www.jusletter-it.eu

Burkhard Schafer / Wiebke Abel

Guter Ork, Böser Ork: Snowden und die staatliche Überwachung von Online-Spielen in Grossbritannien

British and American secret services infiltrated online role games on a massive scale, or so the Snowden documents indicate. But do we need to be worried about this new field of surveillance, or is it more a concern about the appropriate use of taxpayers money on an obviously frivolous endeavour? Using arguments from psychology, cultural studies and anthropology in addition to legal arguments from UK and German law, we argue that far from being a trivial addition to our lives, playing is a constitutive art of «homo ludens» in modern, capitalist societies. By submitting gaming behaviour to the police officer's gaze, we get closer than ever to a form of surveillance that threatens to capture us in our entirety – not just what we are, but what we are longing to be.

Category: Articles
Field of law: Data Protection; Data Security
Region: United Kingdom

Citation: Burkhard Schafer / Wiebke Abel, Guter Ork, Böser Ork: Snowden und die staatliche Überwachung von Online-Spielen in Grossbritannien, in: Jusletter IT 15 May 2014

Inhaltsübersicht

Der Mensch spielt nur, wo er in voller Bedeutung des Worts Mensch ist, und er ist nur da ganz Mensch, wo er spielt. Friedrich Schiller

1 Einleitung

[Rz 1] Am 9. Dezember 2013 kommentierte der britische Guardian «To the National Security Agency analyst writing a briefing to his superiors, the situation was clear: their current surveillance efforts were lacking something. The agency's impressive arsenal of cable taps and sophisticated hacking attacks was not enough. What it really needed was a horde of undercover Orcs».[1] Was sich zuerst wie eine Parodie der Satirezeitschrift «The Onion» liest, hatte einen sehr realen Hintergrund. Unter den letzten Enthüllungen über die Aktivitäten der amerikanischen NSA durch die «Snowden-Dokumente» befanden sich auch Memoranden aus dem Jahre 2008, die anzeigten, dass sowohl die NSA als auch das FBI und der britische Geheimdienst «Government Communications Headquarters» (GCHQ) seit einiger Zeit virtuelle Online-Welten und insbesondere populäre Rollenspiele wie World of Warcraft zur Beobachtung verdächtiger Aktivitäten infiltriert hatten.[2] Die Sicherheitsdienste hatten signifikante Kapazitäten aufgebaut, um insbesondere das Xbox Live Konsolennetzwerk mit seinen mehr als 48 Millionen Spielern zu infiltrieren. Von Orks in World of Warcraft zu Avataren in Second Life reichen die Rollen, die Agenten dabei annahmen, um in Echtzeit Informationen sammeln zu können. Eine NSA-Studie aus dem Jahre 2008 mit dem Titel «Exploiting Terrorist Use of Games & Virtual Environments» beschreibt Online-Rollenspiele als eine Umgebung mit besonders vielen Angriffszielen, in denen sich die Agenten «ungetarnt tarnen können.»[3]

[Rz 2] Das Interesse, das die Sicherheitsdienste an dem Verhalten von Bürgern in virtuellen Welten anscheinend zeigen, veranschaulicht drastisch, wie sehr das virtuelle Online-Leben mit dem realen Offline-Leben immer mehr verschmilzt. Je mehr Zeit wir online verbringen und dort Kontakte und Netzwerke aufbauen, desto mehr wird dieses virtuelle Leben ein essentieller Bestandteil unserer Persönlichkeit. Es findet ein Prozess statt, den man als «Virtualisierung» des Lebens bezeichnen kann. Psychologen und Soziologen beschreiben schon seit einiger Zeit den Einfluss, den dieser Prozess auf unser Leben hat, wenn vieles, was unser Leben ausmacht, aus digitalen Daten und Informationen besteht und bestimmte soziale Kontakte teilweise nur im virtuellen Leben

[1] James Ball(2013), Xbox Live among game services targeted by US and UK; http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life(alle Internetquellen zuletzt aufgerufen am 10. April 2014).

[2] NSA, MHS and GCHQ «Get in the Game» with Target Development for World of Warcraft Online Gaming; https://www.documentcloud.org/documents/889128-games.html.

[3] «Hide in plain sight» im englischen Original.

bestehen und ausgelebt werden.[4] Neben die Virtualisierung tritt dabei zunehmend die «gamification», der Gedanke, dass immer mehr Lebensabläufe in der Form von «Spielen» stattfinden und spieltypische Elemente und Prozesse immer häufiger in spielfremden Kontexten auftreten.[5] Geheimdienste und andere Ermittlungsbehörden haben daher ein verstärktes Interesse daran, Zutritt zu diesen virtuellen Welten zu haben, Zugriff auf diese Daten und die Kommunikation von Spielern zu erlangen. Zum einen ermöglicht dies Aufschlüsse über die sozialen Netzwerke von Zielpersonen. Abstrakt betrachtet sind diese Spielwelten erst einmal ein Kommunikationsmedium, und es ist zumindest nicht a priori auszuschließen, dass es daher auch von kriminellen Gruppen benutzt werden kann, um Informationen auszutauschen – insbesondere dann, wenn die Beteiligten befürchten müssen, dass konventionelle Kommunikationsmedien, wie ihr E-Mail-Konto oder auch nur das Telefon, bereits überwacht werden. Darüber hinaus aber, und dies ist das hauptsächliche Thema dieses Beitrages, ermöglicht es auch Einsichten in die Psychologie von Verdachtspersonen, etwa ihre Risikobereitschaft oder «Führungsqualitäten». Diese schwieriger zu erfassenden Eigenschaften scheinen zumindest auch eine Rolle für die Sicherheitsbehörden gespielt zu haben, wurden doch anscheinend Einsichten in das Spielverhalten auch dazu verwendet, möglicherweise geeignete Rekruten zu identifizieren.[6]

[Rz 3] Die rechtliche Einordnung dieser Art von Überwachungstätigkeiten wirft eine Reihe von neuen Fragen auf, die sich an der Schnittstelle von Datenschutzrecht, polizeilichem Ermittlungsrecht und der Psychologie und Soziologie der neuen Medien bewegen. Unterschieden werden kann dabei auch, ob der polizeiliche Eingriff auf einem konkreten Tatverdacht beruht und sich nur gegen spezifische Verdachtspersonen richtet, oder ob die Überwachung von Online-Spielen Teil der kriminalpräventiven Massenüberwachung geworden ist. In beiden Fällen fragt sich, wie und in welchem Umfang Datenschutzbestimmungen und Ermittlungsgrundsätze, die für die physische Welt entwickelt wurden, auf diese virtuellen Welten anzuwenden sind. Damit stellt sich auch die Frage nach der Natur von (virtuellen) Spielen. In Deutschland hat dabei das Bundesverfassungsgericht (BVerfG) in seinem Urteil zur «Online-Durchsuchung» mit der Schaffung des Grundrechtes auf Vertraulichkeit und Integrität informationstechnischer Systeme («IT Grundrecht») einen rechtlichen Rahmen geschaffen, der versucht, der subjektiven Bedeutung, die wir immer mehr unseren Online-Leben zumessen, gerecht zu werden.[7] In Großbritannien hingegen ist die rechtliche Situation noch weitestgehend ungeklärt. In einem Gutachten von Jemima Stratford QC für die parlamentarische Arbeitsgruppe zu Dronen vom 29. Januar 2014 kommt es allerdings zu erheblichen Zweifeln bezüglich der Rechtmäßigkeit sowohl der Datenerhebung als auch der Datennutzung durch den Britischen Geheimdienst GCHQ.[8] Es ist vielleicht an sich schon bemerkenswert, dass eine Arbeitsgruppe zu Dronen die erste parlamentarische Gruppe gewor-

4 Siehe dazu z.B. Sherry Turkle, The Second Self: Computers and the Human Spirit (Cambridge: MIT Press, 2005); Sherry Turkle, Life on the Screen: Identity in the Age of the Internet (New York: Simon and Schuster, 1995); Sherry Turkle, Simulation and Its Discontents (Cambridge: MIT Press, 2009).

5 Siehe z.B. Groh, Fabian (2012), «Gamification: State of the art definition and utilization». *Proceedings of the 4th seminar on Research Trends in Media Informatics*; Hou, Huei-Tse(2012), «Exploring the behavioral patterns of learners in an educational massively multiple online role-playing game (MMORPG)». *Computers & Education*58.4: 1225–1233.

6 Nicht zu abwegig, sind doch einige der Charaktereigenschaften, die von Online-Spielen ableitbar sind, relevant für Verantwortugspositionen und erlauben auch Rückschlüsse auf die Einstellung der Spieler zu gesellschaftlichen Werten. Siehe etwa Richard Hartshorne/Phillip J. VanFossen/Adam Friedman (2014), MMORPG Roles, Civic Participation and Leadership Among Generation Y. International Journal of Gaming and Computer-Mediated Simulations 4:1, 55–67.

7 Urteil des Bundesverfassungsgerichts 1 BvR 370/07vom 27. Februar 2008.

8 http://www.tom-watson.co.uk/wp-content/uploads/2014/01/APPG-Final.pdf.

den ist, die einen externen rechtlichen Experten zum Thema der Online-Überwachung befragt und das Ergebnis auch öffentlich gemacht macht. Der Grund dafür – und die Hauptsorge für Stratford – ist das Problem der möglicherweise illegalen Weiterverwendung der Daten, die von britischen Behörden gesammelt und an die USA weitergegeben werden. Insbesondere befürchtet sie, dass deren Verwendung für die Planung von Dronen-Angriffen britische Beamte zu potentiellen Beihelfern von Straftaten werden lässt. Obgleich der Bericht daher schwerpunktmäßig Einschränkungen in der Verwendung der Daten analysiert, kommt er auch zu einer skeptischen Einschätzung der Methoden, mit denen die Daten erhoben wurden. Ihre Analyse, wie die meisten der rechtlichen Stellungnahmen zu diesem Thema, nimmt dabei an, dass die auf den Snowden-Dokumenten beruhenden Medienberichte korrekt sind. Dabei reflektiert sie deren selektive und unsichere Natur. Obgleich die britischen Stellen wiederholt versichert haben, dass alle Aktivitäten rechtskonform durchgeführt wurden und auf juristische Beratung beruhten, ist bislang nichts über die Natur oder den Inhalt dieser Rechtsauskunft bekannt. Stratford analysiert nicht die Überwachung von Online-Spielwelten, deren Existenz erst nach ihrem Bericht bekannt wurde. Sie ist aber besonders kritisch gegenüber den Versuchen, eine «pattern of life» Analyse durchzuführen, die sowohl Verdächtige als auch Unbeteiligte in ihrer Gesamtperson zu erfassen sucht. Für diese Art der Analyse sind, wie wir sehen werden, Daten von Spielwelten besonders relevant.

