



# HESSISCHER LANDTAG

04. 02. 2015

## **Antwort der Landesregierung**

**auf die Große Anfrage der Löber, Gremmels, Siebel, Lotz, Müller (Schwalmstadt),  
Schmitt, Warnecke (SPD) und Fraktion**

**betreffend Verbraucherinnen und Verbraucher im Netz schützen - Freiheit des  
Internets mit Datenschutz sichern!**

**Drucksache 19/413**

### **Vorbemerkung der Fragesteller:**

Der digitale Wandel verändert unsere Gesellschaft nachhaltig. Das Internet ist heute ein gesamtgesellschaftlicher Kreativ-, Wirtschafts- und Sozialraum. Dieser Prozess hat Auswirkungen auf alle Lebensbereiche und bietet große Chancen.

Andererseits gibt es auch Bereiche, in denen sich im Netz Risiken für die Verbraucherinnen und Verbraucher ergeben. In diesen Feldern besteht ein Schutzanspruch und Schutzauftrag gegenüber den Nutzerinnen und Nutzern.

Viele Verbraucherinnen und Verbraucher nutzen vermehrt Angebote des E-Commerce, Online-Shopping gehört fest zum Alltag. Gerade hier häufen sich aber auch die Probleme, denn Verbraucherinnen und Verbraucher sind sich oft der möglichen Risiken des E-Commerce nicht bewusst. Auch im Bereich des Urheberrechts kommt es immer wieder zu unbewussten und ungewollten Verstößen durch das Herunterladen unzulässiger Inhalte.

Verbraucherschutz gelingt nicht allein durch Regulierung, sondern durch ein hohes Maß an Transparenz und Aufklärung. Diese Grundsätze gelten gleichermaßen für den Verbraucherschutz im Internet. Dazu tritt im digitalen Rahmen die frühe und nachhaltige Vermittlung von Medien- und Datenschutzkompetenz in den Mittelpunkt. Nur wenn diese Elemente angemessen verzahnt ineinandergreifen, können Verbraucherinnen und Verbraucher im Internet besser geschützt werden und zugleich die Freiheit des Internets als wesentlichen Bestandteil der Demokratie im Zeitalter der Digitalisierung erhalten werden.

### **Verbraucherschutz und Verbraucherinformation**

Über das Netz Einkäufe zu tätigen, an Versteigerungen teilzunehmen etc., hat in den vergangenen Jahren rasant zugenommen. Nach einer Studie des Handelsverbands Deutschland wurden im Jahr 2011 in Deutschland 26,1 Mrd. € im E-Commerce umgesetzt. Die Tendenz ist weiter steigend: Die zitierte Studie prognostizierte für 2012 ein Volumen von 29,5 Mrd. €. Die Gesellschaft für Konsumforschung stellte fest, dass im Jahr 2010 in Deutschland 38,1 Millionen Menschen Angebote zum Online-Shopping genutzt haben, 2011 bereits 41 Millionen.

So wie es offline Fälle von Betrug und Täuschung von Verbraucherinnen und Verbrauchern gibt, so bestehen auch online Risiken. Zu den gesellschaftlich am stärksten diskutierten Beispielen gehören sog. Abo-Fallen. Verbraucherinnen und Verbraucher schließen hierbei ohne eigenes Wissen langfristige Abonnements ab, die teils erheblichen Kostenaufwand mit sich bringen.

Auch im Internet treten Fälle von Betrugsriminalität auf. Phänomene wie Phishing und Identitätsdiebstahl richten gerade bei Privatpersonen finanzielle Schäden an und untergraben das Vertrauen in das Netz als Wirtschaftsraum. Dieser Vertrauensverlust ist letztlich nicht nur für Unternehmen, sondern auch für Verbraucherinnen und Verbraucher von Nachteil. Diese verzichten vor diesem Hintergrund gegebenenfalls auf Vorteile wie beispielsweise ein breites Angebot oder direkte und einfache Vergleichsmöglichkeiten, wenn ihre Sicherheit nicht gewährleistet ist.

Eine Regulierung muss dabei immer die große technische Wandlungsfähigkeit des Internets berücksichtigen. So ist etwa der Trend zur mobilen Internetnutzung eine zentrale Herausforderung. Hiermit verbunden sind u.a. veränderte Anforderungen an Regelungen zur Verbraucherinformation und Transparenz, die sich aus der Nutzung anderer und besonders kleinerer Endgeräte ergeben.

### **Verbraucherrechte**

Die digitale Teilhabe ist heute ein wichtiges Verbraucherrecht. Teilhabe am Internet setzt eine gut ausgebaut, funktionsfähige und den Wachstumsperspektiven des Internets angemessene technische Infrastruktur voraus. Dies gilt insbesondere für den Ausbau des Breitband-Internets. Wichtig sind jedoch auch der diskriminierungsfreie Zugang zum Netz sowie die Absicherung der Netzneutralität.

Die Chancen der Digitalisierung gilt es vor diesem Hintergrund auch für die unabhängige Verbraucherinformation zu nutzen. Das Internet bietet die Möglichkeit für eine sehr zügige, umfangreiche sowie neuen Entwicklungen schnell anpassbare Information der Verbraucherinnen und Verbraucher.

### **Altersgruppenspezifische Fragestellungen**

Betrachtet man die aktive Teilhabe von Nutzerinnen und Nutzern am Internet, so wird deutlich, dass besonders Kinder und Jugendliche ein großes Interesse daran haben, sich über digitale Medien auszutauschen und im Internet über soziale Netzwerke oder Online-Spiele Kontakt zu ähnlich Gesinnten oder Freundinnen und Freunden zu knüpfen. Internetnutzung macht, wie es insbesondere die KIM- und die JIM-Studie zeigen, nicht einsam, sondern erweitert im Gegenteil das Kommunikationsverhalten junger Menschen.

Aus diesen Gründen ist die Gruppe der Kinder und Jugendlichen - in den zitierten Studien werden als Kinder die 6- bis 12-Jährigen und als Jugendliche die 12- bis 19-Jährigen verstanden - besonders zu betrachten und auf ihre Bedürfnisse einzugehen. Diese Altersgruppen für Kinder und Jugendliche sollen auch bei den unten stehenden Fragen zugrunde gelegt werden (abweichend von der juristischen Definition). Die Vermittlung von Medienkompetenz in Bildungseinrichtungen hat hierbei eine zentrale Bedeutung. In verschiedenen Bereichen, wie Datenschutz oder E-Commerce, bedarf es der Regulierung. Die Besonderheiten des Surfverhaltens junger Menschen und die spezifischen Chancen und Risiken sollten bei Maßnahmen berücksichtigt werden.

Neben den Kindern und Jugendlichen müssen auch die älteren Internetnutzerinnen und Internetnutzer stärker in den Fokus gerückt werden. Gerade bei ihnen zeigt sich, dass Unklarheiten über die Möglichkeiten und Sicherheit von Internetangeboten immer noch ein Hinderungsgrund für die Partizipation am Internet ist. Der sich hieraus ergebende "Digital Divide" stellt in der vernetzten Gesellschaft eine große Herausforderung dar. Dennoch sind die Entwicklungen in dieser Altersgruppe bemerkenswert.

Dieser gesamtgesellschaftlich zu begrüßende Prozess der Internetnutzung sollte durch ein angemessenes Verbraucherschutzrecht, das die Interessen und besonderen Anforderungen verschiedener Altersgruppen berücksichtigt, unterstützt werden. Neben einem angemessenen Maß der Regulierung sollten die konsequente Aufklärung über Chancen und Risiken sowie eine altersgruppengerechte Medienkompetenzförderung eine wichtige Rolle spielen.

#### **Digitale Gewalt**

Eine rasante Entwicklung erfährt auch die Zunahme der digitalen Gewalt. Hier ist es besonders wichtig, sich der Gefahren bewusst zu sein und sich vor digitaler Gewalt zu schützen. Unterschiedliche Formen und Stärke von digitaler Gewalt sind hierbei zu unterscheiden. Digitale Gewalt reicht von Filmen von Vergewaltigung, Nötigung oder Körperverletzung über das Veröffentlichlichen von Bildern und Videos oder die Drohung mit der Veröffentlichung. Aber auch Diffamierung, Nachstellung, Bedrohung, Ausspionieren und Ortung sind digitale Gewalt. Bei vielen Fällen von digitaler Gewalt ist den Opfern, aber auch den Täterinnen und Tätern, nicht bekannt, dass es sich um Straftatbestände handelt. Ursachen für die Zunahme sind vielfältig. Handys mit Kamera sind ständig verfügbar. Ein Problem ist auch die Anonymität des Internets. Dadurch sind Verhaltensmuster möglich, für die man nicht herangezogen werden kann.

#### **Datenschutz**

An den Schutz persönlicher Daten stellen die Verbraucherinnen und Verbraucher im digitalen Zeitalter ebenfalls hohe Ansprüche. Nicht allein die in diesem Zusammenhang oftmals für mangelhaften Datenschutz kritisierten sozialen Netzwerke sammeln Daten, erstellen hieraus Profile oder nutzen diese zu Werbezwecken. Ebenso sammeln Anbieter von Online-Shopping, Webmail-Diensten oder Online-Spielen persönliche Daten. Auch die mobile Internetnutzung bringt Veränderungen und Herausforderungen an den Datenschutz mit sich. Die Weitergabe persönlicher Daten geschieht nicht immer im Rahmen des deutschen Datenschutzrechts.

Daher kommt auch mit Blick auf den Datenschutz der Aufklärung der Nutzerinnen und Nutzer sowie der Vermittlung von Medien- und Datenschutzkompetenz große Bedeutung zu. Die Nutzerinnen und Nutzer müssen besser aufgeklärt werden, um die Weitergabe ihrer persönlichen Daten selbst steuern zu können und zu vermeiden, dass diese ohne ihre bewusste Entscheidung an Dritte weitergegeben werden. In diesem Zusammenhang kommt dem Hessischen Datenschutzbeauftragten eine wichtige Rolle zu.

#### **Medienkompetenz**

Die Förderung der Medienkompetenz der Verbraucherinnen und Verbraucher im Internet ist die Grundlage für ein bewusstes und überlegtes Handeln in allen Bereichen. Wer sich nicht auskennt, kann sich auch nicht über mögliche Gefahren oder Unwägbarkeiten bewusst sein.

Ein nachhaltiger und umfassender Informationsansatz sollte ein grundlegender Baustein für die Nutzerinnen und Nutzern im Umgang mit dem Internet sein, denn nur durch wachsende Medienkompetenz kann jede Internetnutzerin und jeder Internetnutzer die Vorteile und Möglichkeiten des Internets sorglos ausschöpfen. Hierbei kann ein Ansatz sein, frühestmöglich den Aspekt der Medienkompetenz in Bildungseinrichtungen zu integrieren und somit die Gefährdung insbesondere von Kindern und Jugendlichen zu verringern. Gleichzeitig sollten generationsübergreifend die Erwachsenen nicht aus dem Fokus gelassen werden, deren Medienkompetenz oftmals unter der der im digitalen Zeitalter aufgewachsenen jüngeren Generation liegt.

#### **Vorbemerkung der Ministerin für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz:**

Kaum ein anderer Bereich ist in den vergangenen Jahren solch rasanten Entwicklungen unterworfen wie die Informationstechnik und in kaum einem anderen Bereich stehen Fragen nach Vertrauenswürdigkeit und Seriosität so im Vordergrund wie im Umgang mit dem Internet. Fairer Zugang zu Daten und Geschäften, Schutz vor Belästigungen und Betrügereien und ein ausgewogenes Verhältnis bei der Anwendung von Urheberrechten sind Kernziele, die wir in den kommenden Jahren gewährleisten müssen. Vertrauen und Sicherheit im Netz zu schaffen und den Nutzen des Internets auszuschöpfen, ohne den Datenschutz und die Rechte der Verbraucherinnen und Verbraucher auf Transparenz zu vernachlässigen, und einen aktiven, informierten Umgang mit ihren Daten im Blick zu behalten - diese Balance gilt es sicherzustellen.

Das Internet und seine immer stärkere Nutzung im privaten, öffentlichen und wirtschaftlichen Bereich verändern unsere Gesellschaft nachhaltig. Das Netz ist das freiheitlichste und effizienteste Informations- und Kommunikationsforum der Welt und bietet vielfältige Möglichkeiten, wie beispielsweise den weltweiten Einkauf von Waren und Dienstleistungen und die Kommunikation über soziale Netzwerke, Foren und Chatrooms. Die neue Freiheit birgt aber auch immer Gefahren und Risiken.

Im neuen Verbraucherschutzkonzept der Hessischen Landesregierung, das mit einer Steigerung um ein Drittel auf 2,2 Mio. € eine deutlich verbesserte Finanzierung der Verbraucherzentrale Hessen und des DHB - Netzwerk Haushalt vorsieht, haben wir festgelegt, dass in der Verbraucherberatung ein stärkerer Fokus auf Themen der digitalen Welt gelegt wird.

Mit der Beantwortung dieser Großen Anfrage besteht die Möglichkeit, die zahlreichen Dimensionen des Themenfeldes "Verbraucherschutz im Internet" zu beleuchten. Dabei wird ein umfassendes Verständnis von Verbraucherschutz zugrunde gelegt, das neben regulativen Maßnahmen stets auch die Verbraucheraufklärung und unabhängige Information umfasst. Ebenso wichtig erscheint der Aspekt, dass gerade durch die weltweite Nutzung des Internets auch der nationale und insbesondere der internationale Rechtsrahmen berührt sind.

Soweit in der Vorbemerkung der Fragesteller und auch bei den nachfolgenden Fragestellungen auf strafrechtliche Erscheinungsformen der Internetkriminalität Bezug genommen wird, ist eine Differenzierung erforderlich. So umfasst zum einen die Internetkriminalität im engeren Sinne all diejenigen Straftaten, durch die das Internet einschließlich der angebotenen Dienste Angriffen ausgesetzt werden oder bei denen das Internet genutzt wird, um Angriffe auf die Sicherheit, Zuverlässigkeit und Integrität von Daten auszuführen. Diese Angriffe erfüllen im Wesentlichen speziell normierte Tatbestände. Hierzu zählen insbesondere das Ausspähen von Daten (§ 202 a StGB), die Datenveränderung (§ 303 a StGB) sowie die Computersabotage (§ 303 b StGB).

Zum anderen gehören zur Internetkriminalität im weiteren Sinne aber auch sonstige allgemeine Straftaten, bei denen das Tatmittel Internet eingesetzt wird. Gerade bei den allgemeinen Straftaten haben sich verschiedene Schwerpunktbereiche gebildet, nämlich z.B. Ebay-Betrugsverfahren, Online-Banking-Datenmissbrauch, Kostenfallen im Internet, Cybermobbing und Tauschbörsen für Kinderpornographie. Die dynamische Entwicklung immer neuer Kriminalitätsformen und die stetig steigende Bedeutung des Internets als Tatmittel sind dabei die besonderen Herausforderungen bei der Bekämpfung der Internetkriminalität.

Statistische Daten zur Anzahl von Ermittlungsverfahren im Bereich der Internetkriminalität im weiteren Sinne stehen nicht zur Verfügung. Denn die statistische Erfassung erfolgt jeweils für die im Strafgesetzbuch normierten Straftatbestände. Die Verwendung des Tatmittels, hier des Internets, wird bei den Allgemeindelikten hingegen nicht gesondert erfasst bzw. ausgewertet. Es dürfte angesichts der zunehmenden Nutzung des Internets aber zu vermuten sein, dass die Anzahl von Allgemeindelikten mit Internetbezug mittlerweile deutlich höher ist als die Zahl computerspezifischer Delikte.

Soweit in der Großen Anfrage im Übrigen der Begriff der "digitalen Gewalt" verwendet wird, handelt es sich nicht um einen fest definierten Rechtsbegriff. Auch ist eine Definition dieses Begriffes in der Großen Anfrage selbst nicht ersichtlich. In der Vorbemerkung der Fragesteller wird dazu lediglich beispielhaft aufgezählt, welche Delikte unter anderem unter den Begriff der "digitalen Gewalt" fallen können. Dies führt zu der Schwierigkeit, dass gerade im strafrechtlichen Bereich unabhängig von der oben angesprochenen Problematik bei der Internetkriminalität im weiteren Sinne die Fragen nach den statistischen Daten nicht beantwortet werden können. Denn die in der Vorbemerkung der Fragesteller beispielhaft aufgezählten Straftaten zählen zu ganz unterschiedlichen Deliktsfeldern, zu deren Schnittmenge valides Zahlenmaterial nicht zusammengestellt werden kann.

Diese Vorbemerkungen vorangestellt, beantwortet die Ministerin für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz die Große Anfrage im Einvernehmen mit der Staatskanzlei, mit dem Minister des Innern und für Sport, mit der Ministerin der Justiz, mit dem Kultusminister, mit dem Minister für Wissenschaft und Kunst, mit dem Minister für Wirtschaft, Energie, Verkehr und Landesentwicklung, mit dem Minister für Soziales und Integration und nach Rücksprache mit dem Hessischen Datenschutzbeauftragten im Namen der Landesregierung wie folgt:

### **Stellenwert und Bedeutung, grundlegende Herausforderungen**

Frage 1. Welchen Stellenwert nimmt die Verbraucherschutzpolitik innerhalb der Netzpolitik der Landesregierung ein?

Das Internet hat sich zu einem unverzichtbaren und festen Bestandteil des Lebensalltags aller gesellschaftlichen Gruppen entwickelt. Die Nutzerinnen und Nutzer sind die wesentlichen Akteure des Internets. Der auf das Internet bezogene Verbraucherschutz ist daher ein wichtiges netzpolitisches Themenfeld, dessen Rolle und Umfang, seine Akteure, die Ausgestaltung künftiger Internetentwicklung mit ihren Chancen wie Risiken sowie die zukünftigen Anforderungen an die Rechtsordnung in Zukunft weiter zu klären sein wird.

Die Landesregierung hat die Relevanz des Themas erkannt. Es ist das Ziel der Landesregierung, die Möglichkeiten des Internets in allen Lebensbereichen bestmöglich nutzbar zu machen und die moderne Informations- und Kommunikationsgesellschaft sowie den Wirtschaftsstandort Hessen weiter zu entwickeln und verbraucherfreundliche Rahmenbedingungen im Internet voranzutreiben. Aufklärung und Transparenz spielen hier ebenso eine wichtige Rolle wie der Schutz der Verbraucherinnen und Verbraucher.

Die Landesregierung misst der Verbraucherschutzpolitik innerhalb ihrer Netzpolitik einen hohen Stellenwert bei. Die Netzpolitik selbst ist als Querschnittsaufgabe beim Hessischen Ministerium des Innern und für Sport verortet. Der digitale Wandel der letzten Jahre stellt die Politik vor neue Herausforderungen beim Verbraucherschutz. Die enormen Chancen, die das Internet und die mobilen Anwendungen bieten, bergen gleichzeitig auch Risiken - vor allem im Bereich des Datenschutzes. Im Hinblick auf die Verbraucherschutzpolitik im Internet bestimmt der Koalitionsvertrag der die Regierungskoalition tragenden Parteien für die 19. Wahlperiode des Hessischen Landtags die folgenden grundlegenden Handlungsschwerpunkte. So setzt sich die Landesregierung bei der Nutzung personenbezogener Daten, insbesondere auch im Internet, für einen Einwilligungsvorbehalt und für praxisgerechte Widerspruchsrechte sowie Löschungsmöglichkeiten für die Verbraucherinnen und Verbraucher ein. Die Landesregierung wird eine Bundesratsinitiative einbringen, um bei Sozialen Netzwerken die höchste Sicherheitseinstellung voreinzustellen, die nur vom Nutzer individuell gelockert werden kann. Außerdem will die Landesregierung die Informationen über Digitales sowie die Regulierung von digitalem Fingerprinting verbessern. Ein bewusster und kompetenter Umgang mit Medien ist eine Schlüsselqualifikation. Daher wird die Landesregierung ihr Engagement bei der Aufklärung von Chancen und Risiken im Umgang mit neuen und digitalen Medien intensivieren und Kriminalität im Internet entschieden begegnen.

Frage 2. Welche grundlegenden Handlungsschwerpunkte sieht die Landesregierung im Bereich der Verbraucherschutzpolitik im Internet?

Für die Landesregierung besteht die grundlegende Herausforderung der Verbraucherschutzpolitik darin, Risiken aus den sich ständig neu entwickelnden und erweiternden Nutzungsmöglichkeiten des Internets für Verbraucherinnen und Verbraucher zu begegnen. Die Verbraucherin oder der Verbraucher ist heute mit immer komplexer werdenden Konsumentenscheidungen konfrontiert und bei der alltäglichen Nutzung des Internets auch durch vielfältige Fallstricke gefährdet, angefangen von unseriösen Gewinnmitteilungen und Lockvogelangeboten über Abzockmethoden bis hin zum Datenmissbrauch. Ein fairer Zugang zu Daten und Geschäften, Schutz vor Belästigungen und Betrügereien, ein diskriminierungsfreier Zugang zum Internet und der Schutz vor missbräuchlichen Abmahnungen von Verbraucherinnen und Verbrauchern wegen Urheberrechtsverletzungen sind Handlungsschwerpunkte in diesem Politikfeld, um die Stärkung der Rechte der Verbraucherinnen und Verbraucher im Internet voranzutreiben.

Die Landesregierung fördert niedrigschwellige Zugangsmöglichkeiten zum Internet und hat sich eine Steigerung der Medienkompetenz aller Bevölkerungsschichten zum Ziel gesetzt. Beispielsweise gewinnt in diesem Zusammenhang auch der Jugendmedienschutz eine besondere Bedeutung. Über die Einhaltung des Staatsvertrages über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien wacht die Hessische Landesanstalt für privaten Rundfunk und neue Medien. Verstöße gegen die Bestimmungen dieses Staatsvertrages sind entweder strafbewehrt oder sie können als Ordnungswidrigkeit verfolgt werden. Zum Beispiel können Telekommunikationsdiensteanbietern Bußgelder bis zu einer Höhe von 500.000 € auferlegt werden, wenn sie Angebote verbreiten oder zugänglich machen, die geeignet sind, die Entwicklung von Kindern oder Jugendlichen zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit zu beeinträchtigen, ohne dafür Sorge zu tragen, dass Kinder oder Jugendliche der betroffenen Altersstufen sie üblicherweise nicht wahrnehmen.

Auf die Antwort zu Frage 1 wird verwiesen.

Frage 3. Wie bewertet die Landesregierung insgesamt die Organisation des Verbraucherschutzes im Netz innerhalb der föderalen Strukturen der Bundesrepublik Deutschland?

Verbraucherpolitik erfordert klare Gesetze, die einfach und praktikabel in der Anwendung sind. Im deutschen Recht gibt es kein "Verbraucherschutzgesetz", das alle Fragen des Verbraucherrechts regelt. Vielmehr ist Verbraucherpolitik eine Querschnittsaufgabe, die viele Bereiche betrifft und primär auf EU- und Bundesebene gesetzlich geregelt wird. Eine enge Abstimmung zwischen Bund, Ländern und EU ist daher gerade im Bereich Verbraucherpolitik von zentraler Bedeutung.

Die Zuständigkeit für den Verbraucherschutz im Internet ist in der Gesetzgebungszuständigkeit zwischen Bund und Ländern entsprechend der jeweils berührten Sachmaterie geteilt. Landesrechtliche Regelungen sind, zum Teil auch durch staatsvertragliche Vereinbarungen der Länder, beispielsweise in den Bereichen Glücksspiel, Datenschutz oder Jugendmedienschutz geschaffen worden. Zumeist erfolgt die Gesetzgebung im Bereich des Verbraucherschutzes im Internet jedoch durch den Bund, wobei für den Vollzug der Gesetze in aller Regel wiederum die Länder zuständig sind. Soweit der Gesetzesvollzug in die Zuständigkeit der Länder fällt, sorgt die Landesregierung für eine sinnvolle Bündelung der Aufsicht.

Die Landesregierung setzt sich bei der Überwachung verbraucherschützender Vorschriften im Internet dafür ein, dass die Vollzugsbehörden der Länder miteinander kooperieren und dass im Interesse eines effektiven Aufgabenvollzugs Rahmenbedingungen für eine sinnvolle Bündelung

von Aufsichtstätigkeiten geschaffen werden. So wurde im Bereich des gesundheitlichen Verbraucherschutzes Anfang 2011 ein Pilotprojekt zur "Überwachung des Internethandels mit Lebensmitteln" gestartet, das das Bundesamt für Lebensmittelsicherheit (BVL) im Auftrag der Länderarbeitsgemeinschaft Verbraucherschutz (LAV) zunächst zusammen mit 10 Ländern durchgeführt hat. Dieses erfolgreiche Projekt wird seit dem 1. Juli 2013 mit 16 Ländern fortgeführt.

Frage 4. Welche Strukturen und Formen der Koordination zwischen den Ländern gibt es für Fragen des Verbraucherschutzes im Internet?

Im Rahmen der Verbraucherschutzministerkonferenz (VSMK), in der die für Verbraucherschutz zuständigen Ministerinnen und Minister, Senatorinnen und Senatoren der Länder und des Bundes als Mitglieder vertreten sind, koordinieren die Länder ihre Aktivitäten im Bereich des Verbraucherschutzes. 2013 hatte das Hessische Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz den Vorsitz.

Vorbereitet wird die VSMK durch die LAV, der die Abteilungsleiterinnen oder Abteilungsleiter der jeweiligen für den Verbraucherschutz zuständigen Ministerien/ Senatsverwaltungen angehören. Zur Unterstützung der Arbeit sind mehrere Unter-Arbeitsgruppen zu verschiedenen Themenbereichen eingerichtet worden, unter anderen auch eine länderübergreifende Arbeitsgemeinschaft Wirtschaftlicher Verbraucherschutz (AG WV). Im Rahmen dieser Kooperationen werden auch Themen des Verbraucherschutzes im Internet aufgegriffen. Zuletzt hat die LAV durch die AG WV bestehende rechtliche Regelungen im Hinblick auf erforderliche Anpassungsbedarfe an die technischen und tatsächlichen Gegebenheiten mobiler Endgeräte und die verbrauchergerechte Ausgestaltung von Nutzungs- und Datenschutzbedingungen von App-Stores und mobilen Angeboten überprüft. An dieser Projektgruppe war auch Hessen beteiligt. Aktuell beschäftigt sich eine Projektgruppe der AG WV mit dem Thema "Daten- und Verbraucherschutz bei digitalen Rechtemanagement-Systemen gewährleisten" und bearbeitet hier gemeinsam mit Vertretern der Justizministerkonferenz Fragen des Urheberrechts und mögliche Lösungsansätze sowie rechtliche Rahmenbedingung für diesen Sektor.

Das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz setzt sich dafür ein, dass zusammen mit den anderen Ländern über die VSMK auf die Notwendigkeit gesetzlicher Änderungen zur Verbesserung des Verbraucherschutzes im Internet hingewiesen wird und der Bund, zu dessen verfassungsgemäßen Kompetenzen in aller Regel die Gesetzgebung im Bereich des Verbraucherschutzes gehört, zur Schaffung entsprechender Regelungen aufgefordert wird.

Auch durch die Arbeit der verschiedenen Arbeitsgruppen der Länder in den verschiedenen verbraucherschutzrelevanten Feldern vernetzen sich die Länder und erarbeiten in Zusammenarbeit mit dem Bund Lösungsvorschläge für bestimmte Handlungsfelder. Das Pilotprojekt zur "Überwachung des Internethandels mit Lebensmitteln", das das Bundesamt für Lebensmittelsicherheit (BVL) im Auftrag der LAV gestartet hat, zeigt die Effektivität und ist ein Beispiel für eine gelungene Zusammenarbeit.

Frage 5. Wie bewertet die Landesregierung die Effizienz dieser Strukturen?

Auf die Antworten zu den Fragen 3 und 4 wird verwiesen.

Frage 6. Welche Herausforderungen für dieses Politikfeld ergeben sich aus Sicht der Landesregierung auf Ebene der Europäischen Union und wie begegnet die Landesregierung diesen?

