangsläufig aktiv agieren können, was mit hohen Kosten verbunden ist. Es lassen sich vielmehr auch fremde Hosts als passive Landmarken nutzen. Auf diese Art sinken die Kosten und es wird möglich die Anzahl Landmarken auf ein ausreichend hohes Niveau zu heben.

Weitere Ansätze der Forschung sind die sog. Delay-Based Geolocation[14] und die Topology-Based Geolocation , welche eine Verfeinerung des Lokalisationsergebnisses auf Basis der o.g. Methoden darstellen.

Der Beitrag wird im nächsten Heft, ZfWG 05.08, fortgesetzt.

12 *Vgl. Padmanabhan, V., Subramanian, L.*: An investigation of geographic mapping techniques for Internet Hosts, In: Proc. Of the ACM SIGCOMM, San Diego, USA, 2001.

13 Vgl. *Gueye et. Al*, aaO , 2004.

14 Vgl. *Basset et al*, aaO, 2006.

ZUR NOTWENDIGKEIT DES VERBOTS VON INTERNETGLÜCKSSPIELEN

VON PROFESSOR DR. MICHAEL ADAMS UND DIPL. KFM. INGO FIEDLER, UNIVERSITÄT HAMBURG

I. Einleitung

Die Europäische Kommission hält das deutsche Verbot von Glücksspielen im Internet für europarechtswidrig.[1] Die Kommission räumt zwar ein, dass die deutsche Begründung für das Verbot – die Bekämpfung von Spielsucht und der Schutz Minderjähriger – zwingende Gründe des öffentlichen Interesses sind. Jedoch betrachtet sie das allgemeine Verbot von Lotterien und Sportwetten im Internet nicht als *geeignete Maßnahme*, um diese Ziele zu erreichen. Zudem werde dem Grundsatz der *Verhältnismäßigkeit* nicht Rechnung getragen, da weniger restriktive Maßnahmen zur Verfügung stünden.
Der Aufsatz zeigt, dass entgegen der Ansicht der Kommission das vollständige Verbot von Internetglücksspielen sowie die Unterbindung der ihr zugrunde liegenden Zahlungsströme und ihrer Werbung in Deutschland eine geeignete und verhältnismäßige Maßnahme darstellen.

II. Die besondere Gefährlichkeit von Glücksspielen im Internet

Bislang wurden die spezifischen Charakteristika von Glücksspielen im Internet nur selten untersucht. Es besteht jedoch die Einschätzung in der wissenschaftlichen Literatur, dass das Vertriebsmedium Internet grundlegend die Art und Weise und die Struktur der Glücksspiele ändert und sie problematischer und zu Spielen mit höherer Suchtgefahr macht.[2] Ein Online-Glücksspiel unterscheidet sich damit maßgeblich von demselben lediglich offline angebotenen Spiel.

Die *besondere Gefährlichkeit des Internetglücksspiels* gegenüber den bisherigen Formen beruht vor allem auf der stärkeren Ausprägung zweier ausschlaggebender Beurteilungskriterien für die Suchtgefahr von Glücksspielen: ihrer Verfügbarkeit und Ereignisfrequenz.

1 Vgl. das Aufforderungsschreiben der Europäischen Kommission vom 1. Februar 2008, Nr. 2007/4866, ZfWG 2008, 32 ff.

2 Vgl. M. Griffiths, 2003, *Internet Gambling: Issues, Concerns, and Recommendations*, CyberPsychology & Behavior, Vol. 6 (6), 557-568, und M. Griffiths & A. Barnes, 2007, *Internet Gambling: An Online empirical study among student gamblers*, International Journal of Mental Health and Addiction, *online*, 19 Seiten.