[Rz 4] In unserem Beitrag entwickeln wir anhand der vorhandenen Fakten einen ersten Fragenkatalog mit den nach unserer Auffassung dringlichsten Rechtsfragen. Im nachfolgenden Teil analysieren wir einige dieser Fragen aus einer rechtsvergleichenden Perspektive. Wir diskutieren die rechtliche Einordnung nach britischem Recht und vergleichen diese mit deutschem Recht. In Großbritannien hat der GCHQ spätestens seit 2008 Online-Spiele überwacht und infiltriert. Daher steht auch für uns die Frage nach der Rechtmäßigkeit dieser Tätigkeiten nach britischem Recht im Vordergrund. Generell ermöglicht das Medium Internet aufgrund seines vernetzten und grenzenlosen Designs extraterritoriale Ermittlungsarbeit. In Online-Rollenspielen können sich Personen verschiedenster Herkunft häufig in Koalitionen zusammenschließen, in World of Warcraft etwa den «Zünften» («guilds»), sodass es in der Regel nicht möglich sein wird, die Überwachung auf Angehörige des eigenen Landes zu beschränken, oder auf Spieler, die sich geographisch innerhalb der eigenen Jurisdiktion befinden. Ebenso wenig wird normalerweise der Ort des Servers, auf dem die virtuelle Welt läuft, eine sachliche Grenze für Ermittlungs- und Überwachungstätigkeiten sein, womit es aus der Perspektive einzelner Spieler unmöglich wird, vorherzusagen, mit welcher Art von staatlicher Überwachung sie konfrontiert werden können. Langfristig verlangt dies daher nach unserer Ansicht eine internationale Harmonisierung von datenschutzrechtlichen und ermittlungstechnischen Gesetzen und Vorschriften. Ob und wie sich dies zumindest innerhalb der EU umsetzen lassen könnte, deuten wir mit unserem Beitrag für das britische und deutsche Recht an.

2 Hintergrund

[Rz 5] Die Snowden-Dokumente zeigen, dass die britische Geheimdienstbehörde GCHQ zusammen mit der NSA Vorreiter im Infiltrieren und Überwachen von Online-Spielen ist.[9] GCHQ ist diejenige britische Geheimdienstbehörde, die sich in erster Linie mit Kryptographie, Verfahren

[9] Groh(Fn. 5).

zur Datenübertragung und der Fernmeldeaufklärung befasst. Der GCHQ, und insbesondere die Unterorganisation «Communications Electronics Security Group (CESG)», ist für die Sicherung der elektronischen Kommunikation und Computersysteme des Vereinigten Königreichs zuständig.[10] Es bildet zusammen mit der NSA und anderen angelsächsischen Geheimdiensten eine Allianz (sogenannte «Fünf Augen», eine UK/USA/CA/AU/NZ Allianz) zur technischen Nachrichtengewinnung. Es ist anzunehmen, dass unter dieser Allianz auch viele der gemeinschaftlichen Internet- und Telekommunikationsspionageaktivitäten ausgeführt wurden, die unter dem Codenamen «Tempora» gelaufen sind. Tempora ist der Codename einer britischen Geheimdienstoperation zur Überwachung des weltweiten Telekommunikationsverkehrs, die in ihrem Umfang wahrscheinlich sogar über das amerikanische PRISM Projekt hinausgeht. Unter den Konzepten «Mastering the Internet» und «Global Telecoms Exploitations», wurden von GCHQ Internetknotenpunkte und transatlantische Datenverbindungen angezapft. Dies erlaubt GCHQ den gesamten Datenverkehr, der über das transatlantische Glasfasernetz nach Großbritannien hineinfließt oder das Land verlässt, auszuspähen. Laut den Snowden-Dokumenten wurden zur Überwachung und Analyse der Daten über 200 Glasfaserverbindungen angezapft und 500 Mitarbeiter eingesetzt. Theoretisch zumindest gibt dies GCHQ Zugriff auf 21.6 Petabytes pro Tag, das zweihundertfache der gesamten Sammlung der Britischen Nationalbibliothek.[11] Laut GCHQ werden dabei Kommunikationen zwischen Parteien in Großbritannien herausgefiltert – dies gibt, wie auch bei der amerikanischen NSA, den Gedanken wieder, dass rein innerstaatliche Aktivitäten nicht in ihren Zuständigkeitsbereich fallen. Es ist aber unklar, wie dies technisch umsetzbar sein soll.

[Rz 6] In diesem Zusammengang mag die «manuelle» Überwachung von Online-Spielen in der Tat kaum mehr als eine Fußnote sein. Wie so oft bei geheimdienstlicher Tätigkeit ist es schwer, Details über die Operationen herauszufinden. Den Snowden-Dokumenten ist zu entnehmen, dass eine der zentralen Motivationen und Begründungen für die Überwachungstätigkeiten war, dass Terroristen oft «feature-reiche» Internetdienste wie E-Mails, VoIP und Webforen ausnutzen, um miteinander zu kommunizieren und Daten auszutauschen. Daher ist es nach Auffassung von GCHQ und NSA sehr wahrscheinlich, dass Terroristen die Kommunikationsmöglichkeiten von Online-Spieleplattformen und virtuellen Welten ebenfalls weitreichend ausnutzen würden.[12] Eine Überwachung und Infiltrierung dieser virtuellen Welten wurde daher als eine vielversprechende Datenquelle angesehen. Diese Annahme wurde auch durch die rapide wachsende Spielerzahl gestützt. Online-Spiele haben mittlerweile eine weltweite Spielerzahl von ca. 400 Milliarden Spielern[13] und die Spielindustrie eine Wachstumsrate von 20%, im Vergleich zu z.B. einer 7,5% Wachstumsrate der Fernsehindustrie.[14]

[Rz 7] Laut dem NSA-Dokument ermöglicht die Überwachung von Online-Spielen die Planung und Durchführung von Hacking-Attacken, eine Profilerstellung der sozialen Netzwerke von Verdächtigen durch sogenannte «buddy lists» und ihre Interaktionen mit anderen Spielern, die Erlangung identifizierender Daten wie z.B. Fotos, Geodaten und einer Sammlung von Kommunikationsdaten. Darüber hinaus könnte Überwachung jederzeit in Rekrutierung von Informanten

[10] Richard Aldrich, GCHQ: The uncensored story of Britain's most secret intelligence agency (HarperPress, London: 2010).

[11] http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

[12] Hartshorne/VanFoussen/Friedman(Fn. 6), S. 3.

[13] Game Market Research, www.newzoo.com

[14] Hartshorne/VanFoussen/Friedman(Fn. 6), S. 6.

umgewandelt werden.

[Rz 8] Die Überwachung soll insbesondere durch Spielpräsenz durchgeführt werden.[15] Dies bedeutet, dass NSA- und GCHQ-Agenten sich als Spieler anmelden, aktiv am Spiel teilnehmen und dieses ggf. auch beeinflussen. Dies ermöglicht ihnen, die relevanten Daten und Spielerinformationen zu sammeln und Rückschlüsse auf Netzwerke in der realen Welt zu ziehen. Bei diesen Tätigkeiten sind sie durch ihre Avatare getarnt und können somit von anderen Spielern und den Spielbetreibern nicht als Ermittler identifiziert werden. Das NSA-Dokument spezifiziert weiterhin als eine Möglichkeit der Datenerlangung, Partnerschaften mit «prominenten» Avataren oder virtuellen Firmenrepräsentationen z.B. in Second Life einzugehen. Dies führt zur weiteren «Einbettung» des verdeckten Ermittlers in das neue soziale Umfeld und zum Aufbau einer «Legende». Anders als in Deutschland, wo der Einsatz verdeckter Ermittler durch § 110a ff. der Strafprozessordnung (StPO) und die «Gemeinsamen Richtlinien der Justizminister und der Innenminister der Länder über die Inanspruchnahme von Informanten sowie über den Einsatz von Vertrauenspersonen (V-Personen) und Verdeckten Ermittlern im Rahmen der Strafverfolgung» streng geregelt ist, fehlt in Großbritannien ein rechtlicher Rahmen. Insbesondere ist er nicht nur subsidiär und bei schwerwiegenden Straftaten zulässig. Dieser ungeregelte Einsatz verdeckter Ermittler hat unlängst zu schweren Missbräuchen in der «Offline-Welt» geführt. Erst kürzlich ist Großbritannien wegen Menschenrechtsverletzungen durch verdeckte Ermittler ins internationale Scheinwerferlicht geraten.[16] In der «Marc Kennedy Affäre»[17] hatten verdeckte Ermittler jahrzehntelang politische Protestgruppen infiltriert. Unter ihren künstlichen Identitäten waren sie feste Beziehungen auch intimer Natur mit Mitgliedern der Zielgruppe eingegangen. Ziel war, ihren neuen Identitäten mehr Glaubhaftigkeit zu verleihen und einen besseren Zugang zu internen Informationen der politischen Gruppen zu erlangen. Einige haben in diesem Doppelleben sogar Kinder gezeugt. Nach Beendigung der verdeckten Ermittlungen – und somit der Aufgabe ihrer künstlichen Identitäten – sind sie aus dem Leben der überwachten Mitglieder spurlos verschwunden. Die Betroffenen dieser Handlungen machen Verletzungen ihrer Menschenrechte auf den Schutz ihrer Privatsphäre geltend.[18] Britische Gerichte haben sich bisher mit dem Thema noch nicht befasst, doch als Konsequenz wird der Einsatz von verdeckten Ermittlern nun stärker reguliert.[19] Allerdings ist es unklar, ob diese Regeln auch auf Online-Welten ausgedehnt werden sollen.

[Rz 9] Die Geheimdienste haben jedoch nicht nur menschliche Agenten eingesetzt, um Online-Spiele zu überwachen, sondern auch Software-Produkte, die insbesondere vom GCHQ entwickelt worden sind.[20] Eine «Vollzeitüberwachung» von Online-Spielen durch menschliche Agenten ist eine ressourcenintensive Aufgabe, die in der Regel mit den bestehenden Kapazitäten nicht durchführbar ist. Daher ist das «Outsourcing» von Überwachungstätigkeiten an Software-Produkte eine Möglichkeit, um Online-Spiele umfassend zu überwachen sowie Metadaten zu sammeln und auszuwerten.

[Rz 10] Fraglich ist, wie diese Überwachungstätigkeiten rechtlich einzuordnen sind. Ganz kon-

15 Hartshorne/VanFoussen/Friedman(Fn. 6), S. 62.

16 Paul Lewis/Rob Evans(2013), UN official calls on British government to investigate undercover police scandal. http://www.theguardian.com/uk/2013/jan/23/un-official-undercover-police-scandal.