Die überwiegende Mehrheit unserer Rechtsvorschriften beruht auf einschlägigen Vorgaben der Europäischen Union. Um die Effizienz des Binnenmarktes zu gewährleisten, ist eine Verbraucherpolitik auf EU-Ebene notwendig. Die Landesregierung hat sich zum Ziel gesetzt, auch zur Gewährleistung eines hohen Verbraucherschutzniveaus und im Interesse der Nutzerinnen und Nutzer des Internets, auf den europäischen Entscheidungs- und Gesetzgebungsprozess so früh wie möglich Einfluss zu nehmen. Dabei setzt sich die Landesregierung insbesondere dafür ein, dass EU-Regulierungen nicht zu einer Absenkung des in Deutschland bereits erreichten Verbraucherschutzniveaus führen. Dies erfolgt insbesondere über das Einbringen von Hessenpositionen in Stellungnahmen des Bundesrates, welche der EU im Vorfeld von Rechtsakten übermittelt werden. Gleichzeitig nutzt die Landesregierung diverse Möglichkeiten zur Einflussnahme und zum Austausch mit der Bundesregierung als auch mit Organen der Europäischen Union, wie insbesondere der Europäischen Kommission sowie den Mitgliedern des Europäischen Parlaments, um für verbraucherfreundliche Regulierungen zu werben. Über die Hessische Landesvertretung in Brüssel werden gegenüber den EU-Institutionen die Interessen des Verbraucherschutzes gewahrt und frühzeitig in den EU-Entscheidungsprozess eingebracht.

In den letzten Jahren sind seitens der Europäischen Union zunehmend Vorstöße zur europäischen Regulierung der Rechte von Verbraucherinnen und Verbrauchern im Internet erfolgt. Diese Initiativen betreffen zum Einen die Rechte von Verbraucherinnen und Verbrauchern beim

Abschluss von Verträgen im Internet (so genannte Button-Lösung) und den Bereich des Datenschutzes. Aktuell im Mittelpunkt steht eine umfassende Überarbeitung und Harmonisierung europäischer Datenschutzstandards mittels des 2012 vorgelegten Entwurfs einer Datenschutz-Grundverordnung, die auch entscheidenden Einfluss auf die Ausgestaltung des Datenschutzes im Internet haben wird. Hessen hat sich dabei bereits in der Vergangenheit für datenschutzfreundliche Voreinstellungen und die Löschung inaktiver Accounts in Sozialen Netzwerken eingesetzt, unter anderem mittels einer Bundesratsinitiative gemeinsam mit Bayern im Frühjahr 2012, im Rahmen des 1. Hessischen Verbrauchertages im Oktober 2012, durch die Veranstaltung anlässlich des EU-Tages der Verbraucherschutzministerkonferenz im März 2013 in Berlin mit EU-Kommissarin Reding sowie durch einen Antrag "Verbraucherrechte in Sozialen Netzwerken stärken" auf der VSMK im Mai 2014.

Auch die Regelung von Netzneutralität ist Gegenstand des Vorschlags einer Verordnung des Europäischen Parlamentes und des Rates über Maßnahmen zum europäischen Binnenmarkt, der elektronischen Kommunikation und zur Verwirklichung des vernetzten Kontinents und zur Änderung der Richtlinien 2002/20/EG, 2002/21/EG und 2002/22/EG und der Verordnungen (EG) Nr. 1211/2009 und (EU) Nr. 531/2012COM (2013) 627final, BR-Drucksache 689/13. Die Landesregierung wird den Prozess weiterhin aktiv begleiten und sich dafür einsetzen, dass die Netzneutralität gewahrt bleibt.

Frage 7. Welche Bedeutung misst die Landesregierung einer Verbesserung des Verbraucherschutzes im Internet bei, um durch die damit verbundene Steigerung der Sicherheit den Herausforderungen zu begegnen, die sich aus dem sogenannten "Digital Divide", also der "Kluft" zwischen Onlinern und Offlinern, ergeben?

Das Internet bietet für Verbraucherinnen und Verbraucher die Möglichkeit, zahlreiche Geschäfte des Alltags wie Wareneinkäufe oder Bankgeschäfte von überall aus abzuwickeln. Darüber hinaus bietet das Internet auch eine wichtige Plattform als Informations- und Kommunikationsmedium. Soziale Netzwerke sind der Dorfmarktplatz früherer Jahrhunderte. Verbraucherinnen und Verbraucher, die keinen Zugang zum Internet haben oder diesen nicht nutzen, sind von einer Inanspruchnahme dieser Angebote ausgeschlossen und teilweise ausgegrenzt, da die Nutzung dieses Mediums im heutigen Leben eine immer wichtigere Rolle spielt.

Die Landesregierung verfolgt das Ziel, möglichst vielen Verbraucherinnen und Verbrauchern in Hessen die Nutzungspotenziale des Internets zu eröffnen und damit die Kluft zwischen Internetnutzerinnen und -nutzern sowie Offlinerinnen und Offlinern zu verringern. Hessen hat deshalb schon 2010 den Aufbau einer leistungsfähigen digitalen Infrastruktur als einen zentralen Schlüsselfaktor für die Zukunftssicherung des Landes erkannt und das Projekt "Mehr Breitband in Hessen" initiiert. Ein Ziel der im Projekt entwickelten NGA-Strategie ist es, Ende 2018 für Hessen eine flächendeckende Versorgung mit schnellem Internet zu erreichen.

Die Versorgung mit einem schnellen Internet soll auf dem Land ebenso gewährleistet sein wie in der Stadt. Es wird eine bedeutende Aufgabe der Landesregierung sein, die Versorgung mit leistungsstarken Breitbandzugängen flächendeckend voranzutreiben. Der physische Zugang zu den Medien ist allerdings nicht mehr als das Hauptproblem des Digital Divides anzusehen. Vielmehr bereitet eine fehlende bzw. geringe Medienkompetenz von Teilen der Bevölkerung der Landesregierung Sorgen. Denn der Bildungshintergrund und die soziale Umgebung scheinen das Nutzungsverhalten zu beeinflussen. Zwar bietet das Internet für bisher benachteiligte Gruppen die Chance, etwa durch gezielte Recherchen, schnell an aktuelle, qualitativ hochwertige Informationen zu gelangen und so an der Informationsgesellschaft teilzuhaben. Eine aktiv informationsorientierte Internetnutzung vermag gesellschaftliche Hürden zu überwinden und Unterschiede aufzuheben. Gleichzeitig besteht aber auch die Gefahr, dass bestehende Ungleichheiten sich verstärken oder neue entstehen, wenn Bevölkerungsgruppen in den Informationsaustausch über das Internet nicht miteinbezogen werden oder das Internet ausschließlich passiv zu Unterhaltungszwecken nutzen.

Darüber hinaus werden unter anderem in Form von Print-Broschüren eine Vielzahl an Angeboten außerhalb des Internets für die Verbraucherinnen und Verbraucher zur Verfügung gestellt. Weitere wichtige Aufklärung in Form von Information und Beratung in diesem Bereich führen die Verbraucherzentrale Hessen und der DHB-Netzwerk Haushalt Hessen mit Hilfe direkter Beratung und in Form von Print-Ratgebern und Broschüren durch. Zur Wahrnehmung ihrer Aufgaben werden beide Organisationen vom Hessischen Verbraucherschutzministerium finanziell gefördert.

Auf die Antworten zu den Fragen 1 und 2 wird verwiesen.

Frage 8. Welchen Veränderungsbedarf sieht die Landesregierung bei der Medienaufsicht hinsichtlich ihrer Funktion als Aufsichts- und Informationsinstanz mit Blick auf das Thema "Verbraucherschutz im Internet"?

Im Koalitionsvertrag der die Regierungskoalition tragenden Parteien wird der Maßstab zur (straf-)rechtlichen Beurteilung von Netzinhalten entsprechend dem Leitsatz "Was außerhalb des Netzes verboten ist, muss auch im Netz verboten sein" vorgegeben. Diesem Leitsatz folgend passt sich stets auch die Medienaufsicht an die aktuellen Entwicklungen der digitalen Welt an.

Nach § 59 Abs. 2 des Rundfunkstaatsvertrages in Verbindung mit § 3 des Gesetzes zu dem Neunten Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (Neunter Rundfunkänderungsstaatsvertrag) überwacht die Hessische Landesanstalt für privaten Rundfunk und neue Medien (LPR Hessen) die Einhaltung der Bestimmungen für Telemedien privater Anbieter einschließlich der allgemeinen Gesetze und der gesetzlichen Bestimmungen zum Schutz der persönlichen Ehre mit Ausnahme des Datenschutzes. Zu den Verbraucherschutzrelevanten Aufsichtstätigkeiten gehört sowohl die Aufsicht über die Einhaltung der Impressumspflichten durch die in Hessen ansässigen Dienstleister als auch die Aufsicht über die Einhaltung der Werbebestimmungen nach § 7 und § 8 des Rundfunkstaatsvertrages.

Darüber hinaus können Verbraucherinnen und Verbraucher neben Verstößen gegen die Impressumspflichten im Internet auch sonstige Auffälligkeiten und Verstöße - insbesondere auch illegale oder jugendgefährdende Inhalte - an die Beschwerdestelle der LPR Hessen melden. Bei illegalen Inhalten stimmt sich die LPR Hessen mit den Polizeibehörden und den Staatsanwaltschaften eng ab.

Verbraucherschutz spielt auch eine große Rolle im Rahmen der Medienkompetenzarbeit der Landesanstalt. Neben der Veröffentlichung verbraucherschutzrelevanter Informationen (wie z.B. Kostenfalle und Handystrahlung) und der Herausgabe eines Baukastens zum Thema "Kinder und Werbung", der zur Fortbildung und Anleitung von Erziehern dient, spielt der Verbraucherschutz bei verschiedenen Medienprojekten und Fortbildungen eine Rolle.

Im Vergleich zu den Regelungen in anderen Ländern bei denen die Zuständigkeiten auf unterschiedliche Landesbehörden verteilt sind, hat sich die in Hessen geregelte Zuständigkeitskonzentration bei der Landesmedienanstalt sehr bewährt. Sie trägt in hohem Maße zur Effektivität und Rechtssicherheit bei. Nach Einschätzung des LPR Hessen hat sich im Verhältnis zu den Staatsanwaltschaften im Land eine pragmatische Verwaltungspraxis entwickelt. Vor diesem Hintergrund sieht die Hessische Landesregierung keinen Veränderungsbedarf.

Frage 9. Welche geschlechtsspezifischen Herausforderungen ergeben sich aus Sicht der Landesregierung hinsichtlich des Verbraucherschutzes im Internet?

Die hierzu befragte Verbraucherzentrale Hessen (VZ Hessen) berichtet, dass aus ihrer täglichen Beratungspraxis bisher keine signifikanten geschlechtsspezifischen Unterschiede erkennbar gewesen sind. Allerdings sind Beschwerden und Vorgänge in der VZ Hessen nicht nach geschlechtsspezifischen Kriterien erfasst worden.

Auch laut dem DHB-Netzwerk Haushalt Hessen sind keine geschlechtsspezifischen Herausforderungen hinsichtlich des Verbraucherschutzes im Internet erkennbar. Nach Auskunft des DHB nutzen Männer das Internet zwar häufiger, doch vorwiegend beruflich. Sie sind daher genauso häufig "gefährdet" wie Frauen.

Laut der Studie der Forschungsgruppe Wahlen "Internet-Strukturdaten IV. Quartal 2013" lag der prozentuale Anteil der Männer, die das Internet nutzten, bei 85 % (plus drei im Vergleich zum IV. Quartal 2012), jener der Frauen unverändert bei 71 %. Aus Sicht der Landesregierung besteht die zentrale Herausforderung darin, diese Tendenz der zunehmenden Annäherung zwischen den weiblichen und männlichen Nutzergruppen weiter zu verstetigen.

Frage 10. Welche altersspezifischen Herausforderungen ergeben sich aus Sicht der Landesregierung hinsichtlich des Verbraucherschutzes im Internet?

Im Umgang mit dem Internet gab es laut Studie der Forschungsgruppe Wahlen "Internet-Strukturdaten IV. Quartal 2013" nur zwischen Bürgern unter und über 60 Jahren noch nennenswerte altersspezifische Unterschiede: Während 94 % der Befragten bis 59 Jahren das Internet nutzten, lag die Zugangsrate bei Befragten ab 60 Jahren lediglich bei 48 %.

Laut dem DHB-Netzwerk Haushalt Hessen reagieren junge Nutzer spontaner, ungeduldiger, sind von ihren Kenntnissen überzeugt und unterliegen häufig dem Gruppenzwang. Alte/ältere Nutzer sind vorsichtiger, verstehen aber die Internetsprache nicht immer und brauchen Hilfestellung.

Mit umfassenden Informationen wird seitens der Landesregierungen über die Gefährdungen im Internet aufgeklärt. Gerade im Hinblick auf die Einbindung älterer Menschen gilt es, das Angebot weiter auszubauen und einen barrierefreien Zugang für alle Verbraucherinnen und Verbraucher zu gewährleisten.

Für Menschen in fortgeschrittenem Alter und vor allem in ihrer Bewegung eingeschränkte Seniorinnen und Senioren bietet das Internet Chancen, den Alltag zu erleichtern, Kontakte zu pflegen und sich Informationen zu beschaffen, die auf anderem Weg nicht zu erreichen wären. Die Vermittlung von Medienkompetenz für ältere Menschen ist deshalb der Landesregierung ein großes Anliegen. Die vom Land Hessen geförderte Landesseniorenvertretung zeigt z.B. auf der Internetseite [www.sozialnetz.de](http://www.sozialnetz.de) unter dem Stichwort "Senioren auf Draht" allen Interessierten Möglichkeiten auf, um die Welt des Internets zur eigenen Nutzung zu erschließen.

Frage 11. Welchen Stellenwert bei der Entwicklung und Weiterentwicklung netzpolitischer Initiativen im Bereich des Verbraucherschutzes nimmt die Einbeziehung der sogenannten "Netzgemeinde" ein?

Die Landesregierung räumt dieser Entwicklung einen hohen Stellenwert ein. Mit der Einbeziehung der sogenannten "Netzgemeinde" können Verbraucherinnen und Verbraucher vor Ort stärker mit den Entscheidungen auf kommunaler Ebene einbezogen werden, umgekehrt profitieren die politischen Akteure und die Verwaltung von den Ideen der Bürgerinnen und Bürger.

Frage 12. Durch welche Maßnahmen beabsichtigt die Landesregierung im Einzelnen, bei der Entwicklung verbraucherpolitischer Maßnahmen innerhalb ihrer Netzpolitik die "Netzgemeinde" einzubeziehen?

Die Landesregierung bezieht bei der Ausgestaltung der Querschnittsaufgabe Netzpolitik die in der Internetwelt gewachsenen formellen (z.B. Kammern, Verbände, Vereine, Kirchen) und informellen Strukturen (Communities) partnerschaftlich mit ein.

Bei der Entwicklung politischer Maßnahmen bezieht die Landesregierung die Verbraucherinnen und Verbraucher auf verschiedene Art und Weise ein. Die Hessische Staatskanzlei betreut einen Facebook-Auftritt der Landesregierung, bei dem auch über verbraucherpolitische Maßnahmen der Landesregierung informiert und aktuelle verbraucherpolitische Themen aufgegriffen werden.

Das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz betreibt darüber hinaus den Twitter-Account [www.twitter.com/Verbraucherinfo](http://www.twitter.com/Verbraucherinfo). Hier wird regelmäßig über aktuelle verbraucherrelevante Themen sowohl der Landesregierung als auch überregional informiert. Die Inhalte der Postings zu Themen wie Energie, Ernährung, Datenschutz, Finanzen, Gesundheit, Recht, Telekommunikation sind sachlich, fundiert, unabhängig, crossmedial.

Bürgerinnen und Bürger haben die Möglichkeit diesen Informationen zu folgen und sich aktiv auszutauschen. Die Angebote des Internetportals [www.Verbraucherfenster.de](http://www.Verbraucherfenster.de) werden auf diesem Wege zusätzlich beworben. Im Rahmen des gesetzlich verankerten Informationsauftrages wird der Einsatz von Social Media nicht nur als sinnvolle Ergänzung sondern als unverzichtbarer Bestandteil der Öffentlichkeitsarbeit erachtet. Verbraucherinnen und Verbraucher haben ebenso die Möglichkeit, über das VerbraucherFenster <http://www.verbraucherfenster.hessen.de> Kontakt mit der Landesregierung aufzunehmen und ihre Anliegen darzulegen, die dann weiter verfolgt und beantwortet werden.

## **Verbraucherschutz und Verbraucherinformation**

Frage 13. In wie vielen Fällen waren in den letzten fünf Jahren hessische Verbraucherinnen und Verbraucher von sogenannten Abo-Fallen betroffen (falls keine exakten Zahlen vorhanden sind, bitte schätzen)?

Bei den so genannten Internet-Abofallen handelt es sich um Internetangebote, bei denen Unternehmen die Entgeltspflichtigkeit ihrer Angebote zu verschleiern suchen. Die Geschäftsidee besteht darin, eine Sammlung von Informationen auf der entsprechenden Website gegen ein Entgelt zur Verfügung zu stellen. Irreführend für die Verbraucherin oder den Verbraucher ist, dass vergleichbare Informationen im Internet sonst kostenlos erhältlich sind. Bei den Serviceangeboten handelt es sich z.B. um Hausaufgabenhilfe, Berufswahlunterstützung, Tests (Intelligenz, Produktvergleich, Führerschein), Ahnenforschung, Lebenserwartungs-Rechner, Routenplaner, Online-Spiele. Bei den angebotenen Waren handelt es sich oftmals um Kochrezepte, E-Cards, "Gratis"-SMS, Musikdateien, Filme und Software sowie In-App-Käufe bzw. App-Billing. Verbraucherinnen oder Verbraucher melden sich an und erhalten wenig später eine Bestätigung eines Vertrages mit einer bestimmten Grundlaufzeit (meist 24 Monate). Es folgen Rechnungen, Mahnungen und Inkassoschreiben.

Seit etwa 2004 beschäftigt das Thema "Abofallen im Internet" die Verbraucherzentralen. Beschwerden dazu gingen laut Verbraucherzentrale Hessen zeitweise in großer Vielzahl ein. Laut einer Untersuchung des Sozialforschungsinstituts Infas vom Sommer 2011 waren damals 5,4 Millionen deutsche Internetnutzer auf eine Abo-Falle im Internet hereingefallen - das sind elf % aller deutschen Internetnutzer. Der wirtschaftliche Schaden war immens: Der durchschnittliche Forderungsbetrag lag bei ca. 100 €. Mit einer bundesweiten Umfrage haben die Verbraucherzentralen vom 14. September bis zum 28. Oktober 2007 Verbraucherinnen und Verbraucher zu ihren Erfahrungen mit ungewollten Abo-Verträgen im Internet befragt. Es haben 6.658 Ver-

braucherinnen und Verbraucher an der Befragung teilgenommen ([http://web.archive.org/web/20110705130704/http://www.verbraucher.de/download/umfrageergeb\\_abzocke.pdf](http://web.archive.org/web/20110705130704/http://www.verbraucher.de/download/umfrageergeb_abzocke.pdf)). Die Verbraucherzentralen der Länder schätzten 2012 die Zahl der bundesweit bei ihnen eingehenden Beschwerden auf rund 22.000 pro Monat. Spezifische Untersuchungen der Verbraucherzentrale Hessen über die Anzahl der durch Abo-Fallen betroffenen hessischen Verbraucherinnen und Verbraucher liegen nicht vor. Laut dem DHB-Netzwerk Haushalt Hessen waren ca. 10.000 Verbraucherinnen und Verbraucher in den letzten fünf Jahren betroffen.

Eine Erfassung und Auswertung des Phänomens "Abo-Falle" wurde in der Polizeilichen Kriminalstatistik (PKS) für Hessen mit Beginn des Jahres 2014 erstmals eingeführt. Eine Schätzung der Zahl ist nicht möglich.

Frage 14. Sind hierbei geschlechtsspezifische Unterschiede erkennbar?

Auf die Antwort zu Frage 13 wird verwiesen. Aufgrund der bundesweit einheitlichen Richtlinien zur Führung der Polizeilichen Kriminalstatistik ist auch künftig keine Erfassung von Opfern vorgesehen, die eine geschlechterspezifische Auswertung ermöglicht.

Aus der täglichen Beratungspraxis der Verbraucherzentrale Hessen sind bislang keine signifikanten geschlechtsspezifischen Unterschiede erkennbar gewesen. Allerdings sind Beschwerden und Vorgänge bei der Verbraucherzentrale Hessen bislang nicht nach geschlechtsspezifischen Kriterien erfasst worden. Geschlechtsspezifische Maßnahmen im Bereich "Digitale Welt" wurden diesseits bislang nicht betrieben.

Laut dem DHB-Netzwerk Haushalt waren Männer häufiger bei Internetverträgen, Frauen häufiger bei Abo-Verträgen am Telefon betroffen.

Frage 15. Welche Veränderung hat sich bei den Fallzahlen seit Inkrafttreten der "Button-Lösung" am 1. August 2012 ergeben?

Mit der Einführung der neuen Verbraucherschutzregelungen zum 1. August 2012, insbesondere des § 312 g BGB, ist die Darstellung der Bestellsituationen so zu gestalten, dass die Verschleiernsmöglichkeiten weitestgehend ausgeschlossen werden. Ein Vertrag mit einer Verbraucherin oder einem Verbraucher im elektronischen Geschäftsverkehr kommt demnach nur zustande, wenn sie/er mit der Bestellung ausdrücklich bestätigt, dass sie/er sich zu einer Zahlung verpflichtet. Bei Bestellungen auf Online-Plattformen im Internet, die über Schaltflächen erfolgen, ist hierzu erforderlich, dass die Bestellschaltfläche gut lesbar mit den Wörtern "zahlungspflichtig bestellen" oder einer entsprechenden eindeutigen Formulierung beschriftet ist.

Die Neuregelung hat das Geschäftsmodell der klassischen Abo-Falle für die "Anbieter" wirtschaftlich uninteressant werden lassen und darf insofern als Erfolg gewertet werden. Das bestätigt auch die Verbraucherzentrale Hessen: Nach Einführung der Neuregelung dauerte es nicht lange, bis der überwiegende Teil der einschlägig bekannten Internetseiten nicht mehr aufrufbar war. Die Beratungszahlen bei der Verbraucherzentrale Hessen sind diesbezüglich stark zurückgegangen. Im Laufe des Jahres 2013 war noch eine kleine Anfragewelle zu verzeichnen. Hierbei ging es meist um Rechnungen, die die Anbieter angeblichen Bestandskunden für das zweite Vertragsjahr zusandten (siehe auch Ziffer 4.). Neue Fälle kamen so gut wie nicht mehr hinzu.

Auch der DHB-Netzwerk Haushalt Hessen gibt ebenfalls an, dass sich die Fallzahlen zunächst halbiert haben, inzwischen sehr selten geworden sind.

Frage 16. Wie bewertet die Landesregierung insgesamt das Risiko, das von den sogenannten Abo-Fallen ausgeht?

Abo-Fallen sind eine weit verbreitete unseriöse Geschäftspraktik im Internet, bei der Verbraucherinnen oder Verbraucher unbeabsichtigt ein kostenpflichtiges Abonnement eingehen. Es handelt sich dabei um Internetangebote, die so trickreich gestaltet sind, dass deren Kostenpflicht für Verbraucherinnen oder Verbraucher nicht ohne weiteres erkennbar ist. Manchmal werden auch die Seiten seriöser Anbieter imitiert. Im Vorfeld der neuen gesetzlichen Regelung hatten zahlreiche Anbieter im Internet unseriös für kostenpflichtige Angebote geworben. Versteckte Kostenfallen im Internet sind nach einem Urteil des Bundesgerichtshofs (BGH) als versuchter Betrug einzustufen. Der 2. Strafsenat bestätigte ein Urteil des Landgerichts Frankfurt am Main von Juni 2012 (Az. 5-27 KLS 12/08). Der Betreiber mehrerer kostenpflichtiger Internet-Angebote wollte damals die Strafe von zwei Jahren Haft auf Bewährung nicht akzeptieren und legte Revision beim BGH ein (Az. 2 StR 616/12). Der BGH führte aus, dass "die Kostenpflichtigkeit der angebotenen Leistung gezielt verschleiert" worden sei. Damit liege eine Täuschungshandlung nach § 263 Strafgesetzbuch (StGB) vor.

Die vielfach in der Realität gar nicht existierenden Forderungen werden von unseriösen Unternehmen aggressiv mittels zahlreicher Mahnungen sowie der Einschaltung von Inkassobüros und Anwälten geltend gemacht. Da die Verbraucherinnen und Verbraucher ob des massiven Drucks

sehr verunsichert werden, zahlen sie oftmals Rechnungen, für die es keine rechtliche Grundlage gibt. Konsequenz: diese einmalige Zahlung wurde aus Sicht der "Anbieter" dann meist als An-erkenntnis des Vertrages gewertet. Weitere Konsequenz war, dass die Verbraucherinnen oder Verbraucher spätestens nach einem Jahr die Folgerechnung für das zweite Vertragsjahr erhiel-ten. Denn aus Sicht der "Anbieter" galt meist eine 24-monatige Grundlaufzeit.

Der DHB-Netzwerk Haushalt Hessen gibt darüber hinaus an, dass vor allem unüberschaubare Kosten und die Preisgabe von persönlichen Daten und deren ungewollte Weitergabe Folgen von Abo-Fallen sind und zu langfristigen finanziellen Bindungen bis hin zur Verschuldung führen können.

Frage 17. Mit welchen Maßnahmen geht die Landesregierung gegen sogenannte Abo-Fallen vor?

Hessen hat im Bundesrat den Gesetzgebungsprozess der so genannten Button-Lösung aktiv unterstützt und sich im Zuge der nationalen Gesetzgebung und auf europäischer Ebene erfolg-reich für eine Ausweitung der Button-Lösung auch auf alle mobilen Endgeräte eingesetzt.

Im Rahmen ihres Informationsportals [www.verbraucherfenster.de](http://www.verbraucherfenster.de) informiert die Landesregie-rung regelmäßig über aktuelle Entwicklungen und klärt Verbraucherinnen und Verbraucher über mögliche neue Risiken und Entwicklungen in dem Bereich auf. Zum Thema "Abo-Falle" kann sich die Verbraucherin oder der Verbraucher in mehreren Beiträgen informieren, unter anderem "Internet-Kostenfallen: Besserer Schutz durch Button-Lösung", "Ihre Rechte als Verbraucher in Europa - von Fluggastrechten bis hin zum Einkauf im Ausland".

Via Twitter wird über die wichtigsten Aspekte hinsichtlich Verbraucherschutzinformationen so-wohl der Landesregierung als auch überregional berichtet.

Die Landesregierung unterstützt die Verbraucherzentrale Hessen und den DHB-Netzwerk Haus-halt Hessen in Form einer institutionellen Förderung. Diese beiden Organisationen informieren und klären Verbraucherinnen und Verbraucher in ihren Beratungen auf und bieten eine wichtige Hilfestellung für betroffene Verbraucherinnen und Verbraucher auch im Bereich Abo-Fallen. Fragen zu diesem Themenkomplex werden in den Beratungen beantwortet. Die Verbraucher-zentrale Hessen informiert persönlich im Rahmen der allgemeinen Rechtsberatung in ihren örtli-chen Beratungsstellen und auf ihren Internetseiten [www.verbraucher.de](http://www.verbraucher.de). Zur Abwehr unberech-tigter Forderungen hält sie entsprechende Musterschreiben bereit. Die Verbraucherzentrale Hes-sen hat allerdings immer wieder die Erfahrung gemacht, dass sich Verbraucherinnen oder Ver-bräucher angesichts der von den Seitenbetreibern aufgebauten Drohkulisse (Übersendung von Urteilen, Inkasso- oder Rechtsanwältsschreiben mit Androhung von Zwangsvollstreckung und Meldung bei Auskunfteien etc.) verunsichert zeigen. Ferner sehen sich die betroffenen Verbrau-cherinnen und Verbraucher - auch diejenigen, die sich schriftlich gegen die geltend gemachten Forderungen zur Wehr gesetzt haben - oftmals noch Jahre später mit entsprechenden Forderun-gen konfrontiert.

Frage 18. Wie bewertet die Landesregierung die gesetzliche Regelung der "Button-Lösung"?

Durch die Button-Lösung werden Online-Händler zu einer aussagekräftigen Schaltfläche ver-pflichtet, die klar kennzeichnen muss, wenn ein Mausklick Geld kostet. Die Anbieter sind seit dem 1. August 2012 dazu verpflichtet, noch vor dem Abschluss eines Vertrages über wesentli-che Vertragselemente wie den Preis oder Vertragslaufzeiten zu informieren - und das klar, ver-ständlich und in hervorgehobener Weise. Für die Verbraucherin oder den Verbraucher bedeutet das mehr Transparenz und Rechtssicherheit. Die Regelung greift auch bei mobilen Geräten wie Smartphones oder Tablets und hat zu einer positiven und deutlich spürbaren Rücknahme von Abo-Fallen geführt. Für die "Anbieter" ist die klassische "Abo-Falle" wirtschaftlich uninteres-sant geworden. Insofern darf die "Button-Lösung" als Erfolg gewertet werden.