17 Marc Kennedy ist einer der Ermittler, der während den Ermittlungen enttarnt wurde.

18 Ibid.

19 Paul Lewis/Rob Evans(2013), Undercover policing faces tighter regulation after Mark Kennedy scandal. http://www.theguardian.com/uk/2013/jun/18/undercover-policing-faces-tighter-regulation.

20 Groh(Fn. 5), S. 8.

kret werfen die durch den Bericht rudimentär beschriebenen ermittlerischen Tätigkeiten einige wichtige Fragen für das Recht der polizeilichen Ermittlung und das Datenschutzrecht auf:

1. Wie sind die Eigenschaften eines Avatars datenschutzrechtlich zu verstehen? Wenn diese mit der natürlichen Person in der realen Welt verknüpft sind und ggf. die Avatareigenschaften zu einem festen Bestandteil der Persönlichkeit des Spielers werden, dann könnte das Sammeln dieser Daten datenschutzrechtlichen Gesetzen und Rechtsvorschriften unterliegen.
2. Sind Informationen, die Spieler in einer «Massively Multiple Online Role-Playing Game» (MMORPG) über sich preisgeben – und dies sind unter anderem die Eigenschaften des Avatars – *öffentlich zugänglich*, wenn das Spiel hinter einer «paywall» liegt oder zumindest der Registrierung bedarf? Hat in diesem Fall der Anbieter des Spiels «freiwillig» der Polizei Zugang gewährt, obwohl er zumindest zu einem gewissen Grad von ihnen getäuscht wurde? In der deutschen «IT Recht» Entscheidung des BVerfG zum Einsatz von «Trojanern» spielte diese Unterscheidung eine wichtige Rolle.[21]
3. Was ist der Status der Ermittler? Wie bereits oben angegeben, sind sie nach deutschem Recht wahrscheinlich als verdeckte Ermittler einzustufen, was bedeuten würde, dass diese Art des Ermittelns nur in besonders schwerwiegenden Fällen zulässig wäre und staatsanwaltschaftlicher Genehmigung bedürfte. Macht es einen Unterschied, dass es im Moment für die Polizei überhaupt nicht möglich ist, dem Spiel als «Polizisten» beizutreten? Dessen Software strukturiert seine Wirklichkeit so, dass Teilnahme nur durch einen der vorgegebenen Avatar-Typen möglich ist, die alle in den Gesamtrahmen der zur virtuellen Welt gehörenden «Legende» als Abenteuerspiel passen. Gibt es hier Handlungsspielraum, oder sogar Handlungsbedürfnis, de lege lata, etwa durch einen normierten «Polizei-Avatar», der das öffentliche und offene Ermitteln in einer Spielwelt ermöglichen würde?[22]
4. Wie weit dürfen die Polizisten Normen verletzen, wenn dies für die verdeckte Untersuchung notwendig ist? Regelmäßig werden sie zumindest die «End User License Agreements» (EULAs) und die Geschäftsbedingungen des Spielanbieters («Terms of Service», kurz ToS) bei der Anmeldung verletzen, da diese die Registrierung typischerweise an den Zweck des Spielens binden. Zumindest in den USA könnte dies aufgrund einer umstrittenen Rechtsreform zur Kriminalisierung von diesen prima facie eigentlich nur vertragsrechtlichen Verletzungen geführt haben,[23] sodass wenigstens unter diesem Gesetz (oder dieser Interpretation des Gesetzes) der verdeckte Ermittler schon durch die Anmeldung eine Straftat begangen hätte.
5. Handeln sie exterritorial und werden dadurch Fragen des internationalen Rechts berührt? In Frage käme hier zum einen eine Verletzung der Souveränität des Landes, auf dessen Servern das Spiel läuft. Oder ist gar das «Recht Aetherias» das hier relevante, wenn wir virtuelle Welten als supranationale, staatenähnliche Gebilde ernst nehmen würden?[24]
6. Wie ist das Betreten einer «virtuellen Wohnung» rechtlich einzuordnen? Ist dies eine «zusätz-

---

21 BVerfG (Fn. 7).

22 So ein Vorschlag von A.S. Rakitianskaia/M.S. Olivier/A.K. Cooper(2011), Nature and forensic investigation of crime in Second Life, http://researchspace.csir.co.za/dspace/bitstream/10204/5399/1/Rakitianskaia_2011.pdf.

23 John C. Dvorak(2011), Violate a TOS or EULA and Go Straight to Jail!, http://www.pcmag.com/article2/0,2817,2392736,00.asp.

24 Journalistisch: Aleks Krotoski(2009), Why World of Warcraft may be the future of the nation-state, http://www.theguardian.com/technology/gamesblog/2009/aug/05/world-warcraft-game-theory; eine akademische Analyse der dahinter stehenden soziologischen und psychologischen Kräften siehe Julian R. Kücklich (2009), Virtual Worlds and Their Discontents Precarious Sovereignty, Governmentality, and the Ideology of Play, Games and Culture, 4.4, S. 340–352.

liche» Hausdurchsuchung oder sind bloß virtuelle Häuser nicht von einschlägigen Gesetzen geschützt (z.B. Art 10 des Grundgesetzes [GG] in Deutschland)?

7. Was ist, juristisch gesehen, der Status der polizeilichen Interaktion mit sogenannten «Non-player Characters» (NPC), künstlichen Intelligenzen, die die Spielwelt bevölkern? Sollten wir ihre Befragung rechtlich als ein «Verhör» konzeptualisieren, als Abfrage einer Datenbank, oder benötigen wir eine dritte Option? Wenn sie dazu gebracht wird, sich anders als von ihrem Programmierer geplant zu verhalten (d.h. nicht nur Informationen, die für das Spiel wichtig sind, preisgibt), ist dies «Hacking», selbst wenn nicht direkt Computer Code verwendet wurde?
8. Das Überwachen einer virtuellen Welt kann ressourcenintensiv sein. Wenn der Verdächtige in einer anderen Zeitzone ist, wie es bei globalen Spielen häufig der Fall sein wird, müsste 24 Stunden lang ein Polizist am Spiel teilnehmen. Anstelle sich persönlich unter dem registrierten Avatar einzuloggen, könnte die Polizei daher auch – wie oben beschrieben – einen Bot verwenden, der zumindest Routineaktionen ohne direkte Kontrolle durchführen kann, etwa andere Spieler fragen, ob sie den Avatar der Zielperson gesehen haben. Da die Polizei dazu einige technische Schutzmaßnahmen der Plattform umgehen muss, wirft dies besondere Fragen auf.

3 Rechtliche Einordnung

[Rz 11] In diesem kurzen Beitrag ist es uns nicht möglich, alle aufgeworfenen Fragen zu analysieren. Unser Fokus im Beitrag liegt daher auf den Punkten 1, 7 und 8, da sie es unter anderem erlauben, Parallelen zur Entscheidung des BVerfG zu ziehen,[25] und somit auf Rechtsprechung zurückzugreifen. Dies ist insbesondere dann relevant, wenn Gesetze hinter dem technischen Fortschritt und hinter den technischen Möglichkeiten zurück bleiben.

3.1 Avatareigenschaften

[Rz 12] Die Frage, wie Eigenschaften eines Avatars datenschutzrechtlich einzuordnen, und somit vor Zugriffen durch staatliche Behörden geschützt sind, bestimmt sich nach den datenschutzrechtlichen Vorschriften des jeweiligen Landes.

[Rz 13] Die Arbeit der britischen Geheimdienste, und somit auch des GCHQ, sind geregelt im «Regulation of Investigatory Powers Act 2000 (RIPA)» (Gesetz über die Regulierung der Ermittlungsbehörden). Allerdings behandelt RIPA, wie der Stratford-Bericht heraushebt, vor allem die Verwertbarkeit der Daten in einem Gerichtsverfahren, was für einen Großteil des geheimdienstlichen Datensammelns irrelevant ist. RIPA erlaubt zudem nur die Erhebung von Metadaten. Es ist wahrscheinlich, dass bereits TEMPORA diese Vorschrift verletzt und auch den Inhalt von Kommunikationen gespeichert hat. Im Kontext der Überwachung von Online-Spielen schließlich ist dies unvermeidbar, da der Inhalt der Kommunikation das Hauptziel des staatlichen Eingriffes darstellt. Zudem sind die Behörden an den «Human Rights Act 1998 (HRA)» (Menschenrechtsgesetz) und an die «European Convention on Human Rights (ECHR)» (Europäische Menschenrechtskonvention) gebunden. Stratford kommt zu dem Ergebnis, dass selbst da, wo RIPA das

[25] BVerfG (Fn. 7).

Verhalten der britischen Geheimdienste erlaubt, RIPA selber in seiner gegenwärtigen Form nicht normkonform und insbesondere mit Europäischem und internationalem Menschenrecht- und Datenschutzrecht unvereinbar ist.[26] Kontrolliert werden Sicherheitsbehörden durch das «Parliamentary Intelligence and Security Committee» (Parlamentarische Intelligenz- und Sicherheitskomitee), den «Interception Commissioner» (Überwachungsbeauftragten) und das «Investigatory Powers Tribunal» (Überwachungsbefugnisse Tribunal). Anders als ihr amerikanisches Gegenstück, dem Foreign Intelligence Surveillance Court (FISA Court oder FIS) gibt es keine Pläne, die Entscheidungen des Tribunals zu veröffentlichen. Von 2000 bis 2009 hatte das Tribunal 956 Beschwerden zu entscheiden, von denen nur vier aufrecht gehalten wurden.[27]

[Rz 14] Relevant für die Ermittlungsbefugnisse des GCHQ ist, wie die Eigenschaften eines Avatars nach britischem Recht einzuordnen sind, und ob diese vor Eingriffen durch Ermittler besonders geschützt sind. RIPA regelt alleine das Verhalten und die Befugnisse von Ermittlungsbehörden, ohne dabei die Ziele der Ermittlungstätigkeiten näher zu definieren. Daher muss hier auf den HRA und die ECHR zurückgegriffen werden. Diese regeln beide in den jeweiligen Art. 8, dass die Privatsphäre, das Familienleben, die Wohnung und der Briefverkehr vor Eingriffen geschützt sind. Dieser Artikel ist also sehr weit gefasst. Die Privatsphäre beinhaltet auch das Speichern, die Verwendung oder Preisgabe persönlicher Informationen. Der Artikel liefert jedoch keine Definition davon, was persönliche Informationen oder Daten sind.