Dass die "Button-Lösung" wirkt, hat auch eine Untersuchung des Bundesverbandes Verbrau-cherzentrale (vzbv) direkt nach Einführung der "Button-Lösung" bestätigt. Schon einen Monat nach Inkrafttreten der "Button-Lösung" waren von 109 einschlägig bekannten Seiten mit Kos-tenfallen 88 - laut Umfrage des Bundesverbandes Verbraucherzentrale - nicht mehr aufrufbar, bei 13 weiteren konnte man sich nicht mehr anmelden.

Das im September 2014 veröffentlichte Gutachten des Bundesministeriums für Justiz und Ver-bräucherschutz (BMJV) über die Auswirkungen des Gesetzes zum besseren Schutz der Verbrau-cherinnen und Verbraucher vor Kostenfallen im elektronischen Geschäftsverkehr (Button-Lösung) kommt ebenfalls zu dem Ergebnis, dass hinsichtlich des materiellen Rechts kein Hand-lungsbedarf besteht. Laut Studie besteht zwar Klärungsbedarf insbesondere hinsichtlich der wesentlichen Eigenschaften und deren Darstellung und Positionierung, diesem kann jedoch wegen der Vielfalt von Optionen nicht in Form von Gesetzen oder Verordnungen nachgekommen wer-den. Auch ist fraglich, ob der deutsche Gesetzgeber hierfür vor dem Hintergrund europarechtli-cher Vorgaben (Verbraucherrechterichtlinie-RL) überhaupt einen Gestaltungsspielraum hätte.

([http://www.bmfv.de/SharedDocs/Downloads/DE/pdfs/20140904\\_BUTTON\\_LOESUNG.pdf;jsessionid=1F89A6BFF1B775E60060DDC6FE0516A6.1\\_cid334?\\_\\_blob=publicationFile](http://www.bmfv.de/SharedDocs/Downloads/DE/pdfs/20140904_BUTTON_LOESUNG.pdf;jsessionid=1F89A6BFF1B775E60060DDC6FE0516A6.1_cid334?__blob=publicationFile))

Frage 19. Hält die Landesregierung diese Regelung für ausreichend?

Die Regelung schafft Klarheit und Transparenz für Verbraucherinnen und Verbraucher. Sie ist in ihrer derzeitigen Form wirksam, wie auch eine Untersuchung des Bundesverbandes Verbraucherzentrale (vzbv) von 2012 und das Gutachten des Bundesministeriums für Justiz und Verbraucherschutz von September 2014 belegen.

Auf die Antwort zur Frage 18 wird verwiesen.

Frage 20. Wenn nein, welchen Verbesserungsbedarf sieht die Landesregierung?

Auf die Antworten zu den Fragen 18 und 19 wird verwiesen.

Die Landesregierung wird die Verbraucherinformation und Verbraucheraufklärung weiter fortführen und dabei die ihr zur Verfügung stehenden Plattformen nutzen. Hierbei muss es insbesondere darum gehen, ältere Menschen und Personen, die das Internet nicht regelmäßig nutzen, zu erreichen.

Frage 21. Sind der Landesregierung Geschäftsmodelle zur Umgehung der "Button-Lösung" bekannt?

Die von der Landesregierung geförderte Verbraucherzentrale Hessen berichtet, dass sich die Strategien hinter Kostenfallen stetig verändern.

Es gibt Internetseiten, die offiziell für Händler bestimmt sind, aber auch von Verbraucherinnen und Verbrauchern in Anspruch genommen werden können. Hinter vermeintlichen Schnäppchen verstecken sich Abo-Fallen. Da sich das Angebot aber offiziell an Gewerbetreibende richtet, haben Verbraucherinnen oder Verbraucher keine Möglichkeiten hiergegen vorzugehen.

Zum anderen werden Lockangebote geschaltet, die sich nach einer kostenlosen Testphase in ein kostenpflichtiges Abo umwandeln. Darauf wird aber nur versteckt hingewiesen. Wie die Informationen für Verbraucherinnen und Verbraucher im Einzelfall darzustellen sind, darüber müssen die Gerichte entscheiden.

Im Netz gibt es inzwischen auch immer mehr Online-Schnäppchen-Marktplätze, die zwar in ihren Vertragsbedingungen vorgeben, sich nur an Unternehmer (und nicht an Verbraucherinnen oder Verbraucher) zu richten. Verbraucherinnen und Verbraucher können sich aber meist problemlos (ohne Nachweis der gewerblichen oder freiberuflichen Tätigkeit) anmelden. Nach der Registrierung erhalten die Betroffenen Rechnungen über eine Grundgebühr von rund 250 € sowie eine Aufnahmegebühr von weiteren rund 200 €. Der Preishinweis ist oft am Bildrand der Anmeldeseite versteckt

Besonders problematisch ist laut Verbraucherzentrale Hessen die sogenannte B2B-Masche. Zwar gibt es auch seriöse B2B-Portale, die im Vorfeld auf sämtliche Kosten hinweisen. Aber laut Verbraucherzentrale häuften sich in der Vergangenheit immer mehr unseriöse Angebote dieser Art: Bei B2B erhält der Nutzer das Angebot, Waren mit sehr hohen Rabatten zu erwerben. Zugrunde gelegt werden Großhandelspreise, an denen man partizipieren kann. Für den Laien geht beim Durchlesen der Seite nicht deutlich hervor, dass B2B vom Grundsatz her für Geschäftsbeziehungen zwischen zwei Unternehmen besteht. Die (private) Verbraucherin oder der (private) Verbraucher meldet sich an, akzeptiert die AGBs und "kauft" günstige Geräte. Erst nach Abschluss erfährt er, dass eine Mitgliedsgebühr entrichtet werden muss. Zahlt der Nutzer nicht, folgt eine Abmahnung.

Das B2B-Handelsportal wirbt gewerbliche Kunden für seine Plattform. Die Gewerbetreibenden sollen sich anmelden und einen Jahresbeitrag zahlen. Die Plattform hat leider nur dann viel zu wenige Angebote. Allein die Anzahl der B2B-Internetseiten der JW-Handelssysteme GmbH/B2B Technologies Chemnitz GmbH vergrößert sich laut Verbraucherzentrale Hessen stetig. Aktuell (12. Juni 2014) sind es diese:

- [b2b-48.de](http://b2b-48.de)
- [b2b-einkaufen.de](http://b2b-einkaufen.de)
- [b2b-einkaufsplattform.de](http://b2b-einkaufsplattform.de)
- [b2b-Handelsportal.com](http://b2b-Handelsportal.com)
- [b2b-Kundenportal.de](http://b2b-Kundenportal.de)
- [B2B-Lagerware.de](http://B2B-Lagerware.de)
- [b2b-shoppen.de](http://b2b-shoppen.de)
- [beschaffungsplattform24.de](http://beschaffungsplattform24.de)
- [beste-lieferanten.de](http://beste-lieferanten.de)
- [Der-Restpostengigant.de](http://Der-Restpostengigant.de)

- Die-besten-Einkaufspreise.de
- discount-lagerverkauf.de
- einkaufen-billiger.com
- einkauf-marktplatz.de
- gewerbe-einkauf.de
- gewerbe-handelsplattform.de
- gewerbemarktplatz24.de
- gewerblicheinkaufen.de
- Handelsgiganten.de
- Handelsspezialisten.de
- justbusiness24.de
- lagerverkauf-deutschland.de
- Lagerware24.de
- lagerware2013.de
- lagerware2014.de
- lagerware-b2b.de
- lagerware-billiger.de
- lagerware-online.de
- lagerwarenwelt.de
- Lieferantengeheimnis.de
- mega-einkaufsquellen.de
- meine-respostenwelt.de
- Melango.de
- nur-fuer-gewerbekunden.de
- nur-gewerbetreibende.de
- Online-Businessportal.de
- onlybusiness48.de
- overstock-business.de
- parfum.women.online-businessportal.de
- platz-fuer-gewerbekunden.de
- preiswert-einkaufen-b2b.de
- restposten99.de
- werksverkauf-germany.de

Neben der oben geschilderten "B2B-Masche" hatte der Bundesverband Verbraucherzentrale (vzbv) seit Inkrafttreten der "Button-Lösung" viele weitere Unternehmen abgemahnt. Auf den Webseiten von acht Unternehmen war überhaupt kein Bestellbutton zu finden, der eindeutig auf die Zahlungspflicht hinwies. Im Übrigen wurden die Vertragsinhalte wie Preis und Laufzeit des Vertrages nicht deutlich hervorgehoben vor dem Bestellbutton dargestellt. Web.de etwa warb mit einer zweimonatigen kostenlosen Testphase für eine Clubmitgliedschaft. Wer nicht rechtzeitig kündigte, war ein Jahr gebunden und sollte monatlich fünf Euro zahlen. Hinweise fanden sich nur im Kleingedruckten, weshalb das Landgericht Koblenz die Werbung für unzulässig hielt und der Klage des vzbv stattgegeben hat. Andere Unternehmen warben mit einer kurzen Vertragslaufzeit zu einem einmalig zu zahlenden Gesamtpreis, obwohl sich der Vertrag automatisch in ein kostenpflichtiges Abonnement umwandelte. Diese Information stand ebenfalls nur im Kleingedruckten - zum Nachteil der Verbraucherinnen und Verbraucher.

Einstieg in eine Kostenfalle kann nach wie vor auch die Teilnahme an Gewinnspielen und Tauschbörsen sowie die Bestellung von Probeabonnements sein.

Eine Übersicht über die Verfahren des vzbv zu Verträgen im Internet vor und nach Einführung der "Button-Lösung" (Kostenfallen im Internet und Praxistest Buttonlösung) ist hier veröffentlicht: [http://www.vzbv.de/cps/rde/xbcr/vzbv/Kostenfallen\\_im\\_Internet.pdf](http://www.vzbv.de/cps/rde/xbcr/vzbv/Kostenfallen_im_Internet.pdf)

Frage 22. Welche Maßnahmen plant oder unternimmt die Landesregierung in Bezug auf diese Geschäftsmodelle?

Es gilt diese Entwicklungen abzuwarten und bei einer starken Zunahme ggf. Nachbesserungen zu überprüfen. Notwendig wäre bei einem weiteren Zuwachs unter anderem eine deutliche Identifizierungspflicht als Händler sowie ein deutlicher Hinweis, der anzeigt, dass sich das Angebot nur an Gewerbetreibende richtet. Die Landesregierung wird zudem die Verbraucherinformation und Verbraucheraufklärung fortführen und dabei die ihr zur Verfügung stehenden Plattformen nutzen.

Die von der Landesregierung geförderte Verbraucherzentrale Hessen wird ebenso weiterhin den einschlägigen Markt beobachten und versuchen, verbraucherschutzgesetzeswidrige Praktiken von Unternehmen durch Wahrnehmung ihrer gesetzlichen Abmahn- und Klagebefugnisse zu unterbinden. Ebenso werden die Verbraucherzentralen die Entwicklung in der Rechtsprechung beobachten und den sich gegebenenfalls ergebenden gesetzgeberischen Nachbesserungsbedarf aufzeigen.

Frage 23. Geht die Landesregierung von einem höheren Gefahrenpotenzial von Abo-Fallen aus, die in Anwendungen (Apps) integriert sind?

Auf die Antworten zu den Fragen 74,78 und 80, 129 und 134 wird verwiesen.

Die "Button-Lösung" gilt grundsätzlich auch für den Vertragsschluss via Smartphone. Trotz des Beschwerderückgangs bei/zu Abo-Fallen im Internet ist laut Verbraucherzentrale Hessen nicht auszuschließen, dass unzulässige Angebotsseiten reaktiviert oder alte Methoden nun bei Bestellungen über Smartphones versucht werden. Beim Smartphone müssen Verbraucherinnen oder Verbraucher sich häufig nicht einmal registrieren, um in eine Kostenfalle zu tappen. Wie sich auch in der Beratungspraxis der Verbraucherzentrale Hessen immer wieder zeigt, kann bereits ein (unbeabsichtigter) Fingertipp auf einen Werbebanner dazu führen, dass angeblich kostenpflichtige Leistungen (wie etwa ein Abonnement mit bestimmter Laufzeit) heruntergeladen und ein relativ geringer Betrag per "Wap-Billing" über die Handyrechnung eingezogen wird. Verbraucherinnen und Verbraucher merken das häufig erst dann, wenn der gewohnte Rechnungsbetrag deutlich und ohne offensichtlichen Grund überschritten wird. Die Verbraucherin oder der Verbraucher hat hier das Problem, dass sie/er sich nicht nur mit dem dahinterstehenden Dienstanbieter, sondern zusätzlich noch mit seinem eigenen Mobilfunkanbieter auseinandersetzen muss. Verweigert sie/er die Zahlung bzw. kürzt sie/er seine Mobilfunkrechnung um den entsprechenden Betrag, sieht sie/er sich zusätzlich mit Sperrandrohungen konfrontiert. Die Verbraucherzentralen werden die Aktivitäten der Abo-Fallen-Betreiber deshalb weiterhin aufmerksam verfolgen und prüfen, ob es noch weiteren Nachbesserungsbedarf zu der mit Wirkung zum 1. August 2012 neu geschaffenen "Button-Lösung" zum Schutz vor Abo-Fallen gibt.

Frage 24. Wie schätzt die Landesregierung die Auswirkungen der "Button-Lösung" für das mobile Internet ein?

Da die Vorschriften zur "Button-Lösung" technikneutral sind, gelten diese Regelungen auch für das mobile Internet und damit für Smartphones und Tablets.

Die Bundesnetzagentur erfasst Beschwerden in diesem Bereich statistisch nicht separat, so dass keine belastbaren Zahlen vorliegen. Allerdings sind der Bundesnetzagentur unter diesem Themenkomplex 2013 insgesamt ca. 135 sowie 2014 bisher ca. 35 Beschwerden bekannt.

Im Übrigen wird auf die Antworten zu den Fragen 23, 74 verwiesen.

### **Mobile Internetnutzung**

Frage 25. Wie viele Fälle von Diebstahl sensibler Daten (wie beispielsweise E-Mail-Adressen oder Kontaktdaten) durch einen Zugriff über Mobiltelefone hat es in den letzten fünf Jahren in Hessen gegeben (falls keine exakten Zahlen vorhanden sind, bitte schätzen, und soweit möglich geschlechtsspezifisch aufschlüsseln)?

Die Polizeilichen Kriminalstatistik (PKS) weist den Zugriff auf sensible Daten bzw. den Diebstahl sensibler Daten über Mobiltelefone nicht aus. Eine Schätzung der Zahl ist nicht möglich, da für eine Schätzung die empirischen Grundlagen fehlen.

Frage 26. Wie viele Fälle hiervon sind in den letzten fünf Jahren bekannt und zur Anzeige gebracht worden (bitte nach Jahren aufschlüsseln)?

Der Polizeilichen Kriminalstatistik (PKS) sind entsprechende Angaben nicht zu entnehmen.

Frage 27. Wie viele Verurteilungen in Zusammenhang mit diesen Taten gab es in den letzten fünf Jahren? (Bitte nach Jahren aufschlüsseln).

Der Polizeilichen Kriminalstatistik (PKS) sind entsprechende Angaben nicht zu entnehmen.

Frage 28. Welche Maßnahmen zur Aufklärung von Verbraucherinnen und Verbrauchern plant die Landesregierung zu ergreifen, in Bezug auf Smartphone-Apps, die sich unerlaubt Berechtigungen verschaffen und somit beispielsweise Nachrichten verschicken oder Daten auslesen (bitte aufschlüsseln nach Art und Träger der Maßnahme sowie Form der Unterstützung)?

Neben den grundsätzlichen Aufklärungskampagnen des Programms Polizeiliche Kriminalprävention (PKS) der Länder und des Bundes, des hessischen Landespräventionsrates und der Landesanstalt für Medien bildet die hessische Polizei Multiplikatorinnen und Multiplikatoren im Bereich Prävention "Cybercrime" aus. In diesem Rahmen wird gemäß der Standards polizeilicher Kriminalprävention der hessischen Polizei auf grundsätzliche Gefahren an Beispielen aktueller Phänomene eingegangen. Eines der dargestellten Themen behandelt Tablets, "Phablets" sowie Smartphones und die Problematik der Rechteinräumung, die mit der Nutzung einiger Apps einhergehen kann. Darüber hinaus wurde mit der Verbraucherzentrale Hessen e.V. eine Kooperationsvereinbarung mit der Intention geschlossen, die Zusammenarbeit auf allen Ebenen zu intensivieren und aktuelle Tatbegehungsweisen und wirksame Schutzmöglichkeiten für die Verbraucherinnen und Verbraucher unter anderem in dem Bereich Internet und neue Medien mit

einem - durch die Kooperation erzielten - größeren Streuungsgrad zu erreichen. Dies soll u.a. durch den Internetauftritt des Verbraucherschutzes, dem "VerbraucherFenster Hessen" sowie durch die Verteilung von Präventions-Flyern und Broschüren in allen Beratungsstellen bewirkt werden.

Die Landesregierung bietet hessischen Verbraucherinnen und Verbrauchern seit 2003 mit dem Verbraucherportal VerbraucherFenster aktuell und praxisnah umfassende Informationen rund um den Verbraucherschutz. In dem Verbraucherportal der Landesregierung, [www.verbraucherfenster.de](http://www.verbraucherfenster.de) werden Verbraucherinnen und Verbraucher regelmäßig über Smartphones sowie von diesen ausgehenden Gefahren und Risiken in Form von Beiträgen oder Experten-Interviews informiert. So war das Thema auch Gegenstand der Interview-Reihe "Datenklau", die mit einem IT-Experten geführt wurde. Wichtige Hinweise über mögliche Risiken und Gefahren bei Apps wurden hier gegeben. Auch Beiträge wie "Wo die Gefahren bei Apps lauern", "Datenschutz bei Apps", "Check your App" - Datenbank für sichere Apps" griffen das Thema auf, um die Verbraucherinnen und Verbraucher zu sensibilisieren. Via Twitter wird zusätzlich über die wichtigsten Aspekte hinsichtlich Verbraucherschutzinformationen aus diesem Bereich berichtet. Zudem wird auf wissenschaftliche Neuigkeiten in Verbraucherschutzfragen aufmerksam gemacht. Die Angebote des VerbraucherFensters werden auf diesem Wege zusätzlich beworben.

Weitere wichtige Aufklärung in Form von Information und Beratung in diesem Bereich führen die Verbraucherzentrale Hessen und DHB-Netzwerk Haushalt Hessen durch. So hat die Verbraucherzentrale Hessen auf ihrer Homepage ein eigenes Kapitel "Smartphones: Alleskönner mit Risiko" online gestellt. Ein Abschnitt beschäftigt sich explizit mit "Apps und Datenschutz".

Darüber hinaus plant das Ministerium des Innern und für Sport derzeit keine eigenen Maßnahmen zur Aufklärung der Bürgerinnen und Bürger, da die Bundesregierung bereits zielgruppengerecht aufbereitete Informationen auf ihrer Internetseite [www.BSI-fuer-Buerger.de](http://www.BSI-fuer-Buerger.de) anbietet. Auch die Internetangebote der Verbraucherzentralen (Bundesverband, Länder-VZ`en) bieten gute Informationsangebote zu diesem Thema. Die Berichterstattung in den Massenmedien nimmt das Thema ebenfalls regelmäßig und aktuell in verstärktem Maße auf, so dass eigene Maßnahmen des Ministeriums des Innern und für Sport nur unwesentlich zur Verbesserung des Informationsangebotes beitragen würden. Ferner hat das Ministerium des Innern und für Sport in der IMK-Arbeitsgruppe "Cybersicherheit" an der Erstellung eines Leitfadens "Sicherheit mobiler Endgeräte" mitgearbeitet. Der Leitfaden ist an kleinere Behörden sowie kleine mittelständische Unternehmen adressiert und geht allgemein auf das Risiko von Schadsoftware und unerwünschten Funktionen in Apps ein.

Frage 29. Berücksichtigt die Landesregierung bei der Verbraucheraufklärung geschlechtsspezifisches Nutzungsverhalten und Gefahrenpotenziale?

Geschlechtsspezifika beim Nutzungsverhalten und Gefahrenpotenziale in Bezug auf die Verwendung von Smartphone-Apps sind der Landesregierung nicht bekannt. Deshalb nimmt die Landesregierung keine geschlechtsbezogene Information vor.

Aus der täglichen Beratungspraxis der Verbraucherzentrale Hessen sind im Bereich "Gefahren von Smartphone-Apps" bislang keine signifikanten geschlechtsspezifischen Unterschiede erkennbar gewesen.

Auf die Beantwortung auf Frage 132 wird verwiesen.

Frage 30. Berücksichtigt die Landesregierung bei der Verbraucheraufklärung altersspezifisches Nutzungsverhalten und Gefahrenpotenziale?

Altersspezifika beim Nutzungsverhalten und Gefahrenpotenziale in Bezug auf die Verwendung von Smartphone-Apps sind der Landesregierung bisher nicht bekannt.

Altersgruppenspezifische Fragestellungen und daraus resultierende Herausforderungen spielen bei der Ausrichtung der Aufklärungsarbeit und Angebote der Verbraucherzentrale Hessen eine Rolle:

- Die Verbraucherzentralen - so auch die von der Landesregierung geförderte Verbraucherzentrale Hessen - widmen sich 2014 im Rahmen des vom BMJV (zuvor: BMELV) geförderten Projekts "Wirtschaftlicher Verbraucherschutz" dem Thema "Apps" insbesondere mit Blick auf die Überprüfung der Einhaltung einschlägiger Verbraucherschutzgesetze und Datenschutzvorschriften. Weiteres Projekt-Unterthema im Bereich "Digitale Welt" sind die Problemstellungen, die sich bei Online-Spielen ergeben: Zum einen wird ein Großteil dieser Spiele als "free-to-play" mit dem Hinweis auf kostenlose Nutzung angeboten, jedoch ist ein erfolgreiches Spielen nur bei Zukauf diverser Features möglich, die in den Nutzungsbedingungen in der Regel nicht aufgezeigt werden.

- Eine weitere wesentliche Problematik ist laut Verbraucherzentrale Hessen die oft minderjährigen Spieler, die auf diese Art und Weise - über ihr Taschengeld-Budget hinaus und ohne Zustimmung der Eltern - zum Kauf virtueller Güter verleitet werden. Die auf den Spieleseiten befindliche Werbung bringt darüber hinaus vielerlei Risiken mit sich, zumal sie insbesondere für Kinder nicht als solche erkennbar ist. Ein versehentlicher Fingertipp während des Spiels genügt für den Abschluss eines (vermeintlichen) Abo-Vertrages. Die Verbraucherzentrale Hessen will zu den genannten Fragestellungen nicht nur Informations- und Beratungsangebote in den acht örtlichen Beratungsstellen anbieten, sondern auch Informationen in ihrem Internetangebot vorhalten.

Sofern im Zusammenhang mit Smartphone-Apps strafbare Handlungen vorliegen oder gehäuft auftreten, will die Verbraucherzentrale Hessen prüfen, ob dieses Thema Gegenstand von gemeinsamen Präventionsmaßnahmen der Verbraucherzentrale Hessen und der Polizei im Rahmen der Kooperationsvereinbarung zwischen der Verbraucherzentrale und dem Hessischen Landeskriminalamt (LKA) sein kann. Diese wurde Mitte Juli 2014 unterzeichnet.

### Digitale Gewalt

Frage 31. Wie beurteilt die Landesregierung Internetplattformen für Reputationsmanagement für die Verbraucherinnen und Verbraucher?

Die Aggregation frei im Internet verfügbarer Informationen durch hoch spezialisierte Suchmaschinen ist der Kern zahlreicher Dienstleistungen im Internet. Die so bereitgestellten Ergebnisse werden sowohl in der Kreditwirtschaft als auch bei der Personalgewinnung sowie im Marketing vielfältig genutzt. Die Landesregierung empfiehlt deshalb den Nutzerinnen und Nutzern, das durch diese Anbieter erzeugte Bild ihrer Person aktiv zu überwachen, um bei fehlerhaften oder unrechtmäßigen Darstellungen gezielt eingreifen zu können. Das reicht je nach individuellem Bedürfnis von gelegentlichem "Googlen" des eigenen Namens über die regelmäßige Kontrolle der wichtigsten Personensuchmaschinen bis hin zur Inanspruchnahme von Internetplattformen für Reputationsmanagement (e-Reputations-Dienste), die die dafür notwendigen Einzelschritte gegen Entgelt abwickeln und konsolidierte Berichte erstellen.

Frage 32. Wie können diese Plattformen mit Unterstützung der Landesregierung bekannter gemacht werden und dadurch von den Verbraucherinnen und Verbraucher besser genutzt werden?

Da es sich hierbei um privatwirtschaftliche Unternehmen handelt, die mit eigenen Geschäftsmodellen operieren, ist eine pauschale Bewerbung seitens der Landesregierung nicht statthaft. Auch Hinweise auf einzelne Unternehmen sind unter wettbewerbsrechtlichen Gesichtspunkten nicht erlaubt. Die Landesregierung stellt auf der Seite "verbraucherfenster.de" allgemeine Hinweise zum Schutz des eigenen Rufs im Internet bereit.

Frage 33. Wie häufig wurden Internetplattformen für Reputationsmanagement in den letzten fünf Jahren genutzt (bitte nach Jahren aufschlüsseln, falls keine Zahlen vorliegen, bitte schätzen)?

Hierzu liegen der Landesregierung keine Informationen vor.

Frage 34. In welchen Polizeipräsidien in Hessen gibt es so genannte Internetkommissariate?

Internetkommissariate gibt es hessenweit in allen Polizeipräsidien: Nordhessen (Kassel), Osthessen (Fulda), Mittelhessen (Gießen), Westhessen (Wiesbaden), Südosthessen (Offenbach), Südhessen (Darmstadt) und Frankfurt am Main.

Zum Hessischen Landeskriminalamt wird in der Antwort zur Frage 58 gesondert Stellung genommen.

Frage 35. Wie werden die Internetkommissariate durch die Landesregierung unterstützt und weiterentwickelt?

Für die Fortschreibung der technischen Ausstattung der Fachkommissariate sowie der für die Auswertung und Bekämpfung zuständigen Organisationseinheiten des Hessischen Landeskriminalamtes werden jährlich ca. 300.000,- € Mittel zentral zur Verfügung gestellt. Die Eckdaten für den seitens der Landesregierung geplanten Ausbau der Internetkommissariate zu gemeinsamen Cybercrime-Kompetenzzentren mit der Justiz werden derzeit erarbeitet.

Frage 36. Wie unterstützt die Landesregierung Verbraucherinnen und Verbraucher beim Schutz vor digitaler Gewalt?

Die Fragen 36, 38 und 39 werden wie folgt gemeinsam beantwortet:

Das Ministerium für Soziales und Integration unterstützt die Aufklärung von Verbraucherinnen und Verbrauchern über digitale Gewalt, deren strafrechtliche Relevanz, die Möglichkeiten sich zur Wehr zu setzen und diesen Grenzüberschreitungen auch vorzubeugen. Die Unterstützung erfolgt zum Einen finanziell durch die Landesförderung. Beratungsangebote werden von verschie-

denen Einrichtungen geleistet, so von auf Prävention und Schutz vor Gewalt spezialisierten Fachberatungsstellen und der Onlineerziehungsberatung der Bundeskonferenz für Erziehungsberatung (bke). Zum Anderen erfolgt sie auch ideell durch die Bekanntmachung der Fachveranstaltungen und Publikationserzeugnisse dieser Organisationen mittels Internetlinks und durch die Verteilung von Flyern.

In den vergangenen Jahren haben die auf den Schutz vor geschlechtsspezifischer Gewalt spezialisierten Beratungsstellen eine Zunahme des Beratungsbedarfs in Folge digital verübter Gewalt beobachtet. Sie haben daher verschiedene Aufklärungsformen ausgelotet und mit professionellen Werbeagenturen ausgearbeitet, die teils aufgrund ihrer überzeugenden Gestaltung durch Preise ausgezeichnet worden sind. Beispielhaft sind die Printmaterialien und Videoclips der Beratungsstelle Frauennotruf Frankfurt am Main, die in ihrer Eigenschaft als Koordinierungsstelle der hessischen Frauennotrufberatungsstellen die Öffentlichkeitsarbeit für das gesamte Netzwerk verantwortet; die Öffentlichkeitsarbeit der letzten Jahre ist online gebündelt unter: [www.frauennotruf-frankfurt.de/Digitale-Gewalt.55.0.html](http://www.frauennotruf-frankfurt.de/Digitale-Gewalt.55.0.html).