[Rz 15] Eine Definition von persönlichen Daten kann im «Data Protection Act 1998 (DPA)» (Datenschutzgesetz) gefunden werden. Dieser regelt in Art. 1 Abs. 1 DPA, dass «personal data» solche Daten sind, die einer lebenden Person zuzuordnen sind, und diese Person aufgrund dieser Daten (Variante a) oder aufgrund dieser Daten und weiterer Informationen, welche ebenfalls im Besitz des Datenkontrolleurs sind, bzw. von diesem leicht zu beschaffen sind (Variante b), identifiziert werden kann. Fraglich ist daher, ob Avatar-Daten unter diesen Begriff fallen und somit durch Art. 8 HRA und ECHR vor Eingriffen durch staatliche Organe geschützt sind.

[Rz 16] Es erscheint offensichtlich, dass Informationen bezüglich des Avatars einer Person in der Regel persönliche Daten sein werden. Persönliche Daten sind z.B. CCTV Aufnahmen, anhand derer eine Person mithilfe von anderen Aufnahmen identifiziert werden kann.[28] Sofern Spielern nicht automatisch und für jedes einloggen aufs Neue ein Avatar durch einen Zufallsgenerator zugewiesen wird, sollte es in der Regel möglich sein, über den Avatar auch dessen Eigentümer zu identifizieren – Avatare *sind* in der Regel Identitäten und lassen daher eine Wiedererkennung zu. Dies aber muss einen Benutzer systematisch mit seinem Avatar verbinden, die Daten dafür sind notwendigerweise persistent. Ohne diese Möglichkeit der Identifizierung von Benutzern durch ihre Avatare wäre es in der Tat sinnlos für Polizei oder Geheimdienste, als «Mitspieler» in Online-Welten Informationen zu sammeln und so spielt denn auch die Möglichkeit der Benutzeridentifikation eine wichtige Rolle in den NSA-Dokumenten. Auch die Technologie kann hier helfen: Artimetrics bezeichnet dabei die Forschungsrichtung, die Algorithmen zur akkuraten Identifizierung, Klassifizierung und Authentifizierung von Avataren in virtuellen Welten

[26] Stratford, S. 3.

[27] http://www.ipt-uk.com/default.asp?sectionID=16.

[28] *Perry v. the United Kingdom* [2003] no. 63737/00, ECHR 2003-III, Crim LR 281, 38 (referring to *Rotaru v. Romania* [GC], no. 28341/95, §§ 43–44, ECHR 2000-V, and *Amann v. Switzerland* [GC], no. 27798/95, §§ 65–67, ECHR 2000-II).

entwickelt.[29] Dabei ist die Ermittlung von kriminellen Online-Aktivitäten eines der intendierten Anwendungsgebiete.[30]

[Rz 17] Insbesondere in Online-Rollenspielen wird häufig die Webcam-Funktion genutzt, da es die Möglichkeit gibt, mithilfe von speziellen Software-Programmen in Echtzeit die eigenen Gesichtsausdrücke via Webcam dem Avatar zu verleihen.[31] Diese Möglichkeit verstärkt die Verschmelzung der realen mit der virtuellen Identität und führt dazu, dass Avatarinformationen noch stärker mit der Persönlichkeit des Spielers verknüpft sind. Identifizierung der zugrundeliegenden Eigentümer des Avatars wird in diesen Fällen erheblich erleichtert sein. Insbesondere auch in virtuellen Welten mit sexuellen Inhalten bringt dies jede Überwachung damit noch näher an den engsten Intimbereich einer Person. In der Tat hat ein kürzlich durch Edward Snowden veröffentlichtes Dokument aufgezeigt, dass der GCHQ seit 2008 die Webcams von Yahoo-Nutzern abgehört und durch die Webcam gemachte Bilder gesammelt hat.[32] Alleine in einem Zeitraum von sechs Monaten im Jahr 2008 hat der GCHQ Bilder von 1,8 Millionen Yahoo-Nutzern gesammelt. Es wurde hierbei zwar nicht der Videostream komplett abgespeichert, aber alle fünf Minuten ein Standbild aufgenommen. Laut dem Dokument hat der GCHQ versucht, mithilfe von automatischer Gesichtserkennungs-Software die Personen auf den abgefangenen Bildern zu identifizieren. Ziel war dabei, verdächtige Personen aus einer existierenden Liste zu erkennen, und neue «Ziele» auszumachen. Die Auswahl der belauschten Chats sei dabei wahllos gewesen. Allerdings kann dem von Snowden veröffentlichten Dokument zum Abhören der Webcams entnommen werden, dass hierbei unter anderem auch Aufnahmen sexueller Natur gewesen sind – in der Tat scheinen einige Ermittler davon überrascht gewesen zu sein, wie häufig Webcam-Benutzer Bilder von intimen Körperteilen übertragen.[33] Hier kann daher davon ausgegangen werden, dass Informationen über einen Avatar in der Regel persönliche Daten i.S.d. DPA sind.

[Rz 18] Online-Spielwelten, Webcams und sexuelle Aktivität online überschneiden sich in mehrerer Hinsicht. Wie bereits erwähnt, sind Webcams zunehmend eine zusätzliche Funktionalität in Online-Spielen.[34] In der Zukunft werden auch zunehmend «Ganzkörpersensoren» hinzukommen, die zusammen mit Webcams dem Online-Spieler erlauben, Bewegungen und Körperreaktionen aus der physischen Welt direkt in die Online-Welt zu übertragen. Die erhöhte Authentizität des Erlebnisses wird dabei die Grenzen zwischen virtuellem und physischem Empfinden und ihre jeweilige Funktion für die Identitätsbildung weiter verwischen.[35] Mit der größeren Authentizi-

---

[29] Roman V. Yampolskiy/Marina L. Gavrilova (2012), Artimetrics: Biometrics for artificial entities, Robotics & Automation Magazine, IEEE 19.4, S. 48–58.

[30] Roman V. Yampolskiy/Gyuchoon Cho/Richard Rosenthal/Marina L. Gavrilova(2011), Evaluation of face recognition algorithms on avatar face datasets, 2011 International Conference on Cyberworlds (CW), S. 93–99. IEEE.

[31] Sie z.B. die Software «SOEmote» von Sony, https://www.soe.com/soemote.

[32] Spencer Ackerman/James Ball, Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ, The Guardian, http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

[33] http://www.ipt-uk.com/default.asp?sectionID=16.

[34] Siehe auch Nikolaos Savva/Alfonsina Scarinzi/Nadia Bianchi-Berthouze (2012),«Continuous recognition of player's affective body expression as dynamic quality of aesthetic experience». *Computational Intelligence and AI in Games*, *IEEE Transactions on*4.3: 199–212; Stéphanie Buisine et al. (2014),«The Role of Body Postures in the Recognition of Emotions in Contextually Rich Scenarios». *International Journal of Human-Computer Interaction*30.1: 52–62; Ben A.M. Schouten et al.(2011), «Human behavior analysis in ambient gaming and playful interaction». *Computer Analysis of Human Behavior*. Springer London, 387–403.

[35] Siehe etwa Andrea Kleinsmith/Nadia Bianchi-Berthouze(2013), «Affective body expression perception and recognition: A survey». *Affective Computing*, *IEEE Transactions on*4.1: 15–33; M.S.H. Aung et al.(2013), «Getting rid of pain-related behaviour to improve social and self perception: a technology-based perspective». *Image Analysis for Multimedia Interactive Services (WIAMIS), 2013 14th International Workshop on*. IEEE.

tät nimmt aber auch die Möglichkeit zu, vom Online-Verhalten Rückschlüsse auf die physische Person des Spielers vorzunehmen. So können etwa von Haltung und Bewegung eines Avatars, der durch Webcam und Sensoren mit dem Spieler verbunden ist, auch Rückschlüsse auf mentale Problem wie Depressionen gemacht werden.[36] Auch damit erhöht sich die datenschutzrechtliche Problematik, die durch die Überwachung von sensorunterstützen Online-Spielen entstehen. Diese größere Ähnlichkeit zur Realität, und die Einbeziehung von optischen und haptischen Elementen hat vorhersehbarer Weise auch zu neuen Formen des Ausdrucks der Sexualität in Online-Welten geführt.[37] Diese kommen dadurch qualitativ immer näher an sexuelle Erlebnisse in der physischen Welt[38] und damit den Kernbereich des Rechts auf Privatheit heran. Neben der *Form* der Interaktion, immer realistischeren Ansätzen, die die Grenzen zwischen physischen Körpern und Online-Repräsentationen verschwimmen lassen, haben viele der Online-Welten auch ein sexuelles *Thema*, entweder indirekt, nur durch die Benutzer erzeugt wie in Second Life;[39] direkt, als das Thema des Online-Spiels selber; oder auch als eine Form der benutzerinitiierten Subversion, wenn ein ansonsten nicht sexuelles Thema vom Plattformeigentümer vorgegeben wurde, die Spieler aber trotzdem Wege finden, dem Spiel erotische Aspekte zu geben. Dies geschah unter anderem in World of Warcraft,[40] dem Online-Spiel, das in der Überwachung durch GCHQ besonderer Aufmerksamkeit erhielt. Es ist nicht bekannt, ob auch Online-Rollenspiele überwacht wurden, die ein explizites sexuelles Thema haben. Möglichkeiten gäbe es genug, von den Eroge-Spielen (ein Portmanteau Wort aus «Erotik» und «Game»), die sich insbesondere in Japan großer Beliebtheit erfreuen[41] und in ihrer interaktiven Form Dating und Flirten zwischen Spielern verlangen, zu Dating/Spielplattformen wie *Red Light Center*, *Singles: Flirt Up Your Life* und *Playboy: The Mansion*. In all diesen Fällen muss davon ausgegangen werden, dass jedwede Überwachung auch sensible persönliche Daten Unbeteiligter sammeln wird.

[Rz 19] Fraglich ist aber, ob auch andere Avatarinformationen sensible Daten sein könnten. Art. 2 DPA definiert, was sensible persönliche Daten sind. Diese sind Informationen über den ethnischen Hintergrund, politische Meinung, religiöse Zugehörigkeit, Gesundheitszustand, das Sexualleben und Vorstrafen. Ob es sich bei Avatardaten auch um *sensible* Daten im Sinne des Art. 2 DPA handelt, ist problematischer. Zum einen ist es natürlich wahr, dass ein Avatar häufig Eigenschaften haben wird, die radikal anders sind als die seines Besitzers. Muskelbepackte Helden sind in Online-Rollenspielen überdurchschnittlich vertreten, es ist unwahrscheinlich, dass

---

36 So etwa Jyoti Joshi et al.(2013), «Can body expressions contribute to automatic depression analysis?». *Automatic Face and Gesture Recognition (FG), 2013 10th IEEE International Conference and Workshops on*. IEEE.

37 Zek Cypress Valkyrie(2011), «Cybersexuality in MMORPGs: Virtual sexual revolution untapped». *Men and Masculinities*14.1: 76–96; Shaowen Bardzell(2010), «Topping from the Viewfinder: The Visual Language of Virtual BDSM Photographs in Second Life». *Journal For Virtual Worlds Research*2.4; G. Kannabiran/S. Bardzell/J. Bardzell(2012). Designing (for) desire: A critical study of technosexualitiy in HCI. In Proc. of ACM NordiCHI2012. ACM: New York.

38 Besonders radikal sind dabei Ansätze, in denen Partizipanten zwar über das Internet interagieren, aber direkt physische Reaktionen auf der Seite des Partners bewirken können. Siehe etwa Jeffrey Bardzell/Shaowen Bardzell(2011), «Pleasure is your birthright: digitally enabled designer sex toys as a case of third-wave HCI». *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM. Besonders interessant aus datenschutzrechtlicher Sicht Carman Neustaedter/ Saul Greenberg (2012),«Intimacy in long-distance relationships over video chat». *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM.

39 See e.g. Robert Alan Brookey/Kristopher L. Cannon(2009), «Sex lives in second life». *Critical Studies in Media Communication*26.2: 145–164; besonders sensible Probleme werden diskutiert in Shaowen Bardzell(2010), «Topping from the Viewfinder: The Visual Language of Virtual BDSM Photographs in Second Life». *Journal For Virtual Worlds Research*2.4: 1–23

40 I. Paviova(2005), Porncraft: WoW erotica and roleplay forums. http://www.mmorgy.com/2005/11/10.

41 Emily Taylor(2007), «Dating-Simulation Games: Leisure and Gaming of Japanese Youth Culture». *Southeast Review of Asian Studies*29.

ihre Eigentümer den gleichen Grad der körperlichen Fitness haben werden. Typischerweise sind Avatare Phantasiefiguren – Zwerge, Orks, Drachen – oder Gestalten der Geschichte. Wer in einem Online-Rollenspiel, das im Mittelalter angesiedelt ist, die Rolle des Großinquisitors annimmt, ist nicht notwendigerweise katholisch, oder auch nur männlich. Weder eine politische Vorliebe für eine Theokratie, noch Gewaltbereitschaft in dem Versuch, sie herbeizuführen, kann ohne weiteres daraus geschlossen werden. Wenn ein Spieler einen Großteil seiner Zeit in solch einer Rolle verbringt, könnten wir mit Turkle[42] argumentieren, dass dies nichtsdestotrotz seine (oder ihre) Identität *ist*, doch wäre dies immer noch eine problematische Ausdehnung des Begriffs der «sensitiven Daten». Andererseits zeigt aber eine Fülle von psychologischen Studien zur Internetbenutzung, dass Eigenschaften aus der Offline-Welt durchaus in die Online-Welt so projiziert werden, dass mit großer Wahrscheinlichkeit Rückschlüsse auf die «echten» Eigenschaften eine Person gezogen werden können.[43] Geschlechterwandel etwa ist möglich, aber selten, und kann häufig durch typische Verhaltensmuster entdeckt werden.[44] Wer durch seinen Avatar an virtuellen Sexspielen teilnimmt, sagt damit auch einiges über seine sexuelle Orientierung aus.[45] Gerade bei «Problemnutzern» lassen sich über das Verhalten im Netz Rückschlüsse auf psychologische und medizinische Probleme herleiten.[46] So können wir sagen, dass in gewisser Weise die Erfassung von Verhalten in virtuellen Welten dem Persönlichkeitskern besonders nahe kommt – es ermöglicht nicht nur Rückschlüsse darauf, was eine Person ist, sondern auch darüber, was sie träumt, gerne sein zu wollen. Zu diesen Eigenschaften des Avatars selber kommen dann noch die relationalen Eigenschaften – der Freundeskreis und auch wieder gerade für Problemnutzer das gesamte soziale Umfeld. Dies wurde auch im NSA-Bericht besonders hervorgehoben, in dem es gerade darum geht, die sozialen Netzwerke, Freundeskreise und Kontakte von Verdachtspersonen aufzuzeigen.

[Rz 20] Insofern sind Avatardaten vor Zugriffen von Ermittlungsbehörden grundsätzlich geschützt und ein Spieler hat das Recht, über die Preisgabe und Verwertung dieser Daten selber zu bestimmen. In Art. 8 HRA kann durch Geheimdienste jedoch eingegriffen werden, wenn dieser Eingriff gerechtfertigt ist. Dies ist immer dann der Fall, wenn der Eingriff notwendig und verhältnismäßig ist. Notwendig ist er gemäß Art. 8 Abs. 2 HRA unter anderem dann, wenn er Kriminalität verhindert. Dies bietet somit Geheimdiensten in Großbritannien die Möglichkeit, die Überwachungstätigkeiten von Online-Spielen durchzuführen, solange ein vom Gesetz definierter Grund vorliegt. Allerdings ist es sehr fraglich, ob unspezifische Überwachungen darunter fallen können.

---

42 Sherry *Turkle*(2011), Life on the Screen, Simonhuster, New York; siehe auch John A. Bargh/Katelyn Y. A. McKenna/Grainne M. Fitzsimons (2002),Can you see the real me? Activation and expression of the «true self» on the Internet, Journal of social issues, 58.1 S. 33–48.

43 Siehe etwa Elizabeth Behm-Morawitz (2013), Mirrored selves: The influence of self-presence in a virtual world on health, appearance, and well-being, Computers in Human Behavior, 29.1: 119–128; Lewis Weaver(2012), Mirrored Morality: An Exploration of Moral Choice in Video Games, Cyberpsychology, Behavior, and Social Networking, 15.11: 610–614.

44 Nick Yee/Jeremy N. Bailenson/Mark Urbanek/Francis Chang/Dan Merget(2007), The unbearable likeness of being digital: The persistence of nonverbal social norms in online virtual environments, CyberPsychology & Behavior. 10.1: 115–121.

45 Krystelle Shaughnessy, E. Sandra Byers(2014), Contextualizing cybersex experience: Heterosexually identified men and women's desire for and experiences with cybersex with three types of partners, Computers in Human Behavior, 32: 178–185.

46 Siehe z.B. Sally J. McMillan/Margaret Morrison(2006), Coming of age with the internet A qualitative exploration of how the internet has become an integral part of young people's lives, New media & society, 8.1: 73–95; Shao-Kang Lo/Chih-Chien Wang/Wenchang Fang(2005), Physical interpersonal relationships and social anxiety among online game players, CyberPsychology & Behavior, 8.1: 15–20.

Sogenannte «fishing expeditions» sind in der Regel unverhältnismäßig, und es fehlt an empirischen Belegen, dass die Überwachung von Spielwelten wirklich zur Verhinderung von Straftaten geführt hätte.

[Rz 21] In Deutschland gilt prinzipiell für Ermittlungen, dass gemäß Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG das Recht auf informationelle Selbstbestimmung einschlägig ist.[47] Dies bedeutet, dass generell der Einzelne die Befugnis hat, über die Preisgabe und Verwendung persönlicher Daten selber zu bestimmen. Es stellt sich daher die Frage, ob die Eigenschaften eines Avatars persönliche Daten des «Eigentümers» des Avatars sind. Ähnlich wie im britischen Recht kann eine Definition von persönlichen Daten im Deutschen Bundesdatenschutzgesetz (BDSG) gefunden werden.

[Rz 22] Gemäß § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Dies bedeutet, Daten sind dann personenbezogen, wenn sie eine Person bestimmen können. Diese Definition ist im Kern identisch mit der nach britischem Recht. Wie oben analysiert, kann auch ein Avatar ein virtuelles Abbild einer Person sein und verknüpft mit Benutzerkontodaten auf die Identität schließen lassen.

[Rz 23] Bei Avatardaten würde es sich nach deutschem Recht dann um sensible Daten handeln, wenn diese in den Kreis der Daten des § 3 Abs. 9 BDSG fallen, also als Daten über ethnische Herkunft, die politische Meinung, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit und das Sexualleben sind. In diesem Falle unterlägen sie nach § 4d Abs. 5 BDSG der Vorabkontrolle. Wir argumentieren hier, gestützt auf die empirischen Studien zur Psychologie der virtuellen Welt, dass die letzten zwei Kategorien direkt einschlägig sein können. Auch virtuelle Ausdrücke der menschlichen Sexualität sind Ausdruck des Sexuallebens. Gerade hier kann «Fantasie» oder «Spiel» nicht sinnvoll von «Wirklichkeit» unterschieden werden. Dass direkter physischer Kontakt dabei fehlt, ist unerheblich, weder verlangt der Wortlaut des Gesetzestexts, dass «Sexualleben» ausschließlich physischer Kontakt ist, noch wäre normativevaluierend solch eine Einschränkung sinnvoll.[48] Gesundheit wiederum schließt auch geistige Gesundheit ein. Gerade über diese lassen sich durch Spielverhalten aber häufig Rückschlüsse ziehen.[49] Problematischer sind Kategorien wie ethnische Herkunft oder Gewerkschaftszugehörigkeit – jemand der einen Ork in World of Warcraft spielt und sich einer Zunft anschließt, deren

---

47 Siehe z.B. BVerfG (Fn. 7).

48 Siehe insbesondere C. Springer(1996), Electronic eros: Bodies and desire in the postindustrial age. Austin, TX, USA: University of Texas Press; siehe auch Matthew Lombard/Matthew T. Jones(2013), «Telepresence and Sexuality: A Review and a Call to Scholars». *Human Technology: An Interdisciplinary Journal on Humans in ICT Environments*9.1: 22–55; M.T. Whitty(2008), Liberating or debilitating? An examination of romantic relationships, sexual relationships and friendships on the Net. Computers in Human Behavior, 24, 1837–1850; D. Waskul/M. Douglass/C. Edgley(2000), Cybersex: Outercourse and the enselfment of the body. Symbolic Interaction, 23(4), 375–397; R.L. Gilbert/M.A. Gonzalez/N. A. Murphy (2011), Sexuality in the 3D Internet and its relationship to real-life sexuality. Psychology & Sexuality, 2(2): 107–122.