Mittels fachlicher Fortbildungsangebote und kurzen wie auch ausführlichen Flyern und Videospots, die auf YouTube wie auch in Kinovorführungen weit gestreut werden, erreichen diese Aufklärungsinhalte ein breites Spektrum an Fachöffentlichkeit und die anzusprechenden Verkehrskreise im Allgemeinen. Erreicht werden sowohl junge Menschen im Kindes- und Jugendlichen-Alter als auch Erwachsene, gezielt solche, die selbst einen Beitrag zum Schutz vor digitaler Gewalt leisten können: neben Eltern auch Schulpersonal, Sport- und Jugendgruppenleitungen, Arbeitgeber und Arbeitgeberinnen.

Paradoxaerweise erweist sich das Internet als eine der wichtigsten Quellen zum Schutz vor digitaler Gewalt. Zwei wissenschaftliche Untersuchungen zur Belastung von jungen Menschen durch Gewalt in ersten Liebesbeziehungen stellten übereinstimmend fest, dass gewaltbelastete Jugendliche sich allenfalls zu 3 % - von sich aus - an professionelle Beratungseinrichtungen wenden (so die an hessischen Schulen von der Hochschule Fulda durchgeführte Untersuchung Teen Dating Violence, TeDaVi, [http://www.fh-fulda.de/index.php?id=stopp\\_violence](http://www.fh-fulda.de/index.php?id=stopp_violence), und die repräsentative Studie der Eidgenössischen Technischen Hochschule Zürich, Gewalt in jugendlichen Paarbeziehungen, [www.gleichstellung-schweiz.ch](http://www.gleichstellung-schweiz.ch)). Beide Untersuchungen stellten jedoch auch fest, dass an zweiter Stelle, nach dem eigenen Freundeskreis und der eigenen Familie, das Internet als wichtige Quelle von Rat und Unterstützung wahrgenommen wird. Die Landesregierung sieht sich darin bestätigt, dass die Übermittlung von Kenntnissen zum Schutz vor digitaler Gewalt durch ansprechende Angebote im Internet erfolgen soll, zumal so der Bekanntheitsgrad dieser Kenntnisse über Links, soziale Medien und Mundpropaganda gesteigert werden kann.

Das ressortübergreifende Netzwerk gegen Gewalt richtet sich mit seinem Programm Medienkompetenz insbesondere an Erwachsene (Eltern, Lehrkräfte, pädagogische Fachkräfte), um sie über die Möglichkeiten und potenziellen Gefahren neuer Medien aufzuklären. Die Website [www.medienkompetenz.de](http://www.medienkompetenz.de) stellt Informationen, Arbeitsmaterialien und praktische Tipps für den Umgang mit Medien zur Verfügung. Zum Teil werden Inhalte zum Download bereitgehalten, zum Teil wird auf Angebote von Netzwerkpartnern verwiesen. Darüber hinaus wurden in einer zweitägigen Aus- und Fortbildung Lehrkräfte, sozialpädagogische Fachkräfte, Lehramtsstudentinnen und -studenten, Polizeibeamtinnen und -beamte in der polizeilichen Jugendarbeit und Eltern zu Multiplikatorinnen und Multiplikatoren ausgebildet. Die Teilnehmerinnen und Teilnehmer erhielten Informationen zu den Medieninhalten, die Kinder und Jugendliche nutzen, sowie zu den Gefahren, die mit dieser Nutzung verbunden sind bzw. sein können, um diese Informationen an andere Erziehungsverantwortliche weiterzugeben. Ziel ist es, diese Multiplikatorinnen und Multiplikatoren weiterhin zu qualifizieren und noch gezielter einzusetzen.

Darüber hinaus hat das Ministerium des Innern und für Sport das Fraunhofer-Institut für sichere Informationstechnik (Fraunhofer-SIT) 2012 mit einer Studie zu den Risiken Sozialer Netzwerke beauftragt und gemeinsam sowohl eine Studie als auch eine Broschüre (Poller, Andreas/Waldmann, Ulrich, SIT Technical Reports SIT-TR-2013-02 - Soziale Netzwerke bewusst nutzen, Ein Dossier zu Datenschutz, Privatsphärenschutz und Unternehmenssicherheit, Herausgeber Waidner, Michael, August 2013, im Folgenden: SIT Technical Reports SIT-TR-2013-02; [https://www.sit.fraunhofer.de/fileadmin/dokumente/studien\\_und\\_technical\\_reports/Soziale-Netzwerke-2013.pdf](https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Soziale-Netzwerke-2013.pdf)) publiziert, die die wesentlichen Informationen für Nutzerinnen und Nutzer und für die Wirtschaft kurz und präzise mit konkreten Handlungsempfehlungen darstellen.

Frage 37. Wie unterstützt die Landesregierung Opfer von digitaler Gewalt?

Dem Opferschutz kommt in Hessen hohe Bedeutung zu. Bei der Polizei sind bis auf die Ebene der Polizeidirektionen Opferschutzbeauftragte eingesetzt worden, unabhängig davon, welche Straftaten der Opferwerdung zugrunde zu legen sind. Alle Opfer werden gemäß § 406h StPO auf ihre Befugnisse als Verletzte hingewiesen. Dies betrifft unter anderem Entschädigungsmöglichkeiten, verschiedene Antragsbefugnisse und die Unterstützung durch Opferhilfeeinrichtungen. Sowohl im Curriculum der Hessischen Hochschule für Polizei und Verwaltung sowie in

Fortbildungsinhalten der Polizeiakademie Hessen findet sich der Opferschutz als Inhalt angemessen wieder.

Es gibt in Hessen verschiedene Anlaufstellen für Opfer von sogenannter "digitaler Gewalt" (vgl. Hilfe, Beratung und Adressen aus "Mobbing - Ein Wegweiser zur Mobbingprävention und Mobbingintervention in Hessen", S. 17-34). Beispielhaft seien hier die hessenweit tätigen Beratungsstellen Pro Familia, die Landesanstalt für privaten Rundfunk und neue Medien (LPR), das Institut für Medienpädagogik und Kommunikation/Landesfilmdienst Hessen e.V. genannt.

Als unmittelbare Ansprechpartner/-innen für betroffene Schülerinnen und Schüler, wenn der Beratungsbedarf über die Unterstützung durch Lehrkräfte und Sozialpädagoginnen und -pädagogen an den jeweiligen Schulen hinausgeht, gelten unter anderem die Schulpsychologinnen und -psychologen an den 15 Staatlichen Schulämtern.

Frage 38. Wie unterstützt die Landesregierung Vereine, Verbände und sonstige Einrichtungen bei der Beratung von Verbraucherinnen und Verbrauchern zum Schutz vor digitaler Gewalt (bitte aufschlüsseln nach kurz- und langfristigen Maßnahmen und Art der Maßnahme)?

Auf die Antwort zur Frage 36 wird verwiesen.

Frage 39. Wie unterstützt die Landesregierung Vereine, Verbände und weitere Einrichtungen bei der Beratung von Verbraucherinnen und Verbrauchern, die Opfer digitaler Gewalt geworden sind (bitte aufschlüsseln nach kurz- und langfristigen Maßnahmen und Art der Maßnahme)?

Auf die Antwort zur Frage 36 wird verwiesen.

Frage 40. Welche Möglichkeiten sieht die Landesregierung für Internetnutzerinnen und -nutzer, digitale Angriffe zu verhindern und sich gegen digitale Angriffe zu wehren?

Das Internet findet aus technischen Gründen stets weltweit statt. Internetkriminalität weist deswegen per se internationale bis globale Züge auf. Die Aufklärung über aktuell weltweite Internet-Phänomene ist deshalb besonders wichtig. Die hessische Polizei bildet Multiplikatorinnen und Multiplikatoren im Bereich Prävention Cybercrime aus. Über die hessische Polizei werden den Internetnutzern Hinweise für einen Grundschutz der genutzten Endgeräte vermittelt. Diese bestehen regelmäßig aus Tipps zur Passwortsicherheit, der permanenten Aktualisierung der installierten Software (inklusive der dazugehörigen Programme/Applikationen wie Java oder Adobe), der Nutzung eines kostenpflichtigen Antivirenprogrammes, der Einrichtung eines separaten Accounts zur Internetnutzung (ohne Administrationsrechte), der kritischen Beleuchtung von Anfragen unbekannter Absender per E-Mail oder anderer Online-Kommunikationsprogramme (unabhängig von den Endgeräten).

Außerdem sollten sich die Internetnutzerinnen und -nutzer regelmäßig über aktuelle Gefahren und geeignete Gegenmaßnahmen informieren, ihr Nutzerverhalten auf die Gefahrenquellen einstellen, die genutzten Kommunikationsgeräte mit der entsprechenden Sicherheitssoftware ausstatten und die höchsten Sicherheitseinstellungen einstellen.

Im Übrigen wird auf die Antworten zu den Fragen 28 und 36 verwiesen.

Frage 41. Hält die Landesregierung die bestehenden strafrechtlichen Regelungen zur Ahndung digitaler Gewalt für ausreichend?

Ein erhebliches, zuletzt im Rahmen des laufenden Dialogs mit der staatsanwaltlichen und gerichtlichen Praxis identifiziertes Normierungsdefizit, betrifft die Strafbarkeit der Datenhehlerei. Diesbezüglich wurde von Hessen kürzlich ein Gesetzentwurf zur Strafbarkeit der Datenhehlerei (erneut) in den Bundesrat eingebracht und am 14. März 2014 unverändert vom Bundesrat beschlossen. Insoweit wird ergänzend auf die Antworten zu Fragen Nr. 181 und 182 Bezug genommen.

Zudem ist zur Verbesserung der Bekämpfung der Kinderpornografie im Internet der veraltete Schriftenbegriff im Strafrecht zu einen modernen Medienbegriff zu erweitern, was als erster und notwendiger Schritt zur Anpassung des Strafgesetzbuches an die Entwicklungen der digitalen Kommunikation zu verstehen ist. Darüber hinaus ist jedoch eine umfassende Reform des Strafgesetzbuches im Hinblick auf die Realitäten der modernen Kommunikation nötig, da das Strafrecht in vielen Fällen noch den Begrifflichkeiten des letzten Jahrhunderts verhaftet ist und deswegen nicht nur im Bereich der Datenhehlerei Strafbarkeitslücken bestehen.

Frage 42. Falls Frage 41 verneint wird: Wo sieht die Landesregierung Änderungsbedarf?

Es wird auf die Antwort zu Frage 41 verwiesen.

Frage 43. Wie viele Fälle von digitaler Gewalt sind in Hessen in den letzten fünf Jahren insgesamt und pro Jahr bekannt geworden (falls keine exakten Zahlen vorhanden sind, bitte schätzen, und soweit möglich geschlechts- und altersspezifisch aufschlüsseln)?

Der Begriff "digitale Gewalt" ist in der Polizeilichen Kriminalstatistik (PKS) nicht definiert. Es handelt sich um einen unbestimmten (Rechts-)Begriff, der im Zusammenhang mit verschiedenen Straftatbeständen steht - wie beispielsweise:

- § 201a StGB Verletzung des höchstpersönlichen Lebensbereiches durch Bildaufnahmen,
- § 201 StGB Verletzung der Vertraulichkeit, des Wortes,
- § 240 StGB Nötigung,
- § 241 StGB Bedrohung,
- § 223 StGB Körperverletzung,
- § 176 StGB Sexueller Missbrauch.

Eine Spezifizierung über die Polizeiliche Kriminalstatistik ist mangels konkreter Erfassung im Sinne der Fragestellung nicht möglich.

Im Übrigen wird für den Justizbereich auf die Ausführungen zu Frage 44 Bezug genommen.

Frage 44. Wie viele Fälle von digitaler Gewalt sind in Hessen in den letzten fünf Jahren insgesamt und pro Jahr strafrechtlich zur Anzeige gebracht worden und in wie vielen Fällen kam es zu einer Verurteilung bzw. in wie vielen Fällen digitaler Gewalt sind zivilrechtliche Schritte eingeleitet worden (bitte soweit möglich geschlechts- und altersspezifisch aufschlüsseln)?

Das Deliktsfeld "digitale Gewalt" wird in den von der hessischen Justiz geführten Statistiken nicht gesondert erfasst, so dass keine statistischen Daten dazu verfügbar sind. Dies gilt auch, soweit die Einleitung zivilrechtlicher Schritte angesprochen ist.

Zur näheren Erläuterung sowie zur ergänzenden Beantwortung wird auf die Ausführungen in der Vorbemerkung Bezug genommen.

Auf die Antwort zur Frage 43 wird verwiesen.

Frage 45. Welche Ursachen über die bereits genannten hinaus sieht die Landesregierung für die Zunahme digitaler Gewalt?

Digitale Medien sind für einen Großteil der Bevölkerung aus ihrem Alltag nicht mehr wegzu-denken. Insbesondere über moderne Internet-Zugangsgeräte (Smartphone und Tablet-Computer) sind vorwiegend jüngere Menschen fast permanent im Internet präsent ("always-on"). Der Fokus bei der Internetnutzung verschiebt sich immer mehr zur Dauerkommunikation über Online-Communities und Messaging-Dienste. Mit der Verschiebung der Kommunikation in die virtuelle Welt einhergehend sind auch Konflikte sowie Aggressionen und Gewalt bis hin zu strafbarem Verhalten verbunden.

Studien zeigen, dass digitale Gewalt besonders bei 14 bis 17 Jährigen (ca. Jahrgangsstufen 7-10) verbreitet ist. Die Zunahme der technischen Möglichkeiten, gepaart mit der Anonymität im Internet, kann die natürliche Hemmschwelle von potenziellen Täterinnen und Tätern senken.

Frage 46. Welche Maßnahmen zur Aufklärung von Verbraucherinnen und Verbrauchern über digitale Gewalt insgesamt sind der Landesregierung bekannt (bitte aufschlüsseln nach Art der Maßnahme)?

Auf die Antwort zu den Fragen 28 und 36 wird verwiesen.

Frage 47. Welche Vereine, Verbände und weiteren Einrichtungen zur Beratung von Verbraucherinnen und Verbrauchern über digitale Gewalt sind der Landesregierung bekannt?

In Hessen gibt es eine Vielzahl von Initiativen zur Beratung von Verbraucherinnen und Verbrauchern. Im Rahmen des Opferschutzes weist die Polizei auf Opferhilfeeinrichtungen hin. Diese Hilfeeinrichtungen sind in einer polizeilichen Datenbank "Opferhilfeeinrichtungen in Hessen" zusammengefasst und für jede Polizeivollzugsbeamtin und jeden Polizeivollzugsbeamten zugänglich. Opfer von Gewalt, also auch digitaler Gewalt, werden von den Opferberatungsstellen über weitere sinnvolle Maßnahmen beraten, unterstützt durch psychosoziale Prozessbeteiligung, bekommen Rechtsanwälte und Psychotherapeuten vermittelt und werden bei Antragstellungen und Behördengängen unterstützt.

Im Bereich der schulischen Medienbildung kooperiert das Kultusministerium mit bzw. unterstützt eine Reihe von außerschulischen Partnern, die die schulischen Jugendmedienschutzmaß-

nahmen durch Initiativen bzw. Projekte ergänzen und in diesem Zusammenhang auch dazu beitragen, dass Schülerinnen und Schüler über das Thema digitale Gewalt aufgeklärt werden. Zu nennen sind hier an erster Stelle die Medienanstalt Landesanstalt für privaten Rundfunk und Neue Medien (LPR) sowie der Hessische Rundfunk (HR), die durch ihre medienpädagogischen Projekte die schulische Medienerziehung fördern. Darüber hinaus bestehen auch Kooperationen mit Vereinen. Zu nennen ist hier beispielhaft das Projekt "Cool and Safe" des Vereins SMOG e.V. Dieses bietet ein webbasiertes Trainingsprogramm für Grundschulkinder an, um ihnen Handlungsoptionen zum Schutz vor Übergriffen aufzuzeigen und sie im Hinblick auf Gefahren - auch im Internet - zu sensibilisieren. Das Angebot wird an hessischen Grundschulen umgesetzt.

Im Rahmen des Pilotprojekts "Digitale Helden", einem Peer-Education-Programm, das durch den Verein "Sicher Dein Web" konzipiert wurde und durch das Kultusministerium unterstützt wird, stellen Schülerinnen und Schüler (Klassen 7 bis 9) ihre Erfahrungen und Ausbildung im Bereich des Jugendmedienschutzes jüngerer Schülerinnen und Schülern zur Verfügung. Betreut werden die Digitalen Helden dabei von Lehrkräften sowie externen Mentorinnen und Mentoren. Das Programm läuft in der derzeitigen Pilotphase zunächst an Frankfurter Schulen. Eine Ausweitung ist in Planung.

Das regionale Projekt "Medienschouts" im Rheingau-Taunus-Kreis und in Wiesbaden verfolgt einen ähnlichen Ansatz wie "Digitale Helden". Seit dem Jahr 2011 werden Schülerinnen und Schüler ab der Klasse 9 und die sie betreuenden Lehrkräfte durch die Fachberatung Medienbildung des Staatlichen Schulamtes in Arbeitsgemeinschaften aus- und fortgebildet.

Frage 48. Welche Maßnahmen zur Aufklärung von Verbraucherinnen und Verbrauchern über digitale Gewalt insgesamt betreibt oder unterstützt die Landesregierung (bitte aufschlüsseln nach Art und Träger der Maßnahme sowie Umfang und zeitliche Dauer der Unterstützung)?

Die Aufklärung über digitale Gewalt erfolgt in der schulischen Bildung vornehmlich im Bereich des Jugendmedienschutzes. Das Kultusministerium baut seine Aktivitäten im Bereich des Jugendmedienschutzes angesichts der zunehmenden Kommunikation über das Internet stetig aus, um Schulen umfassende Unterstützungsmaßnahmen zu bieten.

Der Jugendmedienschutz ist im Unterstützungssystem für Schulen durch einen Landeskoordinator sowie jeweils einen Ansprechpartner in jedem Staatlichen Schulamt aus dem Kreis der Schulpsychologen/-innen oder der Fachberater/-innen Medienbildung verankert.

Im vergangenen Schuljahr startete unter Leitung des Landeskoordinators ein Programm, mit dem in mehrtägigen Fortbildungsreihen landesweit Lehrkräfte zu Jugendmedienschutzberaterinnen und -beratern als Multiplikatoren für ihre Schulen qualifiziert wurden. Diese Fortbildungsreihe wird im kommenden Schuljahr fortgesetzt.

Im Rahmen der Medieninitiative Schule@Zukunft finden Fortbildungsangebote zum Thema Jugendmedienschutz für Lehrkräfte statt. Diese werden durch das Landesschulamt (LSA) entwickelt und angeboten. Zusammen mit dem LSA werden für jedes Schulhalbjahr regionale Fortbildungen für Lehrkräfte bereitgestellt.

Auf dem Hessischen Bildungsserver wird eine Webseite gepflegt, die Lehrkräften, Schülerinnen und Schülern sowie Eltern aktuelle Informationen, Links zu Beratungsstellen und Seiten anderer Institutionen bereitstellt. Für Lehrkräfte werden darüber hinaus Unterrichtsmaterialien und Fortbildungen zum Thema Jugendmedienschutz angeboten.

Ende des vergangenen Jahres ist ein Informationspaket zum Jugendmedienschutz an alle hessischen Schulen versandt worden. Darin wurde ein Überblick über bestehende Maßnahmen und Ansprechpartner gegeben. Enthalten war auch ein Informationsschreiben zum Umgang der Schulen mit dem aktuellen Phänomen "Sexting".

Eine Handreichung zum Jugendmedienschutz für Lehrkräfte ist in Arbeit und soll im Laufe dieses Schuljahres erscheinen. Darin werden u.a. Informationen zum Umgang mit Sozialen Netzwerken im schulischen Kontext, Cybermobbing, Handys an Schulen enthalten sein sowie eine Übersicht über geeignete Unterrichtsmaterialien für Lehrkräfte angeboten.

Neben dieser landesinternen Struktur kooperiert das Kultusministerium mit externen Medienpartnern und weiteren Institutionen, die den Jugendmedienschutz an Schulen unterstützen.

Die Landesanstalt für privaten Rundfunk und neue Medien (LPR) bietet eine Reihe von Projekten und Programmen zum Jugendmedienschutz an Schulen an. Viele dieser Maßnahmen richten sich an Schülerinnen und Schüler, Lehrkräfte und Eltern, unter anderem handelt es sich um schulische Projekttag zu den Themen des Jugendmedienschutzes.

Im vergangenen Schuljahr startete das Kooperationsprojekt "Internet ABC" für hessische Grundschulen, das insbesondere den jungen Schülern sicheres Surfen und die Grundregeln

im Umgang mit dem Internet vermitteln soll. Auch in dieses Projekt sind Eltern durch Elternabende einbezogen worden. Seitens des Kultusministeriums wird das Projekt durch die Fachberater Medienbildung der Staatlichen Schulämter durch Fortbildungen für die Lehrkräfte und pädagogische Unterrichtsmaterialien unterstützt.

Der Hessische Rundfunk (HR) hat im Jahr 2012 im Rahmen seiner Reihe Funkkolleg das Thema Medien behandelt und sich in diesem Zusammenhang auch mit den Gefahren des Internets auseinandergesetzt. Entsprechende Begleitmaterialien für Lehrkräfte wurden durch das Kultusministerium unterstützt und stehen online zur Verfügung.

Das Virtuelle Zentrum für Lehrerbildung der Universität Marburg bietet neben einer Reihe von Fortbildungen zur Mediennutzung und zum Einsatz von Neuen Medien im Unterricht auch eine Online-Fortbildung zum Jugendmedienschutz an. Die Fortbildungen stehen im Rahmen einer phasenübergreifenden Lehrerbildung hessischen Lehrkräften aller Ausbildungsphasen kostenlos zur Verfügung.

Die Landesregierung hat über das Netzwerk gegen Gewalt das Peer-Education-Programm "Digitale Helden" des Vereins "Sicher dein Web e.V." mitinitiiert. "Digitale Helden" ist ein schulisches Mentorenprogramm unter anderem zur Prävention von Onlinemobbing. Sozial engagierte Schülerinnen und Schüler der Jahrgangsstufen 7 bis 9 werden von Medienpädagogen zu "Digitalen Helden" ausgebildet. Mit ihrem Know-how können sie ihre Mitschülerinnen und Mitschüler im Umgang mit dem Internet beraten. Das Programm wird in Kooperation mit dem Hessischen Kultusministerium (HKM) aktuell an neun Pilotschulen umgesetzt.

Im Übrigen wird auf die Antwort zur Frage 36 verwiesen.

### Phishing und Identitätsdiebstahl

Frage 49. Wie viele Fälle von Phishing sind in Hessen in den letzten fünf Jahren bekannt geworden (falls keine exakten Zahlen vorhanden sind, bitte schätzen, und soweit möglich geschlechtsspezifisch aufschlüsseln)?

In der Polizeilichen Kriminalstatistik sind folgende Fälle erfasst:

Jahr	2009	2010	2011	2012	2013
erfasste Fälle	nicht erfasst	1.312	1.849	1.426	638

Im Übrigen wird für den Justizbereich auf die Ausführungen zu Frage 52 Bezug genommen.

Frage 50. In wie vielen der unter Frage 49 aufgeführten Fälle kam es zu einer Verurteilung?

Frage 51. Welcher Schaden entstand im Zeitraum der letzten fünf Jahre durch Phishing (falls keine Zahlen vorliegen, bitte schätzen)?

Die Fragen 50 und 51 werden zusammen beantwortet.

In der Polizeilichen Kriminalstatistik sind folgende Fälle erfasst:

Jahr	2009	2010	2011	2012	2013
Schaden	nicht erfasst	1.958.522 €	2154.643 €	1.360.720 €	642.576 €

Im Übrigen wird für den Justizbereich auf die Ausführungen zu Frage 52 Bezug genommen.

Frage 52. Lassen sich aus der Entwicklung der Fallzahlen und der Entwicklung der entstandenen Schäden Tendenzen ableiten, dass die Bedeutung des Themas "Phishing" nachlässt, zunimmt oder annähernd gleich bleibt?

Die Bewertung aller Indikatoren lässt keinen rückläufigen Trend erkennen. Der in der Polizeilichen Kriminalstatistik ausgewiesene Rückgang im Vergleich zum Jahr 2012 resultiert wesentlich auf geänderten Erfassungsmodalitäten bei Auslandsstraftaten. Bezogen auf den Missbrauch im Online-Banking ist festzustellen, dass der erfolgreiche missbräuchliche Einsatz von "abgephisheten" Daten bei der Einführung neuer Sicherheitsmechanismen jeweils kurzfristig abnimmt und nach Anpassung der Tatbegehungsweise auf Täterseite wieder zunimmt. Die Tatbegehungsweise stellen dabei in der Regel eine Kombination aus technischem Angriff (Schadprogrammen) und betrügerischen Aspekten (Schwachstelle Mensch) dar. Ein Bedeutungsverlust des "Phishing" ist insgesamt auch deshalb nicht zu erwarten, weil die Täter bereits zum jetzigen Zeitpunkt über immense Datenmengen verfügen, die bisher noch nicht zum Einsatz kamen.

Das Deliktsfeld "Phishing" wird in den von der hessischen Justiz geführten Statistiken nicht gesondert erfasst, so dass keine statistischen Daten hierzu verfügbar sind. Dies liegt daran, dass

für Ermittlungsverfahren wegen Phishings bundesweit keine einheitliche Eintragungspraxis existiert und Phishing mithin unter verschiedenen Strafnormen wie z.B. §§ 263, 263a, 202a, 269 StGB etc. erfasst wird.

Unabhängig davon kann aus einer Vielzahl von Verfahren zu Frage 52 festgestellt werden, dass das Erlangen von Daten, die anschließend zu kriminellen Handlungen (z.B. Warenbetrug) genutzt werden, zu den hauptsächlichen Straftaten im Bereich Internetkriminalität gehört. Die Bedeutung dieser Kriminalitätsform ist gleichbleibend hoch.

Zur näheren Erläuterung sowie zur ergänzenden Beantwortung wird im Übrigen auf die Ausführungen in der Vorbemerkung Bezug genommen.

Frage 53. Welche Maßnahmen zur Aufklärung von Verbraucherinnen und Verbrauchern über das Problem "Phishing" sind der Landesregierung bekannt (bitte aufschlüsseln nach Art und Träger der Maßnahme)?

Die Landesregierung bietet hessischen Verbraucherinnen und Verbrauchern seit 2003 mit dem Verbraucherportal VerbraucherFenster aktuell und praxisnah umfassende Informationen rund um den Verbraucherschutz. In dem Verbraucherportal der Landesregierung, [www.verbraucherfenster.de](http://www.verbraucherfenster.de) wurden Verbraucherinnen und Verbraucher bereits mehrfach über das Thema "Phishing" durch Interviews mit Experten und informative Beiträge informiert und über Gefahren aufgeklärt - so etwa im Rahmen der Interview-Serie "Datenklau", die mit einem IT-Experten geführt wurde. Zudem wurde ein Experteninterview mit einer Vertreterin des Bundesamtes für Sicherheit in der Informationstechnik unter dem Titel "Phishing - Wie schütze ich vertrauliche Daten?" geführt. Die Verbraucherin oder der Verbraucher erhält hier praktische Handlungsanweisungen, um bewusst mit entsprechenden Mails umzugehen. Weitere Beiträge, unter anderem "Achtung Identitätsdiebstahl: Betrüger setzen Schadsoftware für Datendiebstahl ein", "Internet-Kriminalität - So schützen Sie sich" und "Phishing-Radar: Online-Forum gegen betrügerische E-Mails" runden das Angebot im VerbraucherFenster ab. Via Twitter wird über die wichtigsten Aspekte hinsichtlich Verbraucherschutzinformationen zusätzlich berichtet. Die Angebote des VerbraucherFensters [www.verbraucherfenster.de](http://www.verbraucherfenster.de) werden auf diesem Wege zusätzlich beworben.

Die von der Landesregierung finanziell geförderte Verbraucherzentrale Hessen leistet Aufklärung durch persönliche und telefonische Beratung, schriftliche Verbraucherinformationen sowie durch entsprechende Presse- und Öffentlichkeitsarbeit (siehe Presseveröffentlichung vom 12. Juni 2014, <http://www.verbraucher.de/erneut-viele-gefaelschte-rechnungen-im-umlauf>).

Bereits seit Jahren informiert die Verbraucherzentrale zu den Themen "Datenschutz/-sicherheit" und "Datensparsamkeit" - häufig auch im Rahmen von Projekten. Auf ihrer Website werden ausführliche Hilfestellungen zum Thema Phishing geboten, vor allem über das so genannte Phishing Radar (<http://www.verbraucher.de/phishing-radar>). Hier erhalten Verbraucher Informationen, Antworten auf häufig gestellte Fragen sowie Tipps zur Sicherheit beim Online-Banking. Weiterhin werden tagesaktuell die neuesten Phishing-Maschen dargestellt. Das Phishing-Radar wurde von den Verbraucherzentralen Ende 2010 mit Förderung des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) im Rahmen des Projekts "Interaktives Internetangebot zu Finanzmarktthemen (Phishing-Radar)" initiiert. Während der 33-monatigen Laufzeit des Projekts wurden von Verbraucherinnen und Verbrauchern und anderen Multiplikatoren mehr als 65.000 E-Mails weitergeleitet. Die Zahl der täglich eingehenden E-Mails ist dabei jedes Jahr gestiegen. Dieses Phishing-Radar hat sich als großer und nachhaltiger Erfolg erwiesen und wird daher von der Verbraucherzentrale Nordrhein-Westfalen weitergeführt. Inhalte und Warnmeldungen werden in die Webseiten anderer Verbraucherzentralen - so auch in den Internetauftritt der Verbraucherzentrale Hessen - eingebunden.

Zudem informiert und klärt der DHB-Netzwerk Haushalt Hessen zu diesem Themenkomplex bei Vorträgen und Informationsveranstaltungen auf.

Neben den grundsätzlichen Aufklärungskampagnen bildet die hessische Polizei Multiplikatorinnen und Multiplikatoren im Bereich Prävention Cybercrime aus. In diesem Rahmen wird gemäß der Standards polizeilicher Kriminalprävention der hessischen Polizei auf grundsätzliche Gefahren an Beispielen aktueller Phänomene aus dem Bereich Cybercrime eingegangen. Die Thematik Phishing bildet einen Schwerpunkt. Weiterhin wird bei Bekanntwerden aktueller Erscheinungsformen in diesem Bereich die Bevölkerung über die Medien (Presse/Internet) zeitnah auf die Thematik hingewiesen.

Konkret sind darüber hinaus nachstehende Beratungsangebote des BSI ([www.bsi-fuerbuerger.de](http://www.bsi-fuerbuerger.de)) sowie der Länder-Polizeien bekannt:

- <http://www.polizei.hessen.de/icc/internetzentral/nav/20c/20c7018a-7eac-9f31-1035-1d240ef798e7.htm>,
- <http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/hishing.html>

- und zahlreiche Jugendschutz-Seiten im Internet (z.B. die der EU-Initiative [www.klicksafe.de](http://www.klicksafe.de)).

Ferner bieten praktisch alle Online-Banking-Anbieter und großen Online-Versandhändler Informationen zum Thema Phishing an.

Frage 54. Welche Maßnahmen zur Aufklärung von Verbraucherinnen und Verbrauchern über das Problem Phishing betreibt oder unterstützt die Landesregierung (bitte aufschlüsseln nach Art und Träger der Maßnahme sowie Form der Unterstützung)?

Die Polizei verfügt in jedem Präsidium und im LKA über einen Cybercrime-Fachberater, der neben den grundsätzlichen Gefahren des Internets auch immer über spezielle und aktuelle Kriminalitätsphänomene wie zum Beispiel das Phishing im Rahmen von Infoveranstaltungen/Vorträgen aufklärt.

Darüber hinaus betreibt das Ministerium des Innern und für Sport selbst keine Maßnahmen zur Aufklärung von Verbraucherinnen und Verbrauchern. Im Rahmen des weiteren Ausbaus des CERT-Hessen sollen auf den Webseiten des CERT-Hessen Verweise zu bestehenden Informationsangeboten Dritter sowie zu aktuellen Bedrohungen veröffentlicht werden. Die Informationsangebote des CERT-Hessen werden dann auch Verbraucherinnen und Verbrauchern sowie kleinen und mittleren Unternehmen (KMUs) zur Verfügung stehen.

Im Übrigen wird auf die Antwort zu den Fragen 28 und 53 verwiesen.

Frage 55. Gibt es geschlechts- oder altersspezifische Maßnahmen zur Aufklärung von Verbraucherinnen und Verbrauchern über das Problem Phishing?

Das Phänomen "Phishing" betrifft Personen unterschiedlichen Alters und Geschlechts, weshalb keine Unterschiede bei den Aufklärungsmaßnahmen gemacht werden.

Geschlechts- oder altersspezifische Maßnahmen in diesem Bereich wurden auch seitens der Verbraucherzentrale Hessen bislang nicht betrieben.

Frage 56. Wie sollten aus Sicht der Landesregierung Maßnahmen zur Aufklärung von Verbraucherinnen und Verbrauchern über das Problem "Phishing" auch an das mobile Kommunikationsverhalten (z.B. Smartphone- oder App-Angebote) der Nutzerinnen und Nutzer angepasst werden?

Smartphones und Tablets spielen mittlerweile eine wichtige Rolle bei der E-Mail-Kommunikation und der Kommunikation in sozialen Netzwerken. Insbesondere werden mobile Endgeräte auch beim Online-Banking und Mobile Payment verwendet. Eine Information und Aufklärung über Phishing und Phishing-Attacken ist daher wichtig.

Am 28. Dezember 2010 haben die Verbraucherzentralen der Länder mit Förderung des BMELV das Projekt "Interaktives Internetangebot zu Finanzmarktthemen" gestartet (Phishing-Radar). Verbraucherinnen und Verbraucher können Phishing-E-Mails an eine Adresse der Verbraucherzentrale Nordrhein-Westfalen weiterleiten. Die zugesandten Phishing-E-Mails werden vollständig in eine Übersicht eingestellt. Per Twitter und einer Übersichtsseite [phishing@vz-nrw.de](mailto:phishing@vz-nrw.de) wird täglich vor den aktuell kursierenden Attacken gewarnt.

Die hessische Polizei bezieht in die Thematik Phishing im Rahmen der in der Antwort zu Frage 53 erläuterten Maßnahmen auch die Problematiken mobiler Endgeräte (Tablets, Phablets und Smartphones) mit ein. Darüber hinaus werden zurzeit durch die hessische Polizei die Rahmenbedingungen für die Nutzung Sozialer Netzwerke, insbesondere Facebook und Twitter, auch für die polizeiliche Kriminalprävention erarbeitet. So soll versucht werden, interaktiv bisher noch nicht erreichte Zielgruppen für die Vermittlung präventiver Informationen zu erschließen.

Im Allgemeinen sollen Beratungs- und Informationsangebote im Bereich der Prävention zielgruppengerecht gestaltet werden.

Frage 57. Sieht die Landesregierung die Notwendigkeit, dass Banken über sichere Standards verfügen und ihre Kunden über Risiken in Bezug auf Phishing informieren?

Die Sicherung der netzbasierenden E-Banking-Lösungen ist Aufgabe der diesen Service anbietenden Banken. Eine regelmäßige Überprüfung der aktuellen Sicherheitstechniken und Anpassung an neue Formen der Online-Kriminalität muss zwingend vorausgesetzt werden und sollte standardisiert erfolgen. Da bei erfolgreichen Phishing-Angriffen oftmals Fehler beim Bankkunden die Tatbegehung ermöglicht haben, erscheint eine Sensibilisierung einer breiten Öffentlichkeit zum Kriminalitätsphänomen Phishing auch durch die Polizei weiterhin zielführend.

Frage 58. Welche Veränderungen hat es innerhalb des LKA seit 2010 im Zusammenhang mit dem Kampf gegen Cybercrime gegeben?

2011 wurden zunächst wesentliche Arbeitsbereiche zur Bekämpfung von Cybercrime in der neu konzipierten Abteilung 3 des HLKA "IuK-Einsatz und Cybercrime" gebündelt. Dies gewährleistet einen schnellen und effektiven Zugriff auf die Ressourcen der Zentralen Einsatz- und Operativtechnik, der Telekommunikationsüberwachung, der digitalen Forensik und der Cybercrime-Ermittlungseinheiten und minimiert organisatorische Schnittstellen. Mit dieser dem Phänomen "Cybercrime" angepassten organisatorischen Weiterentwicklung des HLKA ging eine personelle Verstärkung dieser Fachabteilung des HLKA einher. Aktuell sind dort mehr als 70 IT-Experten, Informatiker und Fachingenieure tätig. Darüber hinaus wurde in der Abteilung 1 des HLKA, bei der Zentralstelle Kriminal- und Verkehrsprävention, der Bereich Prävention Cybercrime aufgebaut. Hier wird in enger Zusammenarbeit und Abstimmung mit der Fachabteilung 3 sowie den für Prävention zuständigen Sachbereichen in den Stäben der Flächenpräsidien die Lage hinsichtlich aktueller Phänomene aus dem Bereich Cybercrime analysiert und in konkrete Präventionsmaßnahmen umgesetzt.

Frage 59. Wie wirken sich die in Frage 58 benannten Maßnahmen auf den Bereich "Phishing" aus?

Unmittelbare Auswirkungen der organisatorischen Anpassungen des Hessischen Landeskriminalamtes auf das Fallaufkommen im Phänomenbereich Phishing lassen sich nicht belegen. Globale Kriminalitätsphänomene können erfahrungsgemäß nicht ausschließlich durch Organisationsentwicklungen einzelner Behörden wirksam und nachhaltig eingedämmt werden. Durch die Ressourcenbündelung in der Abteilung 3 und die enge Zusammenarbeit mit dem Bereich Prävention Cybercrime wurde jedoch eine unverzügliche Reaktion auf die sich schnell wandelnden Phänomene der Cybercrime möglich. Die thematische und personelle Bündelung stellt somit eine wesentliche Voraussetzung dar, um deliktsspezifische ganzheitliche Konzepte (u. a. gegen Phishing) zu erarbeiten, auf Bundesebene abzustimmen/fortzuentwickeln sowie zeitnah umzusetzen. Die hessische Polizei leistet somit einen wichtigen Beitrag zur Bekämpfung von Cybercrime.

Frage 60. Wie viele Fälle von Identitätsdiebstahl sind in den letzten fünf Jahren bekannt und zur Anzeige gebracht worden?

Sachverhalte, die im allgemeinen Sprachgebrauch als "Identitätsdiebstahl" bezeichnet werden, werden in der Polizeilichen Kriminalstatistik (PKS) nicht erfasst. Die illegale Erlangung personenbezogener Daten über Datenetze stellt regelmäßig ein Ausspähen von Daten gegebenenfalls in Verbindung mit einer Datenveränderung dar. Bei den bekannt gewordenen und in der PKS erfassten Fällen handelt es sich um die des Phishing (hierzu wird auch auf die Antwort zu den Fragen 49 und 50 verwiesen). Die widerrechtliche Erlangung personenbezogener Daten erfolgt in der Regel durch Schadprogramme (sogenannte Trojaner). Die eingesetzten Schadprogramme zielen neben bankspezifischen Daten auch auf Zugangsdaten zu Online-Shops, Sozialen Netzwerken, E-Mail-Accounts und Messenger-Diensten ab. Die Nutzer der infizierten Rechner bemerken die Tat in der Regel erst dann, wenn die erlangten Zugangsdaten widerrechtlich zum Einsatz kommen. Der Großteil der erlangten personenbezogenen Daten ("Identitätsdiebstahl") bleibt somit unerkannt, wird nicht zur Anzeige gebracht und fließt daher nicht in polizeiliche Statistiken ein. Es ist von einem hohen Dunkelfeld auszugehen.

Im Übrigen wird für den Justizbereich auf die Ausführungen zu Frage 61 Bezug genommen.

Frage 61. Wie viele Verurteilungen in Zusammenhang mit den in Frage 60 benannten Taten gab es?

Fälle von Identitätsdiebstahl werden in der hessischen Justiz statistisch nicht gesondert erfasst, so dass sich valide Aussagen anhand von Zahlenmaterial hierzu nicht treffen lassen. Es ist jedoch nach dem Bericht der Generalstaatsanwaltschaft Frankfurt am Main allgemein im Bereich Internetkriminalität von einer sehr hohen Zahl an Geschädigten auszugehen.

Zur näheren Erläuterung sowie zur ergänzenden Beantwortung wird auf die Ausführungen in der Vorbemerkung Bezug genommen.

Frage 62. Welche Maßnahmen zur Aufklärung und Sensibilisierung der Verbraucherinnen und Verbraucher in Bezug auf den achtsamen Umgang mit Passwörtern unternimmt und plant die Landesregierung?

Durch mediale Veröffentlichungen weist die hessische Polizei regelmäßig auf diese Thematik hin. Dies geschieht entweder anlassbezogen beim Bekanntwerden aktueller Sicherheitslücken in Betriebssystemen oder Anwendungssoftware oder in unregelmäßigen Abständen, wenn neue Tatbegehungsweisen bekannt werden und dadurch höhere Anforderungen an die Sicherheit, z.B. von Passwörtern, durch die Polizei festgestellt werden.

Im Bereich der schulischen Bildung ist die Aufklärung über den achtsamen Umgang mit Passwörtern bei der digitalen Kommunikation Teil der meisten Projekte und Maßnahmen im Rah-

men des Jugendmedienschutzes für Schülerinnen und Schüler sowie in den einschlägigen Fortbildungsangeboten für Lehrkräfte.

Darüber hinaus sollen alle Lehrkräfte durch eine Handreichung über den sicheren und kritischen Umgang mit Sozialen Netzwerken informiert werden. In diesem Zusammenhang werden sie auch auf einen achtsamen Umgang mit Passwörtern hingewiesen und angeleitet, dies den Schülerinnen und Schülern im Unterricht zu vermitteln.

Die Landesregierung bietet zudem hessischen Verbraucherinnen und Verbrauchern seit 2003 mit dem Verbraucherportal [www.verbraucherfenster.de](http://www.verbraucherfenster.de) aktuell und praxisnah umfassende Informationen rund um den Verbraucherschutz. In dem Verbraucherportal werden Verbraucherinnen und Verbraucher regelmäßig über sichere Passwörter sowie deren Erstellung aufgeklärt, u.a. in den Beiträgen "Sicherheit im Internet: Die besten Passwort-Tipps", "Identitäten-Diebstahl im Internet - Worauf Verbraucher jetzt achten sollten".

Die von der Landesregierung finanziell geförderte Verbraucherzentrale Hessen gibt zusätzlich Tipps. In dem Online-Beitrag "Passwörter sicher gestalten - ein Muss für jeden Internetnutzer" <http://www.verbraucher.de/passwoerter-sicher-gestalten> findet die Verbraucherin und der Verbraucher wertvolle Hinweise und Tipps.

Im Übrigen wird auf die Antwort zur Frage 28 verwiesen.

Frage 63. Welche Gefahren sieht die Landesregierung bei Identitätsdiebstahl von Profilen auf Plattformen (z.B. eBay) und in Sozialen Netzwerken (z.B. Facebook, Twitter)?

Soziale Netzwerke sind für Teile der Bevölkerung ein fester Bestandteil der Lebensführung geworden. Dabei geben die User in nicht unerheblichem Umfang auch sensible und persönliche Daten preis. Dies birgt grundsätzlich die Gefahr des Missbrauchs und sollte daher sorgfältig abgewogen werden. Eine dieser Gefahren ist der Identitätsdiebstahl, bei dem die missbräuchliche Erlangung oder rechtswidrige Nutzung personenbezogener Daten durch Dritte erfolgt - beispielsweise für die betrügerische Verschaffung eines Vermögensvorteils oder zur Diskreditierung und Diffamierung. Durch die Nutzung fremder Identitäten kann es zu wirtschaftlichen Schäden und psychischen Beeinträchtigungen für das Opfer kommen.

Grundsätzlich sieht die Landesregierung Identitätsdiebstahl und den damit verbundenen generellen Vertrauensverlust in eCommerce sowie die Integrität Sozialer Netzwerke als große Herausforderungen an. Nur wenn Kommunikations- und Transaktionspartner darauf vertrauen können, dass die Identität ihres Gegenübers gewährleistet ist, lassen sich die Potentiale digitaler Medien und Dienste ausschöpfen. Die Bundesregierung hat mit dem neuen Personalausweis und der eID-Funktion eine datenschutzfreundliche und sichere Lösung geschaffen, mit der die Identität einer Partei auch im Internet verlässlich nachgewiesen werden kann.

Frage 64. Welche Maßnahmen zur Aufklärung der Verbraucherinnen und Verbraucher ergreift die Landesregierung in Bezug auf Angriffe auf Profildaten?

Die Landesregierung sensibilisiert die Verbraucherinnen und Verbraucher auf vielfältige Art und Weise für einen vorsichtigen Umgang mit Daten und Passwörtern.

Das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz hat in der Vergangenheit mehrfach durch Pressemitteilungen zur Datensparsamkeit in Sozialen Netzwerken und zu einem umsichtigen Umgang mit persönlichen Daten aufgerufen. Weiterhin hat das Onlineportal VerbraucherFenster über den Umgang mit Daten aufgeklärt, unter anderem ausführlich in der Interview-Serie "Datenklau" und den Einzelbeiträgen "Datenschutzverstöße bei dem Sozialen Netzwerk Facebook", "Datenschutz bei Apps", "Identitäten-Diebstahl im Internet - Worauf Verbraucher jetzt achten sollten". Via Twitter wird über die wichtigsten Aspekte hinsichtlich Verbraucherschutzinformationen zusätzlich berichtet. Zudem wird auf wissenswerte Neuigkeiten in Verbraucherschutzfragen aufmerksam gemacht. Die Angebote des VerbraucherFensters [www.verbraucherfenster.de](http://www.verbraucherfenster.de) werden auf diesem Wege zusätzlich beworben.

Auch die Verbraucherzentrale Hessen greift bei der Beratung und Information das Thema regelmäßig auf, online unter anderem in den Beiträgen "Sicheres Surfen in sozialen Netzwerken: Mit persönlichen Daten und Reizen geizen", "Facebook: Missbrauch persönlicher Daten", "Datenmissbrauch: Selbsthilfe bei unzureichendem Schutz". Zudem hat die Verbraucherzentrale den Ratgeber "Meine Daten gehören mir" aufgelegt.

Im Übrigen wird auf die Antworten zu den Fragen 40 und 62 verwiesen.

Frage 65. Sieht die Landesregierung aufgrund der in Frage 64 angesprochenen Problematik den Bedarf, geschlechts- und altersspezifische Aufklärungsmaßnahmen durchzuführen?

Die Landesregierung sieht im Zusammenhang mit der in Frage 64 angesprochenen Problematik keinen Bedarf für geschlechtsspezifische Aufklärungsmaßnahmen. Ihr liegen keine belastbaren

Studien vor, nach denen Frauen und Männer ungleich von Angriffen auf ihre Profildaten betroffen sind. Aufgrund der intensiven Nutzung des Internets und speziell Sozialer Netzwerke durch Kinder, Jugendliche und Heranwachsende erscheint es sinnvoll, die allgemeine Medienkompetenz bereits in der schulischen Ausbildung weiter zu stärken und dabei besonders auf die altersspezifischen Risiken für Kinder und Jugendliche (z.B. Cyber-Grooming, Cyber-Mobbing, Sexting) im Internet einzugehen.

Alle Maßnahmen im Schulbereich sind altersgerecht ausgerichtet.

### Abmahnungen

Frage 66. Wie beurteilt die Landesregierung Abmahnfälle, in denen die Schadensersatzforderungen in keinem Verhältnis zum Ausmaß des Rechtsverstoßes stehen (im Folgenden als missbräuchliche Abmahnungen bezeichnet)?

Die Landesregierung sieht derartige Fälle sehr kritisch. Im Schadensersatzrecht gilt der Grundsatz der Totalreparation - es sind lediglich die Schäden, die tatsächlich entstanden sind, vollständig auszugleichen. Nach § 249 Abs. 1 BGB ist der Zustand wiederherzustellen, der bestehen würde, wenn der zum Ersatz verpflichtende Umstand nicht eingetreten wäre. Ein Schadensersatz ist im deutschen Recht, anders als im anglo-amerikanischen Raum, nicht vorgesehen. Dies ist bei der Bemessung der Schadensersatzhöhe zu berücksichtigen.

Viele Verbraucherinnen und Verbraucher, die zumeist Kinder und Jugendliche sind, begehen Urheberrechtsverletzungen im Internet nicht wissentlich. Sie teilen in Sozialen Netzwerken ein Musikvideo oder ein künstlerisches Werk ohne zu wissen, dass dies gegen Urheberrechte verstößt.

Es ist unstrittig, dass Urheberrechte schützenswert sind und Verletzungen zum Schutz des Künstlers geahndet werden müssen. Aufgrund des oft fehlenden Vorsatzes der Urheberrechtsverletzer sollten die Abmahnkosten bei der ersten Urheberrechtsverletzung jedoch gering sein.

Frage 67. Welche Maßnahmen beabsichtigt die Landesregierung mit Blick auf missbräuchliche Abmahnungen bei Urheberrechtsverletzungen zu ergreifen?

Die Landesregierung setzt sich für ein Urheberrecht ein, das auch im Internet einen fairen Interessenausgleich zwischen Nutzern und Urhebern garantiert, so dass auch im digitalen Zeitalter die Rechte der Schöpfer an ihrem Werk vergütet und gesichert werden und gleichzeitig Werknutzern eine zeitgemäße Nutzung ermöglicht wird.

Eine der großen Herausforderungen ist es, das Urheberrecht an die veränderten Rahmenbedingungen der digitalen Welt anzupassen und die damit verbundenen kulturellen und wirtschaftlichen Potenziale auszuschöpfen. Hierbei spielen die Belange der Verbraucherinnen und Verbraucher als Nutzer der modernen Medien eine wesentliche Rolle. Ziel muss es sein, dass Verbraucherinnen und Verbraucher und Kreative sich auf Augenhöhe begegnen und Abmahnungen sich nicht weiter zu einem eigenen Geschäftsmodell entwickeln.

Frage 68. Wie beabsichtigt die Landesregierung Verbraucherinnen und Verbraucher stärker über unbegründete und missbräuchliche Abmahnungen aufzuklären?

Die Landesregierung erachtet den bisher gewählten Weg, die Verbraucherinnen und Verbraucher über das VerbraucherFenster über aktuelle Themen wie das Thema Abmahnungen zu informieren, als geeigneten Weg einer Aufklärung.

Ein weiterer Weg sollte aber auch die Aufklärung der Bevölkerung über die Folgen der unrechtmäßigen Verwendung urheberrechtlich geschützter Werke sein. Viele Urheberrechtsverletzungen, die eine Abmahnung nach sich ziehen, geschehen in Unkenntnis der Rechtslage. Hier könnte gerade an den Schulen und Berufsschulen angesetzt werden.

Weitere wichtige Aufklärung in Form von Information und Beratung in diesem Bereich führen die Verbraucherzentrale Hessen und der DHB-Netzwerk Haushalt Hessen durch, die vom Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz zur Wahrnehmung ihrer Aufgaben eine institutionelle Förderung erhalten. In einer aktuellen Online-Umfrage überprüfen derzeit die Verbraucherzentralen der Länder, inwieweit Verbraucherinnen und Verbraucher durch das Gesetz gegen unseriöse Geschäftspraktiken vor überhöhten Forderungen geschützt werden. Die Fragen sind bis Ende 2014 auf der Internetseite der Verbraucherzentrale Hessen unter <http://www.verbraucher.de/link1134005A.html> veröffentlicht.

Frage 69. Wird die Landesregierung Änderungen des Rechtsrahmens vorantreiben, durch die das Verfahren bei Abmahnungen erschwert wird, sodass (bspw. durch die Verschärfung der Regelungen zum individuellen Nachweis des Rechtsverstoßes) die "Abmahnindustrie" geschwächt wird?

Auf die Antwort zur Frage 73 wird verwiesen.

Frage 70. Hält die Landesregierung die Begrenzung der Abmahnpauschalen der Höhe nach für sinnvoll?  
Wenn ja, in welchem Umfang?

Auf die Antwort zur Frage 73 wird verwiesen.

Frage 71. Welchen Anteil an gerichtlichen und außergerichtlichen Forderungen hat die "Abmahnindustrie" in diesem Zusammenhang?

Hierzu können aus Sicht des Ministeriums der Justiz keine näheren Angaben gemacht werden, da zum Einen zu den gerichtlichen Forderungen im Kontext mit Abmahnverfahren bei den Gerichten keine gesonderten Statistiken geführt werden. Zum Anderen ist darauf hinzuweisen, dass der außergerichtliche Bestand an Forderungen hinsichtlich seiner Quantität und Qualität der Justiz nicht bekannt wird.

Frage 72. Welche Maßnahmen beabsichtigt die Landesregierung mit Blick auf Abmahnungen zwischen Wettbewerbern und solchen, die als Wettbewerber auftreten, aber keine sind, zu ergreifen?

Eine Abgrenzung zwischen tatsächlichen Wettbewerbern und "Schein"-Wettbewerbern ist im Vorfeld schwierig, so dass präventive Maßnahmen nicht möglich sind.

Frage 73. Sieht die Landesregierung im Bereich der Abmahnungen gesetzgeberischen Handlungsbedarf auf Bundesebene?

Die Fragen 69, 70 und 73 werden, da sie im Kontext miteinander stehen, gemeinsam beantwortet.

Der in § 97 a des Urheberrechtsgesetzes normierte Rechtsrahmen für Abmahnungen ist erst vor kurzem neu gefasst worden, nämlich durch das Gesetz gegen unseriöse Geschäftspraktiken vom 1. Oktober 2013 (BGBl. I S. 3714).

Um Verbraucherinnen und Verbraucher vor überhöhten Abmahngebühren bei Urheberrechtsverletzungen zu schützen, sieht das Gesetz eine Deckelung von Anwalts- und Gerichtsgebühren vor, indem der Streitwert bei ersten Abmahnungen wegen einfacher Urheberrechtsverletzungen pauschal auf 1.000 € festgelegt worden ist. Dies bedeutet in seiner praktischen Auswirkung, dass die Kosten für die erste Abmahnung gegenüber einem privaten Nutzer regelmäßig auf 155,30 € begrenzt werden. Eine Ausnahme von dieser Streitwertfestschreibung wird dem Abmahnenden lediglich für die Fälle zugebilligt, in denen "dieser Wert ... nach den besonderen Umständen des Einzelfalles unbillig" ist. Die Darlegungs- und Beweislast dafür trägt allerdings der Abmahnende.

Da sich nach den Erhebungen der Verbraucherzentralen die durchschnittlichen Anwaltskosten für eine Abmahnung im Bereich des Urheberrechts bisher auf ca. 700 bis 800 € belaufen haben, wird erwartet, dass sich die jetzt geltende Deckelung der Anwaltsgebühr entsprechend anreizmindernd auf im Gebühreninteresse vorgenommene Massenabmahnungen bei Bagatellverstößen auswirken wird.

Insoweit gilt es, zunächst die Auswirkungen dieser Verschärfung des rechtlichen Rahmens für einschlägige Abmahnvorgänge zu beobachten und auch zu evaluieren, bevor gegebenenfalls weitergehende gesetzgeberische Maßnahmen, die ohnehin Bundesrecht betreffen würden, in Betracht gezogen werden können.

Inwieweit die 2013 von der Bundesregierung umgesetzten Maßnahmen in der Praxis greifen, wird die anstehende Evaluation des Gesetzes 2015 zeigen, aus der sich gegebenenfalls weiterer Nachbesserungsbedarf ableiten lässt.

### **Verbrauchersicherheit und Verbraucherrechte im Netz**

Frage 74. Inwiefern hält die Landesregierung den geltenden Rechtsrahmen für ausreichend, um die Sicherheit der Verbraucherinnen und Verbraucher und die Verbraucherrechte im E-Commerce zu gewährleisten?

In den vergangenen zwei Jahren wurde viel erreicht, um die Sicherheit im Internet und im E-Commerce zu verbessern: Seit August 2012 ist mit der so genannten Button-Lösung eine entsprechende gesetzliche Regelung in Kraft. Durch die Button-Lösung werden Online-Händler zu einer aussagekräftigen Schaltfläche verpflichtet. Diese muss klar kennzeichnen, wenn ein Mausklick Geld kostet. Die Regelung greift auch bei mobilen Geräten wie Smartphones oder Tablets. Die Anbieter sind auch verpflichtet, noch vor dem Abschluss eines Vertrages über wesentliche Vertragselemente wie den Preis oder Vertragslaufzeiten zu informieren und das klar, verständlich und in hervorgehobener Weise. Über die EU-Verbraucherrechte-Richtlinie gilt diese Regelung auch seit Mitte Dezember 2013 im gesamten europäischen Binnenmarkt.

Frage 75. Wo besteht aus Sicht der Landesregierung Verbesserungsbedarf?