49 Siehe z.B. Nael Hirzallah(2013), «A Simple Exercise-to-Play Proposal that would Reduce Games Addiction and Keep Players Healthy». *International Journal of Advanced Computer Science & Applications*4.2; Sophia Achab et al.,Massively Multiplayer Online RolePlaying Games: Comparing characteristics of addict vs non-addict online recruited gamers in a French adult populationBMC Psychiatry. Jan 2011, Vol. 11, No. 1: 144; Jonathan Scott/Alison P. Porter-Armstrong(2013), Impact of Multiplayer Online Role-Playing Games upon the Psychosocial Well-Being of Adolescents and Young Adults: Reviewing the Evidence, Psychiatry Journal. Jan 2013, Vol. 2013: 1–8; Olivia Metcalf/Kristen Pammer(2014), Physiological Arousal Deficits in Addicted Gamers Differ Based on Preferred Game Genre, European Addiction Research, Vol. 20, No. 1: 23–32; Emily Collins/Jonathan Freeman(2014), Video Game Use and Cognitive Performance: Does It Vary with the Presence of Problematic Video Game Use? Cyberpsychology, Behavior, and Social Networking, Vol. 17, No. 3: 153–159.

Ziel der Sturz des *Lich Kings* ist, ist natürlich nicht ethnisch ein Ork, hat republikanische Überzeugungen und ist in einer Gewerkschaft. Wie oben beschrieben, ist es zumindest strittig, ob es sich bei Avatardaten auch um sensible Daten handeln kann. Im «Trojanerurteil» beschreibt das Verfassungsgericht die Gefahr der Online-Überwachung als Möglichkeit, dass «sich ein *umfassendes* Bild vom Nutzer des Systems ergeben kann».[50] Für Großbritannien erlaubt RIPA gerade diese «Analyse des Lebensprofils», was aber – wie Emima Stratford argumentiert – wahrscheinlich europarechtswidrig ist. Überwachung von Online-Rollenspielen in virtuellen Welten hat zumindest das Potential, ähnlich schwer in die Persönlichkeitsrechte der Betroffenen einzugreifen. Insbesondere dann, wenn es sich um Daten über sexuelle Handlungen handelt, generell aber eben auch gerade dadurch, dass die Totalität der Daten ein Gesamtbild einer Person wiedergibt.

[Rz 24] Wir können also festhalten, dass Avatardaten in beiden Rechtssystemen persönliche Daten der Spieler darstellen und somit durch Datenschutzgesetze vor Eingriffen geschützt sind. Es ist zumindest nicht auszuschließen, dass es sich potentiell auch um sensible Daten handeln könnte, die besonders vor Zugriffen geschützt sind.

3.2 Informationserlangung

[Rz 25] Fraglich ist weiterhin, wie die Informationserlangung durch die aufgrund ihrer Avatare getarnten Ermittler rechtlich einzuordnen ist.

[Rz 26] Im britischen Rechtssystem ist generell durch eine Gesetzesänderung staatliches Hacking gemäß Art. 10 «Computer Misuse Act 1990» (Computer-Missbrauch-Gesetz) ermöglicht worden. Daher ist hier prinzipiell erst einmal unerheblich, wie der Zugang zu den Kommunikationsdaten erfolgt. Dieses Recht ist jedoch eng an die Voraussetzungen der in RIPA geregelten Ermittlungsbefugnisse geknüpft. Verdeckte Ermittlungen sind generell in Abschnitt 2 RIPA geregelt. Hier ist in Art. 29 RIPA geregelt, dass gezielte verdeckte Ermittlungen (targeted covert surveillance) von Verdächtigen möglich sind. Diese gezielte Ermittlung ist definiert als «verdeckte Überwachung, die im Rahmen einer spezifischen Ermittlung unternommen wird, höchstwahrscheinlich private Informationen über eine Person hervorbringen wird und zum Zwecke der Kriminalitätsprävention oder Verhinderung einer schweren Straftat erfolgt». Details zu den Rechten und Pflichten der verdeckten Ermittler, wie oben diskutiert, fehlen und wurden in der Vergangenheit sehr permissiv gehandhabt. Allerdings sind damit sogenannte «fishing expeditions» nicht erlaubt. Diese ungezielten Überwachungen stellen jedoch laut NSA-Dokumenten zumindest einen großen Teil der Überwachungstätigkeiten von Online-Spielen dar. Viele der Überwachungen waren gerade nicht darauf ausgelegt, bereits identifizierte Verdächtige zu überwachen, sondern insbesondere Metadaten und Kommunikationsdaten auf Auffälligkeiten zu untersuchen. Selbst wenn jedoch ausschließlich ein bestimmter Verdächtiger überwacht werden soll, so muss auch dieser in einem ersten Schritt im Spiel identifiziert werden. Somit besteht in diesem Stadium eine gezielte Überwachung nur dieser spezifischen Person ebenfalls nicht. Daher erscheint es nach britischem Recht fraglich, ob diese Tätigkeiten rechtlich unbedenklich sind.

[Rz 27] Gemäß Art. 8 Abs. 4 RIPA ist es jedoch möglich, diese Voraussetzungen zu umgehen, wenn die Überwachung sich auf Daten bezieht, die während der Übertragung durch ein Telekommunikationssystem abgefangen werden. Da Kommunikationsdaten aus virtuellen Welten durch

[50] BVerfG (Fn. 7).

Telekommunikationsmedien übertragen werden, ist dies hier der Fall. Weiterhin muss ein Minister ein Zertifikat ausgestellt haben, welches die Handlungen für notwendig befindet, und dies aufgrund z.B. einer Terrorgefahr der Fall ist (Art. 5 Abs. 3 RIPA definiert die zulässigen Gründe). Damit gibt es nach britischem Recht eine rechtliche Möglichkeit, unspezifizierte Ermittlungen und Überwachungen von Online-Spielen und virtuellen Welten, also sogenannte fishing expeditions, durchzuführen, wenn ein Minister von der Notwendigkeit überzeugt ist.

[Rz 28] In Deutschland hat das BVerfG in seinem Urteil zum «IT Grundrecht» festgestellt, dass zwischen Datenerhebung, bei der «die Verfassungsschutzbehörde Inhalte der Internetkommunikation auf dem dafür technisch vorgesehenen Weg zur Kenntnis nimmt» und einer solchen, bei der die Integrität der Informationssysteme durch technische Maßnahmen kompromittiert wird und Daten damit durch «hacking» dem System sozusagen entrungen werden müssen, unterschieden werden muss.[51] Vorliegend ist es fraglos der Fall, dass die Beamten als verdeckte Ermittler handeln. Sie verschafften sich außerdem Zugang zu Kommunikation, die nicht jedem zugänglich ist. Insofern ist die Situation anders als etwa das einfache Lesen des Blogs eines Verdächtigen. Durch eine Anmeldung zu andern Zwecken als dem Spielen wird das System auch in einer gewissen Weise «manipuliert» – die Eintragungen, die die Polizisten bei der Registrierung machen, werden vom System in Computercode übersetzt, der dann wiederum eine Reaktion der Plattform – hier Zugang zum Spiel – auslöst. Andererseits erlaubt das Gericht es der Polizei ausdrücklich, durch «Legenden», etwa unter einem Pseudonym, an Diskussionen in einem Chatraum teilzunehmen. Trotz einiger «bedenklicher» Entwicklungen in den USA halten wir es für problematisch, eine Registrierung, die die Geschäftsbedingungen einer Webseite verletzt, als «unautorisierten Zugriff» und damit einem Hack gleichzusetzen. Sofern es sich also um menschliche Ermittler handelt, ist das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht einschlägig und die allgemeinen Datenschutzbestimmungen greifen ein. Auch diese allerdings sind ausreichend, um die «fishing expeditions», die auf populären Online-Spielplattformen stattfanden, bedenklich erscheinen zu lassen.

3.3 Virtuelle Ermittler

[Rz 29] Eine (grundrechtsrelevante) Kompromittierung von ICT-Systemen und virtuellen Welten könnte jedoch dann vorliegen, wenn nicht menschliche Ermittler, sondern Bots die Überwachung übernehmen. Technisch gesehen können die Beamten aufgrund der vom GCHQ entwickelten Software-Programme ohne größere Probleme ein Software-Konstrukt an ihrer Stelle die virtuelle Welt betreten lassen. Dieses könnte sogar eine vorformulierte Frage an alle Avatare stellen, denen es online begegnet: «Ist XYZ online, und wo ist er?» Sobald eine positive Antwort gegeben wird, informiert es die Polizei, so dass ohne große Ressourcenimplikationen eine 24-stündige Überwachung möglich ist. Derartige Bots sind technisch möglich und werden in der Tat häufig von Spielern zum «schwindeln» benutzt.

[Rz 30] Derartige Bot-Spieler stellen für Online-Spielplattformen ein Problem dar: sie werden etwa gerne von Spielern verwendet, die monotone und zeitaufwendige Arbeiten (wie z.B. «Gold abbauen») nicht selber durchführen wollen. Insbesondere für Plattformen, die Werbeeinnahmen als Einnahmequelle haben und daher darauf angewiesen sind, dass Spieler möglichst lange ein-

[51] BVerfG (Fn. 7).

geloggt sind, ist dies ein Problem. Aber auch andere Betreiber versuchen, dieses Verhalten als «Verstoß gegen die Spielregeln» zu unterbinden, auch um «in-Spiel Inflation» von Gütern zu verhindern.[52] Zusätzlich zum Vertragstext, den Terms of Service, der typischerweise das Benutzen von Bots verbietet, gibt es daher eine ganze Reihe von technischen Möglichkeiten, um die Teilnahme von Bots an Online-Spielen, wenn nicht zu verhindern, so doch aufzudecken und zu erschweren. Automatisches Registrieren zum Beispiel können «Agent exclusion clauses» im html-Text einer Websiteverhindern[53], allerdings nur für Bots, die so programmiert sind, diese zu lesen und zu respektieren. Aufwendiger sind «reverse Turing» oder auch «CAPTCHA»-Tests, in denen der Mensch/Bot aufgefordert wird, Aufgaben wie etwa Gesichter- oder Bilderkennung zu bewältigen, die zurzeit Maschinen normalerweise nicht lösen können.[54] Viele dieser Maßnahmen verhindern nur automatische Registrierung, nicht aber Registrierung durch einen Menschen, der dann seinen Bot für ihn Handlungen durchführen lässt. Es gibt aber auch die Möglichkeit, CAPTCHA-Tests realistisch in ein Spielumfeld einzubauen, wo es dann auch noch nach der Registrierung Bots identifizieren und blockieren kann.[55] Zudem gibt es eine ganze Reihe von automatischen und semi-automatischen Methoden, Bots im Spiel durch ihr Verhalten zu identifizieren, entweder interaktiv oder auch durch rein passives Profiling.[56] Die Geheimdienste würden also zumindest diese technischen Sicherungen umgehen müssen.