Der geltende Rechtsrahmen für den Online-Handel versetzt Verbraucherinnen und Verbraucher grundsätzlich angemessen in die Lage, informierte Entscheidungen über die angebotenen Produkte und Dienstleistungen zu treffen und sich einen Eindruck über den Vertragspartner bzw. Anbieter zu verschaffen. Seit Inkrafttreten der "Button-Lösung" sind Verbraucherinnen und Verbraucher auch vor ungewollten kostenpflichtigen Vertragsschlüssen im Internet besser geschützt.

Probleme werden weiterhin im Bereich des Erwerbs digitaler Güter per Download gesehen. Wer digitale Güter wie E-Books, Musik, Filme oder Spiele per Download kauft, muss dabei in der Regel schon umfangreiche allgemeine Geschäftsbedingungen beachten. Hinzu kommt, dass sich in den Nutzungsbedingungen von E-Books in vielen Fällen Klauseln befinden, nach denen das elektronische Buch Einschränkungen im Hinblick auf Weiterverkauf oder Verleih unterliegt.

Die Thematik des Erwerbs und der späteren weiteren Nutzung von digitalen Produkten, die in unkörperlicher Form per Download über das Internet bezogen werden, war bereits Gegenstand der VSMK am 17. Mai 2013 (hierzu wird auch auf die Antwort zu Frage 4 verwiesen). Das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz hat einen Beschluss unterstützt, der darauf abzielt, analoge und digitale Güter hinsichtlich des Erwerbs und der damit einhergehenden Rechte gleichzustellen. In dem Beschluss der VSMK ist zudem auf ein Urteil des Europäischen Gerichtshofes aus dem Jahr 2012 hingewiesen worden, in dem es um den Weiterverkauf einer via Download erworbenen Software ging. Im Hinblick auf eine Übertragbarkeit dieses Urteils auf E-Books, Musik, Filme und weitere digitale Güter ist daher von der VSMK mit Unterstützung des Ministeriums für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz die Anregung an den Bund adressiert worden, eine entsprechende Studie unter Berücksichtigung dieses Urteils in Auftrag zu geben. Aktuell beschäftigt sich eine Projektgruppe der AG WV mit dem Thema "Daten- und Verbraucherschutz bei digitalen Rechte-management-Systemen gewährleisten" und erarbeitet hier gemeinsam mit Vertretern der Justizministerkonferenz Antworten auf Fragen des Urheberrechtes und mögliche Lösungsansätze sowie rechtliche Rahmenbedingungen.

Frage 76. Inwiefern leistet die Landesregierung Aufklärungsarbeit im Hinblick auf die gesetzlichen Rechte und Pflichten der Verbraucherinnen und Verbraucher im E-Commerce?

Die Landesregierung bietet Verbraucherinnen und Verbrauchern seit 2003 mit dem Verbraucherportal [www.verbraucherfenster.de](http://www.verbraucherfenster.de) aktuell und praxisnah umfassende Informationen rund um den Verbraucherschutz. Von Anfang an lag dabei ein Schwerpunkt auf dem wachsenden Internethandel und damit einhergehenden Risiken für die Bürger. Insgesamt sind über die direkte Suche nach dem Stichwort "Internet" derzeit 342 Beiträge abrufbar, unter anderem aus dem Bereich "Schnäppchen aus dem Internet - Was ist bei Online-Auktionen zu beachten?" "Wie Verbraucher im Internet abgezockt werden", "Abo-Fallen im Internet - Kleingedrucktes mit großer Wirkung", "Vertrag ist Vertrag - oder?", "Soziale Netzwerke - Reize und Risiken der schönen neuen virtuellen Internetwelt", "Bank- und Kreditkarten - Vorteile und Risiken", "Gewinnversprechen - und was sich dahinter verbirgt", "Datenschutz - warum eigentlich?".

2013 haben Beiträge der Verbraucherzentrale Hessen zu Online-Angeboten "Anleihen von Privatbankgebern", "Musik- und Filmtauschbörsen" sowie zum "Urheberrecht an Texten und Bildern im Internet" und Informationen zum "Löschen von Internetaccounts" die bisherigen Beiträge im VerbraucherFenster ergänzt.

Weitere wichtige Aufklärung in Form von Information und Beratung in diesem Bereich führen die Verbraucherzentrale Hessen und der DHB-Netzwerk Haushalt durch, die vom Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz zur Wahrnehmung ihrer Aufgaben eine institutionelle Förderung erhalten.

Seit dem 1. Juli 2011 fördert das Land Hessen den Online-Schlichter des Zentrums für Europäischen Verbraucherschutz e.V. in Kehl. Damit steht hessischen Verbraucherinnen und Verbrauchern das Angebot der kostenlosen Streitschlichtung offen, wenn sie über das Internet einen Vertrag mit einem Unternehmen mit Sitz in Deutschland abgeschlossen haben ([www.onlineschlichter.de](http://www.onlineschlichter.de)). Das Verfahren wird stets online abgewickelt und steht nur bestimmten Verbraucherinnen und Verbrauchern und Unternehmen zur Verfügung, deren Fall einen Bezug zu den teilnehmenden Ländern (Baden-Württemberg, Hessen, Bayern, Berlin und Rheinland-Pfalz) oder Unternehmen (Trusted Shops, DEVK und Bundesverband Direktvertrieb Deutschland) aufweist. Seit Start des Projektes 2009 sind insgesamt ca. 2.500 Fälle eingegangen. Die Erfolgsquote liegt bei rund 60 % über den gesamten Zeitraum betrachtet. Durch Öffentlichkeitsarbeit in Form von Pressemitteilungen, Vorträgen bei Verbänden und Beiträge und Interviews auf der Homepage des VerbraucherFensters wird auf die Arbeit des Online-Schlichters hingewiesen.

Frage 77. Gibt es bei den unter Frage 75 benannten Aufklärungsmaßnahmen geschlechts- bzw. altersspezifische Schwerpunkte?

Verschiedene Aktivitäten der Landesregierung zielen darauf ab, Verbraucherinnen und Verbraucher gemeinsam mit geeigneten Partnern zielgruppenspezifisch über ihre Rechte und Pflichten im Internet zu informieren und sie in ihren Handlungskompetenzen zu stärken.

Einen großen Anteil der Aufklärungsarbeit in Hessen leisten die mit Mitteln des Landes finanzierte VZ Hessen und der DHB-Netzwerk Haushalt. Zum Aufklärungs- und Beratungsangebot der VZ Hessen und des DHB-Netzwerk Haushalt wird auf die Antworten zu den Fragen 109 und 110 verwiesen. Eine geschlechtsspezifische Differenzierung erfolgt bei den Maßnahmen zur Verbraucheraufklärung nicht.

Frage 78. Hält die Landesregierung die Informationspflichten der Anbieterinnen und Anbieter gegenüber Verbraucherinnen und Verbrauchern des E-Commerce für vollständig auf den M-Commerce übertragbar?

Die technischen Möglichkeiten des M-Commerce stellen die Realisierung einer verbrauchergerichten Information vor besondere Herausforderungen. Für Anbieter im M-Commerce begründen sich diese vornehmlich aus dem Umstand, dass die von den Verbraucherinnen und Verbrauchern für den M-Commerce eingesetzten Endgeräte wie Smartphones oder Tablets über ein deutlich kleineres Display verfügen als z.B. Desktop-Computer. Mithin können im Rahmen des M-Commerce regelmäßig wesentlich weniger Informationen auf einen Blick präsentiert werden, was zu Lasten der Übersichtlichkeit gehen kann.

Ein immer wiederkehrendes Grundproblem des M-Commerce ist die Frage, wie die zahlreichen gesetzlichen Informationspflichten, denen die Anbieter, egal ob von E-Commerce- oder von M-Commerce-Angeboten unterliegen, angesichts der wesentlich kleineren Bildschirmgrößen von mobilen Endgeräten und den hieraus resultierenden Schwierigkeiten bei der Darstellung umfassender (rechtlicher) Texte rechtskonform umgesetzt werden können.

Einerseits haben M-Commerce-Anbieter - angefangen von der telemedienrechtlichen Anbieterkennzeichnung und den nach der Preisangaben-Verordnung (PAngV) vorgeschriebenen Preisangaben über die E-Commerce-, fernabsatz- und AGB-rechtlichen Informationspflichten einschließlich Widerrufsbelehrung bis hin zu den datenschutzrechtlichen Informationspflichten - umfangreiche Informationspflichten gegenüber den Nutzerinnen und Nutzern einzuhalten. Allein die fernabsatzrechtliche Widerrufsbelehrung besteht aus mindestens 2.000 bis 2.500 Zeichen, die telemedienrechtliche Anbieterkennzeichnung aus 300 bis 800 Zeichen und eine telemedienrechtliche Datenschutzerklärung liegt bei 2.000 bis 5.000 Zeichen. Insgesamt wird ein Informationsumfang von 5.500 bis zu 11.000 Zeichen angenommen, wobei übliche AGB mit einem Umfang von durchschnittlich zwischen 3.000 und 16.000 Zeichen noch nicht berücksichtigt sind. Zudem sind die gesetzlichen Pflichtinformationen "leicht erkennbar, unmittelbar erreichbar und ständig verfügbar" (Anbieterkennzeichnung gemäß § 5 Abs. 1 TMG), "leicht erkennbar und deutlich lesbar oder sonst gut wahrnehmbar" (Preisangaben gemäß § 1 Abs. 6 PAngV), "klar und verständlich" (E-Commerce-rechtliche und fernabsatzrechtliche Informationspflichten gemäß § 312g Abs. 1 Nr. 2 BGB i.V.m. Art. 246 § 3 EGBGB sowie § 312g Abs. 2 BGB bzw. § 312c Abs. 1 BGB i.V.m. Art. 246 § 1 EGBGB) etc., insgesamt lesbar und ohne unzumutbare Anstrengungen verständlich zu erteilen.

Andererseits stehen M-Commerce-Anbietern hierfür aber lediglich die technisch beschränkten Darstellungsmöglichkeiten von längeren (rechtlichen) Texten auf mobilen Endgeräten zur Verfügung. Eine Widerrufsbelehrung müsste mit dem Handy 13 bis 17-mal gescrollt werden, was nicht mehr zumutbar sein dürfte, mit dem Smartphone vier- bis fünfmal, was wohl zumutbar sein dürfte.

Frage 79. Sieht die Landesregierung für die Informationspflicht der Anbieterinnen und Anbieter im M-Commerce besondere Anforderungen gegenüber der Informationspflicht im E-Commerce?

Hierzu wird auf die Antworten zu den Fragen 78 und 80 verwiesen.

Frage 80. Falls Frage 78 bejaht wird: Welche Anforderungen müssen aus Sicht der Landesregierung erfüllt werden?

Aus Sicht von Verbraucherinnen und Verbrauchern bestehen im E-Commerce und im M-Commerce grundsätzlich ähnliche Informationsinteressen. Dabei sorgen die gültigen rechtlichen Anforderungen im Bereich der herkömmlichen E-Commerce-Welt für ein hohes Niveau des Verbraucherschutzes, welches grundsätzlich auch im Bereich mobiler Endgeräte Anwendung findet. Trotzdem zeigen die Erfahrungen in diesem neuen Sektor, dass nicht unerhebliche Gefahren der Manipulation und Irreführung, der Selektion und Preisdiskriminierung im mobilen Commerce vorhanden sind. Vor allem die eingeschränkten Darstellungsmöglichkeiten auf mobilen Endgeräten, die Komplexität und die fehlende Transparenz vieler Apps sowie die Ausgestaltung der Datenschutzbestimmungen und die Einflussnahmemöglichkeit der Nutzer stellen Ver-

braucherinnen und Verbraucher vor Herausforderungen. Es fehlt teilweise an verbraucherfreundlichen Regelungen.

Hessen hat sich bereits in der Vergangenheit für mehr Verbraucherfreundlichkeit beim mobilen Einkauf eingesetzt. Auf Antrag Hessens hat die 9. VSMK den mobilen Commerce auf die Tagesordnung gebracht und einstimmig mit den übrigen Ländern festgestellt, dass es bei Herstellern von Geräten, Betreibern von App-Stores und den Entwicklern von Apps Defizite im Rahmen der Nutzung ihrer Produkte beziehungsweise ihrer Dienste hinsichtlich transparenter, medienrechtlicher und verständlicher Informationen gibt und deshalb eine entsprechende und umfassende Aufklärung über die Rechte der Nutzerinnen und Nutzer für erforderlich gehalten wird. Die AG Wirtschaftlicher Verbraucherschutz (AG WV) wurde gebeten, die bestehenden rechtlichen Regelungen im Hinblick auf erforderliche Anpassungsbedarfe hinsichtlich der Gegebenheiten mobiler Endgeräte zu überprüfen. Hierzu hat die AG WV eine Projektgruppe "Mobile Endgeräte" eingesetzt, in der Hessen sich als Projektmitglied aktiv eingebracht hat.

Gemeinsam mit Experten aus Wissenschaft, Wirtschaft und Verbraucherverbänden hat Hessens Verbraucherschutzministerin diese Handlungsfelder 2014 erneut aufgegriffen und im Rahmen eines Fachgesprächs im Juni in Wiesbaden erörtert, welche konkreten Handlungen notwendig sind, um mehr Verbraucherfreundlichkeit in der mobilen Welt zu erzielen. Eine vereinfachte Darstellung gesetzlicher Informationspflichten von Unternehmen gegenüber Verbraucherinnen und Verbrauchern ist nach Auffassung der Landesregierung geboten. Angesichts der begrenzten Darstellungsmöglichkeiten auf mobilen Endgeräten könnte die Darstellung der Informationen gegebenenfalls mittels grafischer Symbole erfolgen. Zudem sollte gewährleistet sein, dass bei App-Angeboten, die sich an deutsche Verbraucherinnen und Verbraucher richten, die Verbraucherinformationen, Allgemeinen Geschäftsbedingungen und Datenschutzbestimmungen in deutscher Sprache verfasst sein müssen. Für eine verbraucherfreundliche Ausgestaltung wird sich Hessen im Rahmen des Bundesrates einsetzen.

Frage 81. Wie schätzt die Landesregierung die Risiken für Verbraucherinnen und Verbraucher ein, die von Rabatt- und Gutscheinsystemen im Netz ausgehen?

Hauptproblem bei solchen Rabatt- und Gutscheinsystemen ist laut Auskunft des Online-Schlichters, dass Verbraucherinnen und Verbrauchern oft nicht wissen, mit wem sie einen Vertrag abgeschlossen haben. Oftmals ist ihnen nicht bewusst, dass der Vertrag nicht mit dem Vermittlungsportal wie beispielsweise Groupon oder ab-in-den-Urlaub zu Stande kommt, sondern mit dahinterstehenden Händlern und Firmen.

Dies wird insbesondere dann relevant, wenn es zu Schwierigkeiten bei der Abwicklung kommt oder die erworbene Sache oder Dienstleistung Mängel aufweisen. Für Verbraucherinnen und Verbraucher stellt sich dann die Frage, an wen sie sich wenden und wem gegenüber sie eventuell bestehende Rechte geltend machen können. Portale wie Groupon treten lediglich als Vermittler und nicht als Anbieter von Produkten auf. Sie haften dann zum Beispiel nicht für die Mangelfreiheit der erworbenen Produkte oder die Durchführung der versprochenen Leistung, sondern verweisen auf die Verantwortung der jeweiligen Partnerunternehmen. Darüber hinaus seien laut Online-Schlichter die Angebote bei Rabatt- und Gutscheinsystemen oft wenig transparent. In vielen Fällen erfahren Verbraucherinnen und Verbraucher erst nach aufwendiger Recherche Näheres zu den Bedingungen ihrer Käufe. So komme es häufig vor, dass bei Gutscheinsystemen erworbene Dienstleistungen oft nur an bestimmten Tagen oder zu eingeschränkten Uhrzeiten eingelöst werden können.

Laut dem DHB-Netzwerk Haushalt Hessen können Rabatt- und Gutscheinsysteme zu vermehrten Bestellungen und dem Kauf ungenutzter Produkte führen. Im schlimmsten Fall kann es zur Überschuldung kommen. Preisvergleiche, die durchaus angebracht sind, unterbleiben wegen Zeitdruck oder "Verlockung". Zudem kann es zur Zunahme von Werbemails und Spams kommen.

Wirklich bedenklich sind aus Sicht der Verbraucherzentrale Hessen die vielen Angebote vermeintlich "ärztlicher" und kosmetischer Dienstleistungen. Diese reichen vom Bleaching der Zähne, über Tätowierungen, Permanent-Make-up bis hin zu ärztlichen Behandlungen wie Botox-Unterspritzungen und Brustvergrößerungen. Auch Abnehmen durch Laser oder Ultraschall zählen zu den besonders beliebten Angeboten. Einige dieser Methoden sind im Hinblick auf Effektivität und Wirksamkeit an sich kritisch zu betrachten. Deshalb sollte sich die Verbraucherin oder der Verbraucher bei dem Erwerb solcher Gutscheine genau informieren und sich bereits im Vorfeld einen Eindruck vom Anbieter verschaffen.

Frage 82. Plant oder unterstützt die Landesregierung Maßnahmen, um die Verbraucherinnen und Verbraucher über mögliche Risiken von Rabatt- und Gutscheinsystemen im Netz aufzuklären?

E-Commerce und die Nutzung des Internets steigen stetig an. Die Anzahl dubioser Angebote im Netz hat in den vergangenen Jahren dementsprechend zugenommen, aber auch die Nichtlieferung oder die verspätete Lieferung von Waren nach Zahlung per Vorkasse und eine intranspa-

rente Preisgestaltung stellen Verbraucherinnen und Verbraucher im Online-Bereich vor Herausforderungen. Wer online einkauft, möchte sich auch online beschweren. Aus diesem Grund bietet das Hessische Verbraucherschutzministerium seit dem 1. Juli 2011 bei Problemen und Fragen im Bereich Internet-Rechtsstreitigkeiten mit dem Online-Schlichter ([www.online-schlichter.de](http://www.online-schlichter.de)) einen kompetenten Ansprechpartner.

Alle hessischen Verbraucherinnen und Verbraucher, die mit einem Unternehmen, das seinen Sitz in Deutschland hat, einen Vertrag über das Internet geschlossen haben, können sich an den Online-Schlichter wenden. Ebenso können sich alle Verbraucherinnen und Verbraucher aus den EU-Mitgliedstaaten an den Online-Schlichter wenden, wenn das Unternehmen seinen Sitz in Hessen oder einem anderem Bundesland hat, das den Online-Schlichter finanziell fördert.

In ihrem Portal [www.verbraucherfenster.de](http://www.verbraucherfenster.de), das sich an Verbraucherinnen und Verbraucher richtet, informiert die Landesregierung regelmäßig auch über Risiken im Internet sowie von diesen ausgehenden Gefahren in Form von Beiträgen.

Weitere wichtige Aufklärung in Form von Information und Beratung in diesem Bereich führen die Verbraucherzentrale Hessen und der DHB-Netzwerk Haushalt Hessen durch, die vom Hessischen Verbraucherschutzministerium zur Wahrnehmung ihrer Aufgaben eine institutionelle Förderung erhalten. Die Verbraucherzentrale Hessen hat zum Thema "Rabattgutscheine im Internet" eine ausführliche Verbraucherinformation zusammengestellt, siehe unter: <http://www.verbraucher.de/Grouppons-Rabattgutscheine-im-Internet>

Frage 83. Wie schätzt die Landesregierung die Gefahr für die Verbraucherinnen und Verbraucher ein, die von Spam ausgeht?

Die massenhafte Versendung von E-Mails ist ein bekanntes Problem, insbesondere die sogenannten Phishing-Mails. Spam findet aktuell nicht mehr nur im E-Mail-Verkehr, sondern zunehmend auch in Sozialen Netzwerken statt. So laufen Social-Media-Nutzer Gefahr, dass ihr Account von "Spammern" gehackt und anschließend "gekapert" wird. Unverlangte Werbemails kosten die Empfänger Zeit und Geld und belasten als Massensendung die Server. Nur in bestimmten Fällen kann dagegen vorgegangen werden: Werden in der Kopf- und Betreffzeile der Absender oder der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht, kann dies als Ordnungswidrigkeit verfolgt und mit einem Bußgeld geahndet werden. Auch ist die Zusendung von Werbe-E-Mails ohne vorherige ausdrückliche Einwilligung nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) grundsätzlich eine unzumutbare und damit unzulässige Belästigung - abgesehen von einigen Ausnahmen. Daraus resultiert ein Unterlassungsanspruch (der auch der Verbraucherzentrale zusteht und von dieser geltend gemacht werden kann). Die Geltendmachung dieses Unterlassungsanspruchs ist aber für den Bürger ggf. mit einigem Aufwand verbunden.

Laut Auskunft der Bundesnetzagentur sind die Hauptverursacher von E-Mail-Spam weder in Deutschland noch im europäischen Ausland zu finden, so dass eine Rechtsverfolgung schwierig ist. Im Übrigen ist laut Bundesnetzagentur auch bei Spam-Mails, die aus Deutschland stammen, zu beachten, dass die mit Abstand meisten Spam-Mails (etwa 90 %) über infizierte "unschuldige" Rechner versandt würden.

Zum sogenannten Rufnummern-Spam zählen neben E-Mail-Spam auch Telefon- und Fax-Spam. Unter Telefon-Spam fallen insbesondere Spam mittels SMS, Spam in Form von sog. Gewinnversprechen, Ping-Anrufen und Predictive Dialern. Die Zahl der Beschwerden allein im Bereich Rufnummern-Spam belief sich im vergangenen Jahr laut Auskunft der Bundesnetzagentur auf 59.018. Das Volumen hat sich damit im Vergleich zum Vorjahr mehr als verdoppelt (24.063). Hiervon entfallen jedoch nur 4 % auf den Bereich E-Mail-Spam mit Rufnummernbezug. Nur dieser Bereich hat folglich seinen Ausgangspunkt im Internet.

Mögliche Folgen von Spam sind laut DHB-Netzwerk Haushalt Hessen Abzocke, Phishing und das unbewusste Herunterladen von Schadsoftware jeglicher Art.

In den vergangenen Jahren betrug der Spam-Anteil des an die Landesregierung adressierten E-Mail-Verkehrs durchschnittlich über 90 %. Diese Zahlen decken sich mit den Angaben von Sicherheitsdienstleistern zum Spam-Anteil am Gesamt-E-Mail-Verkehr. Das Ministerium des Innern und für Sport betrachtet den hohen Anteil von Spam als ernsthafte Belastung für die Verbraucherinnen und Verbraucher, aber auch für die Landesverwaltung. Die Anlieferung der Spam-Mails beansprucht Ressourcen und verursacht damit ebenso wie die Filterung von Spam am Übergang zwischen Internet und Landesnetz erhebliche Kosten. Ein Teil der Spam-E-Mails dient zudem der Verbreitung von Schadsoftware und dem Phishing. Die dabei zu beobachtende Professionalisierung der Angreifer macht es Verbraucherinnen und Verbrauchern zunehmend schwerer, Phishing-Versuche bzw. den Versuch der Installation von Schadsoftware zu erkennen.

Frage 84. Welche Vor- und Nachteile bieten aus Sicht der Landesregierung Bewertungsportale mit Blick auf ihre Wirkung für die Verbraucherinformation?

Kundenbewertungen spielen beim Online-Kauf eine immer größere Rolle. Jeder dritte Käufer lässt sich laut aktuellen Zahlen des IT-Verbandes Bitkom bei seiner Kaufentscheidung von Bewertungen anderer Käufer beeinflussen.

Bewertungsportale können für die Verbraucherin oder den Verbraucher eine große Hilfe bei der Entscheidungsfindung sein und Unterstützung beim Kauf bieten. Vor allem Erfahrungen anderer Käufer mit einem Produkt können durchaus hilfreich bei der eigenen Kaufentscheidung sein. Bewertungsportale bieten aber auch Missbrauchs- und Manipulationsgefahren. Online-Kundenbewertungen spiegeln teilweise nicht die tatsächliche Meinung von Kunden oder Käufern wider. Gute Rezensionen kommen von Testern, die die Produkte behalten können oder von professionellen Agenturen. Letztere rekrutieren Textschreiber, die gegen Geld Textbeiträge verfassen. Verbraucherinnen und Verbraucher kaufen so möglicherweise Produkte, die für gut befunden werden, aber real qualitativ schlecht sind. Ähnliches gilt für die Anbieter selbst. Diese werden eventuell als schnell, zuverlässig und kompetent bewertet, obwohl Waren in der Realität nicht ankommen. Viele Anbieter und Bewertungsplattformen gehen dagegen vor, indem sie bereits Wortfilter und Software einsetzen, um falsche Bewertungen zu erkennen.

Frage 85. Wie beabsichtigt die Landesregierung Verbraucherinnen und Verbraucher über das Problem der Manipulationsanfälligkeit solcher Bewertungen aufzuklären?

Einheitliche Qualitätskriterien und Mindeststandards für Bewertungsportale könnten Verbraucherinnen und Verbrauchern eine gute Orientierung auf diesem Markt ermöglichen und für mehr Transparenz sorgen. Hessen hat auf der Verbraucherschutzministerkonferenz 2014 einen entsprechenden Beschluss unterstützt.

Das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz hat in der Vergangenheit die Verbraucherinnen und Verbraucher über das Problem in Form von Pressemitteilungen aufgeklärt, über Missbrauchsgefahren informiert und mit praktischen Tipps versorgt. Zudem bietet die Hessische Landesregierung Verbraucherinnen und Verbrauchern mit dem Verbraucherportal [www.verbraucherfenster.de](http://www.verbraucherfenster.de) umfassende Informationen zu diesem Thema. Beispielhaft hierfür werden die Beiträge "Augen auf beim Online-Kauf: Bei Kunden-Online-Bewertungsportalen lauern oftmals Gefahren" und "Online-Shopping - Wie Sie sich vor Fallen schützen" genannt.

Die Verbraucherzentralen und der vzbv betreiben Aufklärungsarbeit im Rahmen ihrer allgemeinen Presse- und Öffentlichkeitsarbeit, durch Marktchecks, Veröffentlichung von Verbraucherinformationen oder Checklisten (meist im Rahmen von Projekten), siehe z.B. hier: <http://www.verbraucherzentrale-rlp.de/die-fallstricke-von-preis-und-bewertungsportalen->, aber auch durch Verweise auf Tests und Veröffentlichungen der Stiftung Warentest.

Aufklärung erfolgt ferner durch die persönliche und telefonische Beratung der Verbraucherzentralen. Die Netzwerkgruppe "Unlauterer Wettbewerb", in der auch die Verbraucherzentrale Hessen vertreten ist, erarbeitet hier regelmäßig entsprechende Beratungsstandpunkte und Hintergrundpapiere für die Beratungskräfte.

Der Bundesverband Verbraucherzentrale hat Ende 2012 im Rahmen des Projekts "Verbraucherrechte in der digitalen Welt" (Surfer haben Rechte) Handlungsempfehlungen an Betreiber von Bewertungsportalen zusammengestellt ([https://www.surfer-haben-rechte.de/cps/rde/xbcr/digitalrechte/Empfehlungspapier\\_Bewertungsportale-2012.pdf](https://www.surfer-haben-rechte.de/cps/rde/xbcr/digitalrechte/Empfehlungspapier_Bewertungsportale-2012.pdf)). Allgemeine Informationen und Checklisten sind unter <https://www.surfer-haben-rechte.de/cps/rde/xchg/digitalrechte/hs.xsl/2421.htm#tba2456> veröffentlicht. Hier erhält die Verbraucherin oder der Verbraucher zudem Tipps, worauf sie/er achten muss, wenn sie/er selbst Bewertungen verfassen will.

Frage 86. Sind Zertifizierungssysteme aus Sicht der Landesregierung geeignet, um dieser Problematik zu begegnen?

Bewertungsportale im Internet stehen häufig wegen fehlender Unabhängigkeit, Manipulationen und mangelnder Transparenz in der Kritik. Zertifizierungssysteme könnten daher durchaus geeignet sein, dieser Problematik zu begegnen.

Angesichts der Vielzahl der im Internet kursierenden Gütesiegel ist es für die Verbraucherin oder den Verbraucher allerdings recht schwer, den Durchblick im Gütesiegel-Dschungel zu behalten. Es gibt sowohl frei erfundene Gütesiegel als auch solche, die wenig aussagekräftig sind, da die Betreiber und Shops nicht gründlich geprüft werden oder nur auf Kriterien, die für die Verbraucherin oder den Verbraucher irrelevant sind.

Für Gütesiegel gelten bislang weder besondere gesetzliche Vorschriften, noch kann ausgeschlossen werden, dass ein Logo gefälscht oder in unberechtigter Weise genutzt wurde. Falls ein Gü-

tesiegel nur erteilt wird, wenn der Betreiber vorher anhand relevanter Qualitätskriterien geprüft wurde (relevante Aspekte sind hier Neutralität und Fachkompetenz), kann dies aber gleichwohl einen Zugewinn an Sicherheit für die Verbraucherin oder den Verbraucher bedeuten.

Verbraucherinnen und Verbraucher werden aber auch im Falle der Einführung eines Zertifizierungssystems für Bewertungsportale nicht umhin kommen, selbst zu prüfen, um was für ein Siegel es sich im Einzelfall handelt und aufgrund welcher Kriterien ein Portalbetreiber zertifiziert wurde.

Die 10. Verbraucherschutzministerkonferenz 2014 hat sich aufgrund dieser Problematik dafür ausgesprochen, Anreize für die Verwendung besonders glaubhafter und verbraucherfreundlicher Siegel zu schaffen. Dazu soll ein gemeinsamer Workshop von Bund und Ländern beitragen, auf dem die Anforderungen und die Aussagefähigkeit von Labeln, Güte- sowie weiterer Qualitätszeichen erörtert werden. Dadurch soll gewährleistet werden, die Orientierung für Verbraucherinnen und Verbraucher über Siegel zu verbessern. In diesem Zusammenhang hielten die Länder auf der 10. VSMK verpflichtende Mindestanforderungen für die Siegelverwendung im Rahmen einer bundesgesetzlichen Regelung für zielführend. Die Bundesregierung ist aufgefordert zu prüfen, welche geeigneten Maßnahmen und Anforderungen für Siegel im Lichte des europäischen Rechts statuiert werden können. Mögliche Kriterien für ein Zertifizierungssystem wie beispielsweise ein Gütesiegel könnten strenge Voraussetzungen für die Abgabe einer Bewertung, die Aktualität und Vollständigkeit der Verbraucherinformationen, eine einfache Bedienung sowie verbraucherfreundliche Vor- und Filtereinstellungen und transparente Darstellungsformen sein.

Frage 87. Wie sollte aus Sicht der Landesregierung gegen Unternehmen vorgegangen werden, die Gütesiegel unberechtigt kopieren und dadurch Verbraucherinnen und Verbraucher täuschen?

Das Gesetz gegen Unlauteren Wettbewerb (UWG) statuiert, dass (auch) die Werbung mit Gütesiegeln keine Irreführung des Verkehrs (der Verbraucherin/des Verbrauchers) bewirken darf (§ 5 Abs. 1 Nr. 1 UWG). Unlauter ist ausdrücklich die Verwendung von Gütezeichen, Qualitätskennzeichen oder Ähnlichem ohne die erforderliche Genehmigung (Nr. 2 Anh. zu § 3 Abs. 3 UWG).

Unlauter ist es beispielsweise, wenn das Siegel nicht aufgrund neutraler, objektiv vorgegebener, transparenter und von größeren Fachkreisen anerkannter Kriterien vergeben wird. Deren Einhaltung muss kontrolliert werden. Unterbleibt jegliche Kontrolle, kann die siegelbasierte Werbung schon aus diesem Grund irreführend sein.

Die Verbraucherzentralen können Verstöße gegen das Recht zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (§§ ... BGB) und gegen das Gesetz gegen den Unlauteren Wettbewerb (UWG) abmahnen beziehungsweise aufgrund der ihr zustehenden Verbandsklagebefugnis mit Unterlassungsklage gerichtlich dagegen vorgehen. Die rechtlichen Voraussetzungen, um gegen mit Gütesiegeln täuschende Unternehmen vorzugehen, sind somit gegeben.

Frage 88. Sind der Landesregierung Fallzahlen und Schadenswerte bekannt, die aus einer Täuschung von Verbraucherinnen und Verbrauchern über die Warenqualität im Online-Shopping resultieren?

Der Landesregierung liegen keine Angaben zu Fallzahlen und Schadenswerten im Sinne der Anfrage vor. Fallzahlen und Schadenswerte in Bezug auf (Waren-)Kreditbetrug im Internet werden zwar in der Polizeilichen Kriminalstatistik (PKS) erfasst. Es kann jedoch nicht gesondert ausgewertet werden, ob der Erwerb bei einer Privatperson oder bei einem Online-Händler erfolgte.

Dem Online-Schlichter, der beim Zentrum für Europäischen Verbraucherschutz in Kehl angesiedelt ist, sind keine Fälle, in denen mit falschen Marken geworben wird oder in denen es um nachgemachte Produkte geht, bekannt.

Frage 89. Wie beurteilt die Landesregierung das Problem sogenannter "Fake-Shops", bei denen nach Vorkasse keine Ware an Verbraucherinnen und Verbraucher gesendet wird und keine Reaktion auf Anfragen erfolgt?

Unter sogenannten "Fake-Shops" versteht man Internetseiten, die einen seriösen Online-Shop vortäuschen, jedoch keine oder nur minderwertige Imitate der angebotenen und durch den Kunden bezahlten Ware versenden. Eine Kontaktaufnahme gestaltet sich oftmals schwierig, da die im Impressum angegebenen Personen gar nicht existieren oder es sich um missbräuchlich verwendete Personendaten handelt. Fälle dieser Art gibt es immer wieder. Die Betroffenen sollten sich an die Polizei bzw. Staatsanwaltschaft wenden. Diese sogenannten Online-Shops, die z.B. eine Zahlung mittels Vorkasse verlangen und die versprochene Ware dann nicht liefern oder mangelhafte/minderwertige Ware liefern, werden als problematisch eingeschätzt. Derartige Fälle dürften regelmäßig als Betrug im Sinne des § 263 StGB zu qualifizieren sein.

Verbraucherinnen und Verbraucher sollten sich zudem beim Online-Shopping den Shop-Anbieter genau ansehen. Wird als Zahlungsmethode nur "Vorkasse" angeboten, könnte dies auf

einen unseriösen Anbieter schließen lassen. Ein Blick ins Impressum sollte Auskunft über den Shop geben. Verbraucherinnen und Verbraucher können das Unternehmen auch über eine Internetsuchmaschine prüfen. Sofern es gehäuft Probleme mit einem Shop gibt, findet sich dies meist schon in entsprechenden Foren. Auch sollte man von Vorkasse absehen, wenn man Zweifel hat und die Zahlung absichern. Bei vielen Zahlungsarten kann man den Betrag zurückbuchen oder einen Käuferschutz geltend machen. Schließlich hilft auch ein Preisvergleich der angebotenen Ware. Wenn ein Angebot zu günstig ist, ist fraglich, ob sich dahinter ein seriöses Angebot versteckt.

Probleme mit "Fake-Shops im Internet" tauchen seit einigen Jahren auch in der Beratungspraxis der Verbraucherzentrale Hessen auf. Die Schein-Portale machen häufig nur auf den ersten Blick einen guten Eindruck. Teilweise sind Impressum, Kontaktdaten und manchmal sogar Gütesiegel für sicheres Einkaufen im Netz aufgeführt. Sie erwecken damit den Eindruck eines verlässlichen Online-Shops. Die Landesregierung steht dieser Entwicklung kritisch gegenüber.

Frage 90. Wie viele Fälle von Betrug durch sogenannte "Fake-Shops" wurden in den vergangenen fünf Jahren bekannt?

Bei der beim Zentrum für Europäischen Verbraucherschutz eingerichteten eCommerce-Verbindungsstelle gingen im Jahr 2013 24 Fälle ein, 2014 gingen bisher 6 Fälle ein. Bei dem DHB-Netzwerk Haushalt Hessen sind Betrugsfälle dieser Art erst seit zwei Jahren ein Thema, eine genaue Zahl kann nicht genannt werden.

Der Landesregierung liegen keine Angaben zu Fallzahlen im Sinne der Anfrage vor. Im Übrigen wird auf die Antworten zu den Fragen 88 und 89 verwiesen.

Frage 91. Welche Schadenssumme entstand in diesem Zeitraum durch sogenannte "Fake-Shops" insgesamt und durchschnittlich pro Fall?

Der von der Landesregierung finanziell geförderte DHB-Netzwerk Haushalt Hessen gibt an, dass die Fälle direkt an die Kriminalpolizei verwiesen wurden. Die Schadenssumme variierte zwischen 40 Euro und 1.500 €.

Der Verbraucherzentrale Hessen liegen hierzu keine belastbaren Zahlen vor.

Der Landesregierung liegen keine Angaben zu Fallzahlen im Sinne der Anfrage vor. Im Übrigen wird auf die Antwort zu der Frage 90 verwiesen.

Frage 92. Welche Maßnahmen plant oder unternimmt die Landesregierung zur Bekämpfung dieses Problems?

Die Landesregierung sieht in einer konsequenten (strafrechtlichen) Verfolgung und einer weiteren Sensibilisierung und Aufklärung geeignete Maßnahmen zum besseren Schutz für Verbraucherinnen und Verbraucher.

Auf die Antwort zu Frage 40 wird verwiesen.

Frage 93. Welche Pflichten haben die Provider im Hinblick auf die Sicherheit der Zahlungsdienste im Internet?

Frage 94. Wie steht die Landesregierung zu einer Verpflichtung der Provider zur Überprüfung der Sicherheitsmechanismen der Zahlungsdienstleister, um Missbrauch zu verhindern?

Die Fragen 93 und 94 werden zusammen beantwortet.

Losgelöst von einer Verpflichtung der Provider zur Überprüfung wird eine Erhöhung der Sicherheitsmechanismen der Zahlungsdienstleister zur Verhinderung des Missbrauchs begrüßt. Jegliche Beseitigung von Tatgelegenheiten - sei es im realen oder im virtuellen Raum - ist erstrebenswert, wenn die Begehung von Straftaten erschwert oder verhindert werden kann.

Frage 95. Welche Zahlungssysteme im Internet sind der Landesregierung bekannt?

Frage 96. Wie beurteilt die Landesregierung die unterschiedlichen Bezahlsysteme im Internet hinsichtlich ihrer Sicherheit, möglicher Missbrauchsformen und sonstiger verbraucherpolitischer Aspekte?

Die Fragen 95 und 96 werden zusammen beantwortet.

Die Mehrheit der Online-Händler bietet sowohl herkömmliche Bezahlverfahren wie Lastschrift, Zahlung per Vorkasse oder per Nachnahme als auch elektronische Bezahlverfahren wie die Zahlung per Kreditkarte oder Zahlung per Überweisung im Internet an. Grundsätzlich gilt: Alle Bezahlverfahren haben ihre Vor- und Nachteile. Die Verbraucherinnen und Verbraucher sollten im Einzelfall Komfort und Sicherheit gegeneinander abwägen, bevor sie sich für eine Zahlungsmethode entscheiden. Zudem ist es wichtig, den eigenen Computer so weit wie möglich durch

technische Hilfsmittel zu schützen und sich immer über die neuesten Entwicklungen zu informieren. Dabei sollte grundsätzlich darauf geachtet werden, dass alle Daten über eine sichere SSL-Verbindung verschlüsselt übertragen werden - sowohl die persönlichen Angaben als auch alle Informationen zu Bankverbindungen oder Kreditkarteninformationen. Dies ist daran zu erkennen, dass in der URL-Zeile des Browsers statt https nur http am Anfang der Webadresse angezeigt wird.

Durch die im Vergleich zum stationären Handel fehlende Barzahlungsmöglichkeit im E-Commerce besteht grundsätzlich - selbst für Personen mit Internetkenntnissen - die Gefahr, Opfer von Phishing- oder Pharming-Angriffen zu werden, bei denen Daten ausgespäht werden.

Zum Thema Phishing wird auf die Antworten zu den Fragen 49 ff. verwiesen.

Frage 97. Welche Maßnahmen ergreift die Landesregierung, um die Verbraucherinnen und Verbraucher über mögliche Risiken zu informieren?

Vielfältige Informationen dienen dazu, die Verbraucherinnen und Verbraucher über ihre Rechte und Pflichten sowie Gefahren im Internet aufzuklären: Im Verbraucherportal der Landesregierung [www.verbraucherfenster.de](http://www.verbraucherfenster.de) wie auch durch die Beratung und das Informationsangebot der Verbraucherzentrale Hessen, online unter der Rubrik Finanzen/Girokonto, werden die Verbraucherinnen und Verbraucher regelmäßig zu möglichen Risiken im Bereich "Online-Banking" aufgeklärt. Unter der Rubrik Finanzen/Geldanlage und Kredit/Girokonto und Bargeld werden für diesen Bereich relevante und aktuelle Informationen in das Portal eingestellt.

Via Twitter wird über die wichtigsten Aspekte hinsichtlich Verbraucherschutzinformationen zusätzlich berichtet. Die Angebote des VerbraucherFensters [www.verbraucherfenster.de](http://www.verbraucherfenster.de) werden auf diesem Wege zusätzlich beworben.

Auf die Antwort zu Frage 40 wird verwiesen.

Frage 98. Sind der Landesregierung die Sicherheitsmechanismen bekannt und wer überprüft deren Wirksamkeit?

Aufgrund der rasanten Entwicklungen in diesem Bereich liegen der Landesregierung keine umfassenden Erkenntnisse zu dem Markt von Anbietern für Bezahlssysteme im Internet vor. Somit kann auch keine Bewertung der Sicherheitsmechanismen erfolgen.

Die Initiative D21 hat Qualitätskriterien für Online-Shops definiert, die teilweise auch bestimmte Sicherheitsstandards für das Bezahlverfahren umfassen. Sie sind online einzusehen unter [www.internet-guetesiegel.de](http://www.internet-guetesiegel.de). Informationen zur sicheren Bezahlung im Internet stellt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de) zur Verfügung.

Frage 99. Wie steht die Landesregierung zu anonymen Bezahlformen im Netz?

Bei anonymen Bezahlssystemen muss die Verbraucherin oder der Verbraucher an keiner Stelle persönliche Daten oder Bank- oder Kreditkartendaten angeben. Aus Datenschutzgründen sind anonyme Bezahlformen daher zu begrüßen.

Bei den anonymen Bezahlformen handelt es sich oft um sogenannte Prepaid-Angebote, deren Karten zum Teil wieder aufladbar sind. Hierbei können Kunden in einer der Verkaufsstellen eine Karte mit einem bestimmten Wert mit einer PIN-Nummer kaufen. Die PIN-Codes können auch digital erworben werden. Auf der jeweiligen Website oder dem Webshop, die mit dem jeweiligen Prepaid-Anbieter kooperiert, tippt man anschließend im Rahmen des Bezahlvorganges die Ziffernfolge ein. Das Guthaben der Karte wird überprüft und sofort gebucht.

Dem Vorteil des sparsamen Umgangs mit persönlichen Daten auf der einen Seite kann auf der anderen Seite das Interesse an einer wirksamen Geldwäscheprävention durch Herstellung der Transparenz von Zahlungsströmen entgegenstehen. Anonyme Bezahlformen im Internet werden durch Straftäter bzw. Straftätergruppen genutzt, um Gelder ohne Nachweis zu transferieren. Sowohl im Bereich der Allgemeinkriminalität, aber auch der Organisierten und der Politisch Motivierten Kriminalität nutzen Straftäter diese Bezahlformen, um illegale Gelder zu transferieren. Insbesondere der Geldwäsche und Verstößen gegen das Steuerrecht wird durch anonyme Bezahlformen Vorschub geleistet.

### **Verbraucherrechte in der Strategie der Landesregierung**

Frage 100. Welche Rolle spielt das Internet insgesamt in der Strategie der Landesregierung zur Aufklärung von Verbraucherinnen und Verbrauchern?

Die Landesregierung informiert die Verbraucherinnen und Verbraucher regelmäßig über aktuelle verbraucherrelevante Themen. Neben dem VerbraucherFenster Hessen

fenster.hessen.de und dem Twitter-Account [www.twitter.com/Verbraucherinfo](http://www.twitter.com/Verbraucherinfo), die das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz betreut, werden zur Aufklärung der Verbraucherinnen und Verbraucher zeitweise auch die Internetkanäle der Staatskanzlei genutzt, um verbraucherrelevante Informationen zu verbreiten. Neben dem Informationsportal [hessen.de](http://hessen.de), wird auch über die Landeskanäle von Facebook und Twitter über die angesprochenen Themen informiert.

Frage 101. Enthält die Strategie der Landesregierung geschlechts- bzw. altersspezifische Inhalte zur Aufklärung von Verbraucherinnen und Verbrauchern?

Auf die Antwort zur Frage 29 und 132 wird verwiesen.

Frage 102. Welche Maßnahmen beabsichtigt die Landesregierung umzusetzen, um die Verbraucherrechte beim Online-Shopping zu stärken?

Wer online einkauft, möchte sich auch online beschweren. E-Commerce und die Nutzung des Internets steigen stetig an. Nicht nur die Anzahl dubioser Angebote im Netz hat in den vergangenen Jahren dementsprechend zugenommen, auch die Nichtlieferung oder die verspätete Lieferung von Waren nach Zahlung per Vorkasse und eine intransparente Preisgestaltung stellen Verbraucherinnen und Verbraucher im Online-Bereich vor Herausforderungen. Aus diesem Grund bietet das Hessische Verbraucherschutzministerium seit dem 1. Juli 2011 bei Problemen und Fragen im Bereich Internet-Rechtsstreitigkeiten mit dem Online-Schlichter einen kompetenten Ansprechpartner. Der Online-Schlichter wird vom Zentrum für Europäischen Verbraucherschutz e.V. angeboten und u.a. von Hessen finanziert.

Alle Verbraucherinnen und Verbraucher sowie Unternehmen aus Hessen, die einen Vertrag über das Internet abgeschlossen haben, können sich an den Online-Schlichter wenden, wenn ihr Vertragspartner ein Unternehmen mit Sitz in Deutschland ist und alle Verbraucherinnen und Verbraucher aus den EU-Mitgliedstaaten, wenn das Unternehmen seinen Sitz in Hessen oder einem anderen Land, das sich an dem Projekt beteiligt, hat. Es ist eine Win-win-Situation für alle Streitbeteiligten: Die bisher vom Online-Schlichter gemachten Erfahrungen zeigen, dass eine Online-Schlichtungsstelle Verbraucherinnen und Verbrauchern eine schnelle und kostengünstige Möglichkeit bieten könnte, eine Rechtstreitigkeit mit einem Unternehmen gütlich beizulegen. Eine gütliche Beilegung solcher Rechtstreitigkeiten durch Schlichtungsverfahren hat auch eine positive Auswirkung auf die künftige Geschäftsbeziehung zwischen Verbraucherinnen und Verbraucher und Unternehmen und entlastet darüber hinaus die Justiz. Verfahren der außergerichtlichen Streitbeilegung sind in der Regel weniger aufwendig, kostspielig und langwierig als Gerichtsverfahren und haben damit grundsätzlich Vorzüge für beide Seiten. Gerade bei einem oft geringen Streitwert ist die Hemmschwelle der Verbraucherin oder des Verbrauchers, zu klagen, hoch. Eine Schlichtung kann hier eine gute Alternative sein. Auch die Pläne der EU, eine Online-Plattform für die außergerichtliche Streitbeilegung einzurichten und die Mitgliedstaaten ab Juli 2015 zu verpflichten, flächendeckend außergerichtliche Streitbeilegungsstellen zu schaffen, unterstreichen die wachsende Bedeutung der Tätigkeit des Online-Schlichters im nationalen und europäischen Kontext.

Im Jahr 2013 hat der Online-Schlichter 1.142 Fälle bearbeitet. Die Erfolgsquote lag 2013 bei rund 70 %. Im Jahr 2013 wurden die Fälle in rund 8 Wochen abgeschlossen.

Hessen hat sich darüber hinaus im Bundesrat für die Einführung der Button-Lösung stark gemacht. Mit der so genannten Button-Lösung soll verhindert werden, dass Verbraucherinnen und Verbraucher bei Online-Geschäften über entstehende Kosten getäuscht werden. Anbieter müssen kostenpflichtige Angebote deutlich kennzeichnen, so dass Verbraucherinnen und Verbraucher genau und sicher erkennen können, wenn ein "Klick" Geld kostet. Sofern die Bestellung der Verbraucherin oder des Verbrauchers über einen "Button" erfolgt, muss dieser mit einer eindeutigen Beschriftung wie "kostenpflichtig bestellen" oder "kaufen" versehen sein.

Frage 103. Welche Rolle spielt das Internet aus Sicht der Landesregierung zur Information von Verbraucherinnen und Verbrauchern in den Bereichen

- a) Lebensmittel(sicherheit),
- b) Gastronomie,
- c) Gesundheit?

Die Nutzung von Medien hat sich in den letzten Jahren durch die wachsende Verbreitung des Internets stark verändert. Das Internet wird inzwischen in fast allen Bereichen als eine der Hauptinformationsquellen angesehen. Immer mehr Verbraucherinnen und Verbraucher nutzen das Internet allerdings auch um Waren aller Art, so auch Lebensmittel zu kaufen. Diesem Trend müssen sich die Lebensmittelüberwachungsbehörden stellen.

Ein wichtiger Schritt dabei ist die Kontrolle von Lebensmitteln, die über das Internet gehandelt werden. Zu diesem Zweck wurde im Juli 2013 beim BVL die gemeinsame Zentralstelle der Länder "Kontrolle der im Internet gehandelten Erzeugnisse des Lebensmittel- und Futtermittelgesetzbuches (LFGB) und Tabakerzeugnisse", kurz G@ZIELT eingerichtet. Die im Auftrag der

Länder geführte Zentralstelle bietet den Vorteil, den Internethandel, der an keiner Grenze Halt macht, besser beobachten zu können. Bei den durchgeführten Recherchen im Lebensmittelbereich liegt der Fokus der Recherche auf der Suche nach risikobehafteten Lebensmitteln, die die Verbraucherinnen und Verbraucher evtl. gesundheitlich schädigen oder täuschen können, bzw. auf Betrieben, die den Lebensmittelüberwachungsbehörden noch nicht bekannt sind. Die Ergebnisse der Recherchen werden an die zuständigen Überwachungsbehörden weitergegeben, damit diese im Rahmen ihrer Zuständigkeit erforderliche Maßnahmen ergreifen können, zum Beispiel die Löschung des Angebotes im Internet oder die Registrierungspflicht des Lebensmittelunternehmers durchzusetzen.

Bestehen unmittelbare Risiken für die Gesundheit der Verbraucherin oder des Verbrauchers, so ist der Lebensmittelunternehmer nach europäischem Recht verpflichtet, das betroffene Produkt schnellstmöglich zurückzunehmen. In Fällen akuter Gesundheitsgefährdung durch bestimmte Erzeugnisse werden einschlägige Informationen der Verbraucherin oder dem Verbraucher durch die üblichen Kommunikationswege (öffentliche Warnungen, Pressemitteilungen etc.) zur Verfügung gestellt. Diese Informationen werden i.d.R. über die verschiedenen Medien eingespeist und auf der Homepage des Unternehmens und auf dem bundesweiten Portal [www.Lebensmittelwarnung.de](http://www.Lebensmittelwarnung.de) eingestellt. Diese seit 2011 bestehende Internet-Seite enthält Informationen nach § 40 Lebensmittel- und Futtermittelgesetzbuch (LFGB) über Lebensmittel und mit Lebensmitteln verwechselbare Produkte, die in Deutschland auf dem Markt sind und möglicherweise bereits an Endverbraucherinnen und Endverbraucher abgegeben wurden und von denen eine gesundheitliche Gefahr ausgeht. Die auf dem Portal veröffentlichten Informationen sind von den Lebensmittelunternehmern oder von der amtlichen Lebensmittelüberwachung veranlasst worden und von überregionaler Bedeutung. Die nach dem Sitzlandprinzip zuständige Behörde stellt die jeweilige Meldung auf dem Portal ein und Verbraucherinnen und Verbraucher können sich über ein RSS-Feed informieren lassen.

Auf Grundlage der Verordnung (EG) Nr. 178/ 2002 wurde innerhalb der EU ein Schnellwarnsystem für Lebensmittel und Futtermittel (Rapid Alert System for Food and Feed, RASFF) implementiert. Es sorgt für eine lückenlose, schnelle internetbasierte Weitergabe von Informationen zwischen den Mitgliedsstaaten und der Kommission, wenn Produkte entdeckt werden, die eine Gefahr für die Gesundheit darstellen. Seit 2003 stellt die EU-Kommission wöchentlich einen Bericht über alle Warn- und Informationsmeldungen ins Internet.

Im Verbraucherportal der Hessischen Landesregierung, [www.verbraucherfenster.de](http://www.verbraucherfenster.de) werden umfassende Informationen zu Themen der Ernährung, der Lebensmittelsicherheit und dem Verbraucherschutz zusammengestellt. Beispielsweise bietet das Portal die Babynahrung-Produktsuche, in welcher regelmäßig Produktinformationen aktualisiert werden.

Darüber hinaus bietet das VerbraucherFenster Hessen der Verbraucherin oder dem Verbraucher die Möglichkeit, vertrauliche Hinweise auf Lebensmittelunternehmen, die mit Lebensmitteln nicht sachgerecht umgehen oder Lebensmittel nicht ordnungsgemäß kennzeichnen, den Lebensmittelüberwachungsbehörden zu melden. Für diese Fälle wird ein Kontaktformular für vertrauliche Informationen unter [www.verbraucherfenster.hessen.de](http://www.verbraucherfenster.hessen.de) zur Verfügung gestellt.

Das Internetportal [www.Lebensmittelklarheit.de](http://www.Lebensmittelklarheit.de) des Bundesverbandes Verbraucherzentralen und der Verbraucherverbände ermöglicht Verbraucherinnen und Verbrauchern, sich aktiv in den Diskussionsprozess über die unklare Kennzeichnung von Lebensmitteln oder über irreführende Produktaufmachungen einzubringen. Die Verbraucherin oder der Verbraucher kann aus ihrer/seiner passiven, beobachtenden Rolle heraus kommen und aktiv durch Einsenden von konkreten Produktbeispielen zu Wort kommen und in einen Dialog mit der Wirtschaft treten.

Die Arbeiten des Bundesinstituts für Risikobewertung (BfR) und des Robert-Koch-Instituts (RKI) als nationale unabhängige Institutionen, ebenso wie die Tätigkeit der Europäischen Behörde für Lebensmittelsicherheit (EFSA) erstreckt sich auf eine Vielzahl von Bereichen, um die Verbraucherinnen und Verbraucher in der EU vor lebensmittelbedingten Risiken zu schützen. Forschungsergebnisse und Risikobewertungen werden der Verbraucherin oder dem Verbraucher über das Internet transparent gemacht und zur Verfügung gestellt.

Frage 104. Wie soll der Lebensmitteleinkauf online dem Lebensmittelkauf außerhalb des Internets angepasst werden, bezogen auf z.B. Kennzeichnungsvorschriften, Pflichtangaben, Zutatenliste?

Die ab 13. Dezember 2014 anzuwendenden Vorgaben der Verordnung (EU) Nr. 1169/2011 (Lebensmittelinformationsverordnung) beinhalten umfassende Regelungen zur Bereitstellung von verpflichtenden Informationen bei einem Fernabsatz von Lebensmitteln.

Frage 105. Beabsichtigt die Landesregierung, rechtliche Regelungen für die gesundheitsbewusste Werbung im Internet, wie "laktosefrei", zu schaffen?

Die rechtlichen Vorgaben der Verordnung (EG) Nr. 1924/2006 über Nährwert- und gesundheitsbezogene Angaben über Lebensmittel sind grundsätzlich auch auf Werbeaktivitäten der Lebensmittelunternehmen im Internet anzuwenden. Für die Angabe "laktosefrei" bestehen derzeit keine spezifischen Vorgaben auf EU-Ebene. Gemäß den Ausführungen im Erwägungsgrund 42 der Verordnung (EU) Nr. 609/2013 über Lebensmittel für Säuglinge und Kleinkinder, Lebensmittel für besondere medizinische Zwecke und Tagesrationen für gewichtskontrollierende Ernährung wird angestrebt, die Bedingungen für die Verwendung dieser Angabe zukünftig auf europäischer Ebene zu harmonisieren und im Rahmen der Verordnung (EU) Nr. 1169/2011 (Lebensmittelinformationsverordnung) zu regeln. Die Landesregierung wird dieses Regelungsvorhaben unterstützend begleiten.

Frage 106. In welchen weiteren Bereichen beabsichtigt die Landesregierung, Transparenz in Verbraucherschutzfragen durch die verstärkte Bereitstellung von Informationen zu gewährleisten?