[Rz 31] Da das britische Rechtssystem, wie oben unter 3.2 erörtert, staatliches Hacken prinzipiell zulässt, könnten britische Geheimdienste und andere Ermittlungsbehörden im gesetzlichen Rahmen diese virtuellen Welten auch mit Bots infiltrieren. Hier würde diese Art der Infiltrierung aber in erster Linie vertragsrechtliche Fragen mit dem Spielentwickler aufwerfen, da die Schutzmaßnahmen gegen Bots nicht dem Schutz der Spieler und deren Privatsphäre dienen.

[Rz 32] In Deutschland würde dagegen die Frage aufgeworfen, ob dies einen vergleichbaren Tatbestand zu der Überwachung durch den Bundestrojaner erzeugt – auch dort werden softwaregestützte Schutzmechanismen überwunden, um eine Infiltrierung durch ein semi-autonomes Software-Konstrukt zu ermöglichen und dadurch die Sicherheit und Vertraulichkeit von ICT-Systemen kompromittiert. Allerdings dienen die zu überwindenden Schutzmaßnahmen hier nicht dem Privatheitsschutz, was ein potentiell relevanter Unterschied ist. Zwar werden technologische Schutzmaßnahmen umgangen und dadurch die Integrität des Informationssystems kompromittiert, um im Ergebnis einen Eingriff in die Privatsphäre zu ermöglichen, doch fehlt es hier

---

52 Gianvecchio et al.(2009), Battle of Botcraft: fighting bots in online games with human observational proofs, Proceedings of the 16th ACM conference on Computer and communications security, ACM; Aurangzeb et al.(2009), Mining for gold farmers: Automatic detection of deviant players in mmogs, International Conference on Computational Science and Engineering, CSE'09. Vol. 4. IEEE. Zum Problem der Inflation in virtuellen Welten siehe Jaron Harambam/Stef Aupers/Dick Houtman (2011), Game over? Negotiating modern capitalism in virtual game worlds, European Journal of Cultural Studies, 14.3: 299–319.

53 M.L. Boonk et al. (2005), Agent Exclusion on Websites, LEA, 13–20.

54 Siehe z.B. Adam Cornelissen/Franc Grootjen(2008), A modern turing test: Bot detection in MMORPGS, Proceedings of the 20th Belgian-Dutch Conference on Artificial Intelligence (BNAIC2008), 49–55; Yong Rui/Zicheng Liu(2004), ARTiFACIAL: Automated reverse Turing test using FACIAL features, Multimedia Systems 9.6: 493–502; Amalia Rusu/Venu Govindaraju(2004), Handwritten CAPTCHA: Using the difference in the abilities of humans and machines in reading handwritten words, IEEE Ninth International Workshop on Frontiers in Handwriting Recognition, IWFHR-9.

55 Yang-Wai Chow/Willy Susilo/Hua-Yu Zhou(2010), CAPTCHA challenges for massively multiplayer online games: Mini-game CAPTCHAs, IEEE 2010 International Conference on Cyberworlds (CW).

56 Siehe z.B. Roman V. Yampolskiy/Venu Govindaraju(2008), Embedded noninteractive continuous bot detection, Computers in Entertainment (CIE), 5.4 , Nr. 7; Ruck Thawonmas/Yoshitaka Kashifuji/Kuan-Ta Chen(2008), Detection of MMORPG bots based on behavior analysis, Proceedings of the 2008 International Conference on Advances in Computer Entertainment Technology, ACM.

an dem direkten kausalen Zusammenhang zwischen der technologischen Umgehungsmaßnahme und der Verletzung der Privatsphäre. Zwar hat das BVerfG nicht ausdrücklich gesagt, dass die Manipulation des Informationssystems eine Umgehung von dedizierten Maßnahmen zum Schutz der Privatheit sein muss, doch scheint eine solche enge Interpretation sachangemessen zu sein. Sollte zum Beispiel die Polizei einen DRM-Schutz (Digital Rights Management) umgehen, um einen Videoclip mit verdächtigen Informationen auf ihrem eigenen Musikplayer spielen zu können, so scheint dies nicht die Art von Bedenken zu erzeugen, die das Gericht in seiner Entscheidung leiteten. Ziel der DRM ist es, Verletzung von Urheberrecht zu verhindern, Ziel der CAPTCHA-Software ist es, Inflation von virtuellem Gold zu verhindern, die legitimen Interessen des Eigentümers dieser Schutzmaßnahmen werden durch das polizeiliche Handeln nicht geschädigt. Im Gegensatz dazu schädigt die Polizei genau das intendierte Gut, wenn sie technologische Maßnahmen zum Schutz der Privatsphäre in ihrer Ermittlungsarbeit umgeht.

[Rz 33] Eine interessante Variante ergibt sich, wenn die Untersuchungsbeamten oder Geheimdienstler selber wiederum Daten nicht von anderen Spielern, sondern von künstlichen Intelligenzkonstrukten (AI) erlangen. Virtuelle Welten haben ihre eigene Geographie und ihre Suche ähnelt daher einer Suche in der wirklichen Welt. Um die Richtung zu finden, helfen häufig virtuelle *non-player Charaktere* (NPC). Diese NPC werden vom Spielentwickler programmiert und vom Plattformbesitzer zur Verfügung gestellt. NPC haben eine Vielzahl von Aufgaben und Rollen, die sie in dem Spiel übernehmen können, als Gegner oder Verbündete von wirklichen Spielern, als Teil der Umwelt oder auch in einem gewissen Rahmen als Schiedsrichter, die z.B. Spieler abmahnen, wenn diese Regelverstöße begehen.[57] Sie sammeln aber auch Daten über Spieler und geben diese auf Anfrage an dritte Personen weiter, wenn dies für das Spiel notwendig ist. So kann etwa ein NPC einem Spieler erst als Verbündeter beistehen, ihn dann aber auch an Feinde «verraten». Wie ein solches «Verhör» eines NPC durch einen Polizisten oder Geheimdienstler rechtlich einzustufen ist, ist unklar. Technisch betrachtet handelt es sich um eine Datenbankabfrage, aber die Art wie diese graphisch repräsentiert wird, bringt sie näher an ein Verhör. Handelt es sich um eine Datenbankabfrage, so stellt sich die Frage, ob die Täuschungshandlungen der Beamten «hacking» darstellen. Subjektiv mag dies nicht so aussehen – der Beamte tippt eine Frage ein («Wo ist Ork Grul, wir brauchen ihn für einen Angriff auf die Burg?») und erhält eine Antwort («Er ist in der Taverne»). Doch diese natürlich-sprachliche Interaktion verschleiert die zugrundeliegende Logik: Aus der Sicht des Computers erhält er einen symbolischen Input und produziert nach strikten Regeln einen Output, dies ist nicht anders als z.B. ein Einloggen mit einem Passwort. Wenn es daher eine Manipulation der Integrität eines Informationssystems ist, ohne Autorität eine Passwortaufforderung zu umgehen, so kann man argumentieren, dass es genauso eine Manipulation ist, eine Reaktion eines NPC unter Vorspielung eines falschen Sachverhalts zu erzwingen. In beiden Fällen wird der Computer dazu gebracht, anders als vom Programmierer geplant zu reagieren.

[57] Zu Non-Player-Charakteren siehe z.B. Brian Mac Namee, P. Cunningham(2001), «Proposal for an Agent Architecture for Proactive Persistent Non-Player Characters» in D. O'Donoghue (ed.) Proceedings of the 12th Irish Conference on AI and Cognitive Science (Dublin: Trinity College Dublin, Department of Computer Science, TCD-CS-2001-20) 221–232; zu ihrer Verwendung als Schiedsrichter siehe G. Sukthankar/K. Sycara(2007), «Policy Recognition for Multi-Player Tactical Scenarios» *Proceedings of the 6th International Joint Conference on Autonomous Agents and Multiagent Systems*(AAMAS 2007), ACM, New York, 1–8.

4 Zusammenfassung und Ausblick

[Rz 34] Der Mensch ist Homo Faber und Homo Ludens, Schöpfer und Spieler. In virtuellen Welten werden beide Bestimmungen eins, hier wird er zum Schöpfer seiner eigenen Welten, zum Zwecke des Spiels. In diesen Welten wird er aber auch Schöpfer seines (digitalen) Selbst, der ultimative «self-made man». Nicht was der genetische Zufall uns zugeteilt hat, bestimmt dort unsere Eigenschaften, sondern was wir frei für uns wählen. Für Hannah Arendt insbesondere ist Homo Faber zu unterscheiden vom «Animal Laborans» dem «arbeitenden Tier».[58] Als Animal Laborans reduziert sich unser Dasein auf das Arbeiten zur Existenzsicherung und unsere Produkte auf ihren praktischen Nutzen zu diesem Endzweck. Für Homo Faber jedoch ist das menschliche Werk als für sich stehend wertvoll. Die gleiche phänomenologische Unterscheidung finden wir oft in den Selbstbeschreibungen von Partizipierenden in Online-Rollenspielen. Das profane Alltagsleben ist nur von instrumentellem Nutzen, das wirkliche Leben findet im Spiel statt, wo unsere Schöpfungen, und dies schließt unseren Avatar ein, Wert in sich selbst erhalten.[59] Stärker noch finden wir diese Divergenz in der Unterscheidung zwischen dem Viator Mundi, dem Mensch als einem Reisenden durch die Welt, in der er nie ganz heimisch wird, und dem Faber Mundi als einem Schöpfer und damit Beherrscher der Welt. Ideengeschichtlich wird dabei der erstere mit dem Mittelalter, Faber Mundi dagegen mit dem Selbstverständnis der Neuzeit identifiziert.[60] Im virtuellen Raum vervollkommnet sich diese Entwicklung, werden hier doch Welten nun wirklich neu geschaffen und nicht nur wie in der Vergangenheit unter den Zwängen und Einschränkungen physikalischer Gesetze modifiziert.

[Rz 35] Vor Arendt, und ohne den Term «Homo Faber», aber in gezielter Abgrenzung gegen die Mechanisierung der Lebensabläufe, die die industrielle Revolution brachte, betonte Friedrich Schiller in seinen Briefen «Über die ästhetische Erziehung des Menschen» die Bedeutung des Spielens. Zumindest für ihn stehen sich Homo Ludens und Homo Faber unvereinbar gegenüber. «Nur im Spiel», so Schiller, «ist die Ganzheitlichkeit der menschlichen Fähigkeiten zu realisieren». Wir erinnern uns in diesem Zusammenhang, dass das deutsche BVerfG gerade die Erfassung des Menschen in seiner Ganzheitlichkeit als die große Gefahr der Online-Überwachung hervorgehoben hatte. Wenn wir der Schiller'schen Analyse folgen, so können wir der Überwachung von Online-Spielen ein besonders großes Gefahrepotential zuschreiben. Zu einer ähnlichen Analyse kommnt Herbert Marcuse. In «Der eindimensionale Mensch» betont er die Bedeutung des Spiels als Gegengewicht zur Vorherrschaft der «instrumentellen Vernunft», die für Industriegesellschaften charakteristisch ist. Diese lasse keinen Platz mehr für Ganzheit, Persönlichkeitsentfaltung und autonome Selbstwerdung – demokratische Werte, die gerade auch durch permanente Überwachung gefährdet sind.

[Rz 36] So argumentierte etwa Bloustein, dass:

> «*[t]he man who is compelled to live every minute of his life among others and whose every need,*

---

58 Hanna Arendt(1958), *The Human Condition*(Chicago: University of Chicago Press); siehe dazu auch Martin Levin(1979), «On Animal Laborans and Homo Politicus in Hannah Arendt A Note». *Political theory*7.4: 521–531.

59 Nick Yee(2006), «The psychology of massively multi-user online role-playing games: Motivations, emotional investment, relationships and problematic usage». *Avatars at work and play*. Springer Netherlands, 187–207.

60 Siehe etwa Michael Ruoff(2002), *Schnee von morgen: das Neue in der Technik*. Königshausen & Neumann. Zum Begriff des Viator Mundi siehe E. Hockstetter (1950),«Viator Mundi. Einige Bemerkungenzur Situation des Menschen bei Wilhelm von Ockham», Franziskanische Studien32: 1–20; für eine Analyse aus der Perspektive der Kommunikationstechnologie siehe C.K. Oberholzer(1975), «Man and his Communication Techniques-A philosophical treatise». *Communicatio*1.1: 1–6.

thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man».[61]

[Rz 37] Ähnlich argumentiert Simitis, dass der Konflikt zwischen den «demokratischen Rechten» auf Redefreiheit und Transparenz mit dem Schutz der Privatsphäre oft auf einem Missverständnis beruht und dass ganz im Gegenteil auch die Privatsphäre eine wichtige Rolle darin spielt, Teilnahme am öffentlichen Leben zu erleichtern. In der Tat zeigt die Erfahrung mit totalitären Systemen, dass die systematische Verletzung der Privatsphäre oft zu einer «Gesellschaft der Mitläufer» führen kann.[62]

[Rz 38] Die gegenseitige Abhängigkeit zwischen Schutz der Privatsphäre und Schutz anderer zentraler Charakteristiken der offenen, pluralistischen Demokratie wird auch von Charles Raab hervorgehoben, der argumentiert, dass Werte wie persönliche Autonomie, Privatsphäre und informationelle Selbstbestimmung «*are important not primarily because individuals may wish to live in isolation (for they do not, mostly), but so that they can participate in social and political relationships at various levels of scale, and so that they can undertake projects and pursue their own goals*».[63]

[Rz 39] Wenn nun der einzige Ort in der industriellen Gesellschaft, in der Autonomie und Gesamtentfaltung der Persönlichkeit noch möglich sind, im Spiel ist, und andererseits staatliche Überwachung eine Gefahr für diese Werte darstellt, so müssen wir schließen, dass die Überwachung von Spielen in der Tat eine potentiell besonders schwere Verletzung von Bürgerrechten in der demokratischen Gesellschaft sein kann.

[Rz 40] Das Konzept des «Homo Ludens» ist vor allem durch Johan Huizinga bekannt geworden.[64] Dieser versuchte zu zeigen, dass sich unsere kulturellen Systeme wie Politik, Wissenschaft, Religion und insbesondere auch das Recht ursprünglich aus spielerischen Verhaltensweisen durch Selbstorganisation entwickelten. Aus Spiel wird «heiliger Ernst», wenn es sich über Ritualisierungen institutionell verfestigt. Sobald sich die Regeln einge-«spielt» haben, sind sie nicht mehr ohne weiteres zu ändern, nehmen nun Zwangscharakter an. In Online-Welten finden wir, dass zwar einerseits Freiräume geschaffen werden, in denen alte Zwänge in Frage gestellt werden können. Andererseits zeigen aber empirische Studien, dass sich normative Regeln aus der physischen Welt subtil wieder Raum schaffen.[65]

[Rz 41] Letztlich sind sowohl Homo Ludens als auch Homo Faber durch den Spielbegriff definierbar. Für Warwitz und Rudolf etwa sind Homo Ludens und Homo Faber zwei unterschiedliche Formen der Weltaneignung im Spiel.[66] Homo Ludens findet im selbstgenügsamen, zweckfreien Spiel trotz oder gerader wegen seiner Zufälligkeit und seinen nicht-essentiellen Möglichkeiten

---

61 E.J. Bloustein(1964), Privacy as an aspect of human dignity: An answer to Dean Prosser, NYUL Rev. 39: 962.

62 S. Simitis(1987), Reviewing Privacy in an Information Society, University of Pennsylvania Law Review, 135: 707–746.

63 C. Raab(2012), Privacy, Social Values and the Public Interest, Politische Vierteljahresschrift 46: 129–152.

64 Johan Huizinga(1949), *Homo ludens*. Taylor & Francis; siehe auch Roger Caillois (2001), *Man, play, and games*. University of Illinois Press.

65 Nick Yee et al. (2007),«The unbearable likeness of being digital: The persistence of nonverbal social norms in online virtual environments». *CyberPsychology & Behavior*10.1: 115–121.

66 Siegbert A. Warwitz/Anita Rudolf(2014), *Der Mensch braucht das Spielen*. In: Dies.: *Vom Sinn des Spielens. Reflexionen und Spielideen*. Baltmannsweiler. 3. Auflage.

Sinn. Der Prozess der Sinngebung führt aber auch als Nebenprodukt zur Welterkenntnis. Homo Faber hingegen betont Lernen durch das zweckgerichtete, strategische Spielen und gewinnt so Welterkenntnis. Er instrumentalisiert somit das Spiel gezielt als Lernspiel. In virtuellen Online-Rollenspielen finden wir beide Ausprägungen des Spieltypus. Zum einen gibt es Spiele, die das Zufallselement von traditionellen «Bleistift und Papier» Rollenspielen wie *Dungeons and Dragons* übernehmen und in virtuellen Welten umsetzen.[67] Strategie ist wichtig, doch eröffnet der Zufall einen Platz für das Unvorhergesehene und Unplanbare. Das Ziel ist in erster Linie hedonistisch,[68] und doch ist der «Nebeneffekt» der Sinngebung und Welterkenntnis relevant auch für Homo Politikus und den Mensch als politisches und soziales Wesen. Insbesondere können sozial und politisch wichtige Eigenschaften erworben werden, wie auch die Fähigkeit zum politischen Widerstand.[69]Auch hier zeigt sich die Gefahr, wenn Spielwelten der staatlichen Überwachung ohne zureichenden Rechtsschutz preisgegeben werden. Auf der anderen Seite findet sich auch der Typus des «Homo Faber beim Spiel», mit mehreren Studien, die das Potential von virtuellen Online-Rollenspielen für strukturiertes Lernen hervorheben.[70] In virtuellen Online-Spielen kommen somit Homo Faber und Homo Ludens zusammen, sie sind nicht nur ein nebensächlicher Zeitvertreib, sondern können für unser Selbstverständnis und unsere Identitäten konstitutive Funktionen übernehmen.

[Rz 42] Die Bedeutung des Spiels für das Entstehen des Rechts als soziales Phänomen wurde von Huizinga betont. Eine andere, normativ-anthropologische Verbindung zwischen Recht und Spiel findet sich im einflussreichen Versuch einer Neubegründung des Naturrechts durch John Finnis. In dessen *Natural law and Natural Rights* ist «Spielen» als einer der kulturübergreifenden menschlichen Werte aufgelistet, denen letztendlich alle gerechten Gesetzte dienen müssen.[71]

[Rz 43] Dass britische und amerikanische Geheimdienste in großem Maße Online-Spiele überwachen, mag am Anfang wie eine schlechte Parodie klingen, zu evokativ ist das mentale Bild des Möchtegern James Bond, dessen einzige Chance auf «Aktion» es ist, in World of Warcraft als Elf feindliche Orks zu überwachen. Vor dem Hintergrund der Enthüllungen über PRISM und TEMPORA erscheint es schlimmstenfalls als eine Verschwendung von Steuergeldern, nichts mehr als eine amüsante Fußnote zum Skandal. Wir haben zu zeigen versucht, dass dies ein gefährliches Missverständnis wäre. Überwachung von Spielwelten ist potentiell einer der schwerwiegendsten Angriffe auf den Privatheitsschutz, der denkbar ist. Wie wir zu zeigen versucht haben, erlaubt die Überwachung von Online-Spielen nicht nur empirisch verlässliche Rückschlüsse auf die «reale» Person des Spielers, ihre physischen, emotionalen und sexuellen Charakteristika, es erfasst zudem ihre Träume, Wünsche und Hoffnungen, nicht nur wer oder was wir sind, sondern auch was wir gerne sein würden. Sie stellt damit einen Schritt zur Gesamterfassung einer Person dar, eine

---

67 Joris Dormans(2006), «On the Role of the Die: A brief ludologic study of pen-and-paper roleplaying games and their rules». *Game Studies*6.1.

68 Jiming Wu/Clyde Holsapple(2014), «Imaginal and emotional experiences in pleasure-oriented IT usage: A hedonic consumption perspective». *Information & Management*51.1: 80–92.

69 So Katherine Angel Cross(2013), «The New Laboratory of Dreams: Role-playing Games as Resistance». *WSQ: Women's Studies Quarterly*40.3: 70–88.

70 So etwa Rodney P. Riegle/W.A. Matejka(2006), «The learning guild: MMORPGs as educational environments». *Annual Conference on Distance Teaching & Learning*; Marcus D. Childress/Ray Braswell(2006), «Using massively multiplayer online roleplaying games for online learning». *Distance Education*27.2: 187–196.

71 John Finnis*c*Oxford University Press, 2011, S. 87 ff; Für eine Anwendung dieser Gedanken zur Technologieregulierung siehe R. Black(2002), «Ethics and the Products of Science», in R.E. Spier (ed.) *Science and Technology Ethics*(London: Routledge) 39–59.

Möglichkeit die sowohl für Großbritannien, aber auch für Deutschland eines erheblich strikteren Rechtsrahmens bedarf, als dies zur Zeit der Fall ist.

Wiebke Abel, Postdoctoral Research Fellow SCRIPT Centre, School of Law, The University of Edinburgh, Old College Edinburgh EH8 9YL wabel@staffmail.ed.ac.uk
Burkhard Schafer, Professor for Computational Legal Theory, Director SCRIPT Centre School of Law, The University of Edinburgh, Old College Edinburgh EH8 9YL b.schafer@ed.ac.uk