Schon heute stellt die Landesregierung umfassende Informationen bereit, um Transparenz für Bürgerinnen und Bürger zu schaffen. Die Landesregierung bietet hessischen Verbraucherinnen und Verbrauchern seit 2003 mit dem Verbraucherportal [www.verbraucherfenster.de](http://www.verbraucherfenster.de) aktuell und praxisnah umfassende Informationen rund um den Verbraucherschutz an. Das VerbraucherFenster informiert die Verbraucherinnen und Verbraucher in verschiedenen Rubriken umfassend zu einzelnen Themen und Fragestellungen. Diese Rubriken sind: Ernährung & Lebensmittel, Finanzen & Recht, Gesundheit & Soziales, Umwelt & Energie, Internet & Telekommunikation und sicher leben.

Umfassende Informationen über die Tätigkeiten der Landesregierung im Bereich Verbraucherschutz gibt zudem der Verbraucherschutzbericht "Verbraucherschutz in Hessen", der im Jahr 2013 veröffentlicht wurde. Er steht zum Download bereit unter: [https://umweltministerium.hessen.de/sites/default/files/media/hmuelv/verbraucherschutzbericht\\_2013webungeschuetzt.pdf](https://umweltministerium.hessen.de/sites/default/files/media/hmuelv/verbraucherschutzbericht_2013webungeschuetzt.pdf)

Im Lebensmittelbereich spricht sich die Landesregierung für die Einführung einer verpflichtenden Herkunftskennzeichnung von tiefgefrorenem Obst und Gemüse aus.

Zudem informieren die einzelnen Ressorts der Landesregierung die Verbraucherinnen und Verbraucher themenspezifisch zu allen wichtigen Fragen on- als auch offline. So gibt es Informationsportale zu:

- Nano-Sicherheit (HMWEVL) <http://www.nano-sicherheit.de/>,
- ein Gesundheitsportal (HMSI) <http://www.sozialnetz.de/ca/b/f/>,
- und ein Pflegeportal (HMSI) <http://www.pflege-in-hessen.de/>.

Im Rahmen des gesetzlich verankerten Informationsauftrages wird der Einsatz von Social Media als Teil der Öffentlichkeitsarbeit als sinnvolle Ergänzung erachtet. Via Twitter wird über die wichtigsten Aspekte hinsichtlich Verbraucherschutzinformationen sowohl der Landesregierung als auch überregional berichtet. Zudem wird auf wissenswerte Neuigkeiten in Verbraucherschutzfragen aufmerksam gemacht. Die Angebote des VerbraucherFensters [www.verbraucherfenster.de](http://www.verbraucherfenster.de) werden auf diesem Wege zusätzlich beworben.

Auch der DHB-Netzwerk Haushalt Hessen und die Verbraucherzentrale Hessen, die von der Hessischen Landesregierung finanziell gefördert werden, informieren innerhalb ihrer Beratungstätigkeit umfassend zu verschiedenen Themenschwerpunkten.

Frage 107. In welchen Formaten und unter welchen Bedingungen werden in den genannten Bereichen Informationen bereitgestellt?  
Werden die Open-Data-Kriterien berücksichtigt?

Die Informationen werden im Interesse der Allgemeinheit ohne jede Einschränkung zur freien Nutzung, zur Weiterverbreitung und zur freien Weiterverwendung bei den Online-Angeboten der Landesregierung frei zugänglich gemacht. Hinsichtlich der Informationsbereitstellung wird auf die Antwort zu Frage 104 verwiesen.

Bei der Veröffentlichung von Daten müssen die Grundsätze der Wirtschaftlichkeit und die Vorgaben des Datenschutzes und der Persönlichkeitsrechte berücksichtigt werden. Wenn die Verwaltung Daten veröffentlicht, erfolgt dies nach den Vorgaben der INSPIRE-Richtlinie. Die Open-Data-Kriterien haben keine Verbindlichkeit für die Hessische Landesregierung.

Die Informationsbereitstellung im Lebensmittelbereich muss vornehmlich den rechtlichen Anforderungen der Verordnung (EU) Nr. 1169/2011 (Lebensmittelinformationsverordnung) genügen.

Frage 108. Beabsichtigt die Landesregierung, die Verpflichtungen von Unternehmen zur Bereitstellung von Verbraucherinformationen zu intensivieren?

- a) Falls ja: in welchen Bereichen?
- b) Falls ja: Welche Rolle spielt hier das Internet als Informationsmedium?

**Zu a:** Die Landesregierung beabsichtigt im Rahmen einer verbesserten Verbraucherinformation grundsätzlich diesbezügliche Verpflichtungen von Unternehmen auszuweiten, setzt aber in einem ersten Schritt zunächst auf freiwillige Vereinbarungen mit der Wirtschaft. So wird die Einführung eines Hygienesiegels für Betriebe, die im Rahmen der amtlichen Lebensmittelkontrolle überdurchschnittlich gut abschneiden, geprüft. Ferner unterstützt Hessen weiterhin den Bundesratsbeschluss vom Frühjahr 2013 in dem der Bund aufgefordert wurde, die bestehenden gesetzlichen Informationsvorschriften in einem einheitlichen, in sich schlüssigen Transparenzsystem zusammenzufassen.

**Zu b:** Bei der Information der Verbraucherinnen und Verbraucher spielt das Internet inzwischen eine herausragende Rolle und wird daher auch zukünftig ein wesentliches Instrument zur Verbraucherinformation sein. Das Internet kann insbesondere auch bei Fernabsatzgeschäften eine wichtige Funktion als Informationsmedium übernehmen. Konkrete Angaben über die zukünftige Ausgestaltung können derzeit nicht gemacht werden.

### **Rolle der Verbraucherzentralen**

Frage 109. Welche Rolle sieht die Verbraucherpolitik der Landesregierung für die Verbraucherzentralen im Bereich des Verbraucherschutzes im Internet?

Das Land Hessen finanziert die Verbraucherorganisationen hierzulande mit institutioneller Förderung. Durch diese Zuwendungen wird die Verbraucherzentrale Hessen u.a. personell in die Lage versetzt, Märkte zu beobachten und zu analysieren sowie ggf. konkret Verbraucherrechte durchzusetzen.

So konnte die Verbraucherzentrale Hessen beispielsweise im Jahr 2011 Online-Händler wegen Verstößen gegen Kennzeichnungsvorschriften im Lebensmittelbereich erfolgreich abmahnen. Konkret ging es dabei um Lebensmittel, die im Internet angeboten wurden und als glutenfrei gekennzeichnet waren, obwohl die jeweiligen Lebensmittel Gluten enthielten.

Das Instrument der Rechtsdurchsetzung soll künftig durch den Aufbau einer internen Rechtsabteilung der Verbraucherzentrale weiter gestärkt werden. Dazu sollen zusätzliche Landesmittel bereitgestellt werden.

Dieser Ansatz ist richtig. Denn Verbraucherschutz im Internet ist nur in bestimmten Fällen Gegenstand staatlicher Vollzugs- oder Aufsichtsmaßnahmen. Häufig muss Verbraucherschutz im Internet von betroffenen Verbraucherinnen und Verbrauchern auf dem zivilrechtlichen Weg durchgesetzt werden. Deshalb fällt den Verbraucherzentralen bei der Durchsetzung des Verbraucherschutzes im Internet eine ganz zentrale Rolle zu. Es ist gerade die Aufgabe der Verbraucherzentralen, den Verbraucherinnen und Verbrauchern mit Informationen, Bildungsangeboten und persönlicher Beratung bei der Lösung von Problemen und Fragestellungen rund um den Konsum zur Seite zu stehen.

Die Verbraucherzentrale Hessen erfüllt aus Sicht der Landesregierung beim Verbraucherschutz im Internet eine wichtige Sensorfunktion. Diese lässt sich an der Entwicklung der Internet-Abo-Fallen und der Gesetzesinitiative zur Button-Lösung veranschaulichen. Zu Beginn des Jahres 2006 gab es die ersten Verbraucherbeschwerden zu den sogenannten Abo-Fallen. Eine Online-Umfrage der Verbraucherzentralen verdeutlichte das Ausmaß und den wirtschaftlichen Schaden. In der Folge formulierten die Verbraucherzentralen an den Gesetzgeber (Bund) die Forderung einer Button-Lösung, die schließlich im August 2012 in Kraft trat. Darüber hinaus berät und informiert die Verbraucherzentrale Hessen Verbraucherinnen und Verbraucher über deren Rechte beim Online-Einkauf.

Ähnlich verhält es sich auch mit anderen Problemstellungen zum Verbraucherschutz im Internet - auch hier arbeitet die Verbraucherzentrale Hessen mit einer Kombination aus Beratung, Information und Sensorfunktion. Beispielhaft seien hier die untergeschobenen Verträge über mobile Endgeräte oder das Thema Datenschutz im Internet erwähnt.

Frage 110. Welche von den Verbraucherzentralen betriebenen Projekte zur Aufklärung von Verbraucherinnen und Verbrauchern zu verbraucherpolitischen Fragen im Netz unterstützt die Landesregierung und wie hoch ist die finanzielle Unterstützung des Landes für die Projekte jeweils?

Die Landesregierung unterstützt die Verbraucherzentrale mit einer institutionellen Förderung zur Finanzierung der Verbraucherinformation und Beratung. Diese Förderung betrug im Jahr 2013 insgesamt 1.477.790 €. Damit wird die Verbraucherzentrale unter anderem in die Lage versetzt, ihr Internetangebot zu betreiben. Auf dieser Seite haben Verbraucherinnen und Verbraucher u.a. Zugriff auf alle Musterbriefe der Verbraucherzentrale.

Ferner besteht seit dem Jahr 2006 eine Kooperation zwischen dem Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz und der Verbraucherzentrale Hessen im Blick auf die Erstellung und Qualitätssicherung von Fachbeiträgen für das Portal [www.verbraucherfenster.de](http://www.verbraucherfenster.de). Diese Dienstleistung wurde im Jahr 2013 mit 15.000 € gefördert.

In der Vergangenheit hat die Landesregierung zusätzlich die von der Verbraucherzentrale erstellten und betriebenen Seiten [www.berufsstarter.verbraucher.de](http://www.berufsstarter.verbraucher.de) und [www.lehrer.verbraucher.de](http://www.lehrer.verbraucher.de) (Lehrerinfothek) finanziert. Mit der Lehrerinfothek hat die Verbraucherzentrale Hessen Lehrerinnen und Lehrern einen Überblick über Materialien zu rechtlichen und wirtschaftlichen Verbraucherthemen angeboten, die für die Gestaltung des Unterrichtsangebotes geeignet - und nicht in Schulbüchern enthalten - sind. Aktuell gibt es Informationen für Lehrer unter <http://www.verbraucherbildung.de/materialkompass>.

Neben der Förderung von Einzelmaßnahmen sowie der institutionellen Förderung unterstützt die Landesregierung auch auf andere Weise die Angebote der Verbraucherzentrale Hessen. So hat sich Hessen mit einem Antrag zur Verbraucherschutzministerkonferenz 2014 dafür stark gemacht, dass das von der Verbraucherzentrale Hessen betriebene Portal [www.lebensmittelklarheit.de](http://www.lebensmittelklarheit.de) auch künftig vom Bund finanziert wird. Dieses Portal übt nach Ansicht der Landesregierung eine wichtige Marktwächterfunktion aus. Ferner wird damit der gewünschte Dialog zwischen den Kunden der Lebensmittelindustrie sowie dem Handel hergestellt. Hierdurch wird ein Beitrag geleistet, Lebensmittelverpackungen so zu gestalten, dass Verbraucherinnen und Verbraucher sich nicht getäuscht fühlen.

Die Landesregierung hat ferner gegenüber der Verbraucherzentrale Hessen den Wunsch deutlich gemacht, dass mittelfristig auch den hessischen Verbraucherinnen und Verbrauchern die Möglichkeit einer Beratung per E-Mail zur Verfügung steht.

Das Internet und andere Medien können aber den persönlichen Kontakt zu den Verbraucherinnen und Verbrauchern nicht ersetzen. Dafür unterhält die Verbraucherzentrale Hessen derzeit 8 Verbraucherberatungsstellen.

### **Diskriminierungsfreier Zugang**

Frage 111. Welche Bedeutung hat aus Sicht der Landesregierung der diskriminierungsfreie Zugang zum Internet für die digitale Teilhabe?

Ein diskriminierungsfreier Zugang zum Internet ist die unabdingbare Voraussetzung für die Teilhabe aller Bevölkerungsgruppen an der Informationsgesellschaft. Die Kommunikationsmöglichkeiten über das Internet in seiner Funktion als offenes und freies Medium müssen gewährleistet bleiben; jede Form der Diskriminierung im Netz ist zu vermeiden.

Anlass zur Sorge ist jedoch das Bestehen einer "digitalen Kompetenzlücke": So weist die EU-Kommission in ihrem "Fortschrittsanzeiger 2014" zur Digitalen Agenda darauf hin, dass in Europa nach wie vor eine "Unterschicht der digitalen Analphabeten" zu entstehen drohe, da 20 % der Europäer zu den mehr oder weniger bekennenden "Offlinern" gehören.

Ein barrierefreies, schnelles Internet wird immer mehr die Grundlage unseres wirtschaftlichen Handelns. Zugleich wird die Breitbandversorgung auch ein immer wichtigeres gesellschaftspolitisches Instrument. Nur wenn es uns gelingt, Hessen flächendeckend mit schnellem Internet zu erschließen, bleiben auch Regionen abseits der Ballungsräume attraktiv. Für Projekte, die im Rahmen des besonderen Breitband-Darlehens- und Bürgerschaftsprogramms (siehe hierzu auch Antwort zu Frage 114) und unter der geltenden "Bundesrahmenregelung Leerrohre" umgesetzt werden, ist der diskriminierungsfreie Zugang auf Vorleistungsebene ("open access") weiteren Netzbetreibern und Diensteanbietern verpflichtend vom Netzbetreiber zu gewähren.

Frage 112. Hält die Landesregierung den bestehenden Rechtsrahmen zur Herstellung bzw. Sicherung der Netzneutralität für angemessen?

Aus Sicht der Landesregierung ist der bestehende Rechtsrahmen für derzeitige Geschäftsmodelle der Telekommunikationsnetzbetreiber in Deutschland zwar weitgehend ausreichend, bietet aber

keine angemessenen Regelungen zur Wahrung der Netzneutralität für künftige Entwicklungen, insbesondere bezüglich einer zu erwartenden Zunahme von kostenpflichtigen Spezialdiensten.

Frage 113. Welchen Anpassungsbedarf sieht die Landesregierung zur weiteren Absicherung der Netzneutralität?

Die Regelung von Netzneutralität ist Gegenstand des Vorschlags einer Verordnung des Europäischen Parlamentes und des Rates über Maßnahmen zum europäischen Binnenmarkt der elektronischen Kommunikation und zur Verwirklichung des vernetzten Kontinents und zur Änderung der Richtlinien 2002/20/EG, 2002/21/EG und 2002/22/EG und der Verordnungen (EG) Nr. 1211/2009 und (EU) Nr. 531/2012COM (2013) 627final, BR-Drucksache 689/13. Die Landesregierung wird den Prozess aktiv begleiten und sich für einen diskriminierungsfreien Zugang zu Inhalten und Diensten im Internet sowie für eine diskriminierungsfreie Datenübermittlung einsetzen. Sie ist sich bewusst, dass es technische und wirtschaftliche Gründe für eine Nichtgleichbehandlung sämtlicher Datenpakete im Internet gibt. Bisher funktionierende Dienste unter Nutzung von z.B. Voice-over-IP oder Quality-of-Service-Angebote für Geschäftskunden sind auch volkswirtschaftlich von großer Bedeutung und deshalb weiterhin zu ermöglichen. Um das offene Internet jedoch nicht durch ein zunehmendes Angebot von Spezialdiensten zu gefährden, soll in künftigen Regelungen, wie auch vom Bundesrat in seinem Beschluss zum Entwurf der Digital Single Market Initiative der EU-Kommission (BR-Drs. 689/13) vorgeschlagen, ein klares Regel-Ausnahme-Verhältnis zugunsten des offenen Internets gegenüber Spezialdiensten festgelegt werden.

Das sogenannte "Offene Internet" soll den Regelfall darstellen, Spezialdienste sollen hingegen die Ausnahme bleiben. Anderenfalls bestünde die Gefahr, dass die meist auf höhere Gewinnerzielung angelegten Spezialdienste das offene Internet so einschränken, dass Bevölkerungsteile von einer umfassenden Nutzung des Internets als Informationsquelle und -träger ausgeschlossen werden. Die Überwachung der Einhaltung der Diskriminierungsfreiheit sowie gegebenenfalls Sanktionierungen sollen durch die nationale Regulierungsbehörde erfolgen.

Der gültige Rechtsrahmen ermöglicht es der Landesregierung, die Herstellung und Sicherung der Netzneutralität zu begleiten und ihr Verständnis von Netzneutralität in die entsprechenden Prozesse einfließen zu lassen. Auf Bundesebene besteht derzeit mit der Verordnungsermächtigung des § 41a des Telekommunikationsgesetzes eine Möglichkeit, flexibel regulierend die Anforderungen an eine diskriminierungsfreie Datenübermittlung und einen diskriminierungsfreien Zugang zu Inhalten und Anwendungen zu bestimmen. In diesem Zusammenhang hatte das Bundesministerium für Wirtschaft und Energie einen Entwurf einer Verordnung zur Gewährleistung der Netzneutralität vorgelegt (<http://www.bmwi.de/DE/Themen/Digitale-Welt/Digitale-Infrastrukturen/netzneutralitaet,did=577722.html> - abgerufen am 17.06.2014).

Die Landesregierung schließt sich der Sichtweise der Bundesregierung an und geht von der rechtlichen Umsetzung der Regulierung der Netzneutralität auf europäischer Ebene sowie einer Ausgestaltung dieses Ziels auch auf der Basis von freiwilligen Vereinbarungen aus. Derzeit ist die Diskussion um die Digital Single Market Initiative der Europäischen Kommission abzuwarten.

Frage 114. Mit welchen Maßnahmen unterstützt die Landesregierung den Ausbau der Breitband-Infrastruktur in Hessen?

Hessen hat schon 2010 den Aufbau einer leistungsfähigen digitalen Infrastruktur als einen zentralen Schlüsselfaktor für die Zukunftssicherung des Landes erkannt und das Projekt "Mehr Breitband in Hessen" initiiert. Ein Ziel der im Projekt entwickelten NGA-Strategie ist es, Ende 2018 für Hessen eine flächendeckende Versorgung mit schnellem Internet zu erreichen.

Dazu wurden seitens des Landes ein Darlehens- und Bürgschaftsprogramm über 350 Mio. € aufgelegt. Zusätzlich wurden mit EU-, Bundes- und Landesfördermitteln den Landkreisen weitere Förderinstrumente zur Verfügung gestellt. Dazu gehören GRW-Mittel für die Erschließung von Gewerbegebieten, EFRE-Mittel zur Förderung von Breitbandberatungsstellen sowie Machbarkeits- und Umsetzungsstudien, IKZ-Mittel zur Förderung von interkommunaler Zusammenarbeit bei Breitbandclustern. ELER-Mittel sind für die Breitbandförderung im ländlichen Raum angemeldet.

Da der marktgetriebene Breitbandausbau allein nicht ausreicht, um Breitband für alle Bürgerinnen und Bürger des Landes zu erschwinglichen Preisen flächendeckend zugänglich zu machen, kommt den kommunalen Unternehmen hierbei große Bedeutung zu. Mit der Änderung der Hessischen Gemeindeordnung trägt die Landesregierung diesem Sachverhalt Rechnung.

Das Land Hessen setzt neben der monetären Förderung auf intensive Beratung durch ein kaskadierendes Informationssystem: Die 21 hessischen Breitband-Landkreiskoordinatoren werden durch die vier regionalen Breitbandberater des Landes unterstützt und durch die Geschäftsstelle Breitband des Landes koordiniert. Mit dem hessischen Breitband-Informationssystem (hesbis)

können alle regionalen Akteure Ausbaumaßnahmen planen und dokumentieren. Das Informationsangebot wird durch einen Webauftritt, den jährlich stattfindenden Breitbandgipfel, verschiedene Fachveranstaltungen und diverse Leitfäden abgerundet.

Frage 115. Wie beurteilt die Landesregierung die vorhandene Datenlage zum Stand des Breitbandausbaus in Hessen?

Das Projekt "Mehr Breitband in Hessen" unterstützt alle hessischen Landkreise bei der Planung und Durchführung des Infrastrukturausbaus. Integraler Bestandteil dieses Prozesses ist die Durchführung einer vom Land geförderten NGA-Machbarkeitsstudie durch die Landkreise. In die Studie fließen sowohl bereits vorhandene Angebote der Netzanbieter vor Ort ein, als auch Planung und Bedarf an breitbandigen Zugängen. Zusätzlich werden Versorgungsdaten aus dem Bundesbreitbandatlas und dem Infrastrukturatlas des Bundes generiert. Darüber hinaus stellen Anbieter dem Land und den Kommunen ihre Daten direkt zur Verfügung. Daraus lässt sich ableiten, wo welche Ausbauaktivitäten notwendig sind, um die Region in der Fläche zu erschließen. Weitere umfassende Informationen bietet das landeseigene Informationssystem "hesbis", das als integriertes System (Kartendarstellung) alle relevanten Informationen zum Breitbandausbau in Hessen allen Akteuren, auch den Bürgerinnen und Bürgern, zur Verfügung stellt.

Frage 116. Wie beurteilt die Landesregierung das Konzept einer Breitband-Universaldienstverpflichtung?

Grundsätzlich sollte der Breitbandausbau primär marktgetrieben erfolgen und im ländlichen Raum durch Kooperationsmodelle mit Telekommunikationsbetreibern und kommunale Aktivitäten beschleunigt werden. Im Einklang mit den europäischen Beihilfavorschriften wird der Ausbau durch Förderungen flankiert.

Bei der Auferlegung von Universaldienstverpflichtungen sind wettbewerbsverzerrende Wirkungen, negative Investitionsanreize und hohe Kosten zu befürchten.

Frage 117. Wie wirkt sich eine Breitband-Universaldienstverpflichtung aus Sicht der Landesregierung auf die Geschwindigkeit des Breitband-Ausbaus in Hessen aus?

Gemäß Tätigkeitsbericht Telekommunikation 2012/2013 der Bundesnetzagentur wurden Mitte 2013 von insgesamt anschließbaren 40,7 Millionen Haushalten in Deutschland nur insgesamt 28,4 Millionen Breitbandanschlüsse genutzt.

Die vermarktete Bandbreite verteilte sich prozentual folgendermaßen:

6,3 % bis zu 2 Mbit/s,  
 8,3 % 2 Mbit/s,  
 32,0 % über 2 MBit/s bis unter 10 Mbit/s,  
 39,4 % 10 Mbit/s bis unter 30 MBit/s,  
 12,2 % 30 MBit/s bis unter 100 MBit/s,  
 1,8 % über 100 MBit/s.

Der Landesregierung liegen keine genauen Angaben darüber vor, welche genaue Bandbreite aktuell tatsächlich von der Mehrzahl der deutschen Haushalte bzw. Bürger genutzt wird. Es ist aber davon auszugehen, dass diese Bandbreite deutlich unter 30 MBit/s liegt.

In Hessen sind in allen hessischen Landkreisen Ausbauaktivitäten in verschiedenen Phasen zu verzeichnen, die sich an der in der hessischen NGA-Strategie verankerten Bandbreite von 50 MBit/s orientieren.

Eine Auferlegung einer Universaldienstverpflichtung zum jetzigen Zeitpunkt würde sowohl zu einer Absenkung der Ausbau-Bandbreite als auch zu einer deutlichen Verlangsamung der Ausbaugeschwindigkeit führen. Investierende Unternehmen würden massiv verunsichert; Planungen in Kommunen würden erschwert oder abgebrochen. Der bürokratische Aufwand zur Umsetzung eines Universaldienstes würde zu einer weiteren deutlichen Verzögerung des Breitbandausbaus führen.

Frage 118. Welche Maßnahmen zur Förderung der freien Nutzung öffentlicher WLANs plant die Landesregierung?

Frage 119. Welchen rechtlichen Handlungsbedarf sieht die Landesregierung hierbei?

Die Fragen 118 und 119 werden gemeinsam beantwortet.

W-LAN (wireless-local-area-network) bezeichnet ein lokales Funknetz. Die signifikante Verbreitung von Drahtlosnetzwerken unterstreicht die Entwicklung zu mehr Mobilität und flexibleren Arbeitsbedingungen. Seitdem die Debatte über Cybersicherheit zunehmend auch in der Öffentlichkeit diskutiert wird, ist deutlich geworden, dass das Internet ohne Sicherheit nicht denkbar ist. Das Land Hessen befürwortet den Aufbau privater WLAN-Netze in Ergänzung der lei-

tungsgebundenen- und der mobilfunkbasierten Infrastruktur. Derzeit sind Techniken im Einsatz oder in der Erprobung, die eine private und gleichzeitig systemgetrennte öffentliche Nutzung desselben Netzes vorsehen, wobei die Gewährleistung der Datensicherheit hier Priorität hat. Aufgrund dieser Erfahrungen sind die Ergebnisse auszuwerten und im Nachgang zu prüfen, ob die Rechtslage ausreichend ist.

Die Förderung der freien Nutzung von W-LAN-Netzen könnte durch Beschränkung des Haftungsrisikos für W-LAN Betreiber erfolgen, indem die Haftungsbeschränkung für Access-Provider gemäß § 8 Telemediengesetz (TMG) auf andere Betreiber erweitert wird. Hierdurch würde mehr Schutz vor Haftungs- und Abmahnrisiken gewährt, die oftmals die Bereitschaft behindern, öffentliche W-LAN Netze beispielsweise in Cafés oder Hotels zu betreiben.

### **Altersgruppenspezifische Fragestellungen: Kinder (6- bis 13-Jährige)**

Frage 120. Welche Herausforderungen ergeben sich aus Sicht der Landesregierung, um den Verbraucherschutz im Internet speziell für Kinder zu verbessern?

Die veränderten Nutzungsformen durch das Internet und neue Mediengewohnheiten erfordern es, bestehende Lücken im Kinder- und Jugendmedienschutz zu schließen und rechtliche Rahmenbedingungen anzupassen. Besondere Aufmerksamkeit verdienen dabei Altersangaben von Apps und Webseiten, freiwillige Selbstkontrollen der Anbieter und Jugendschutzprogramme.

Frage 121. Erkennt die Landesregierung geschlechtsspezifische Herausforderungen für den Verbraucherschutz im Internet speziell für Kinder?

Frage 122. Welche konkreten Maßnahmen plant oder vollzieht die Landesregierung, um Kinder über die für ihre Altersgruppe spezifischen Risiken im Internet aufzuklären?

Die Fragen 121 und 122 werden zusammen beantwortet.

Alle hessischen Schulen vermitteln "Medienerziehung" als Teil von Medienbildung im Unterricht und im Rahmen des Schullebens auf altersgerechte Weise. Dabei wird auch das unterschiedliche mediale Nutzungsverhalten von Jungen und Mädchen angemessen berücksichtigt. Darüber hinaus setzen einzelne Schulen in Abhängigkeit vom Schulprofil individuelle Schwerpunkte für Medienbildung.

In ihrer Unterrichtsentwicklung werden die Schulen dabei durch die Fachberater/-innen Medienbildung an den Staatlichen Schulämtern, durch externe Medienpädagogen etwa über die Medienanstalten, die mit dem Kultusministerium kooperieren, sowie durch altersspezifische Schulprojekte unterstützt.

Ein wichtiger Kooperationspartner ist in diesem Zusammenhang die Landesanstalt für privaten Rundfunk und Neue Medien (LPR), die seitens des Kultusministeriums auf der Basis einer Kooperationsvereinbarung für die Umsetzung schulischer Medienkompetenzprojekte finanziell unterstützt wird. So werden beispielsweise im Rahmen des Projekts "Webklicker - Wir klicken clever! Sicheres Surfen im Netz" Fünft- und Sechstklässler auf den sicheren Umgang mit dem Internet vorbereitet, indem sie in zwei Projekttagen Wissen rund um das Internet und Aufklärung über richtiges Verhalten in Sozialen Netzwerken und Chaträumen erhalten und das Erlernete auf einer Webseite dokumentieren. Diese Webseite wird den Eltern präsentiert. Durch eine begleitende Lehrerfortbildung soll das Wissen zum Thema nachhaltig in der Schule verbleiben.

Im vergangenen Schuljahr startete das Kooperationsprojekt "Internet ABC" für hessische Grundschulen mit der LPR, das insbesondere den jungen Schülern sicheres Surfen und die Grundregeln im Umgang mit dem Internet vermitteln soll. Auch in dieses Projekt sind die Eltern durch einen Elternabend mit einbezogen. Seitens des Kultusministeriums wird das Projekt durch die Fachberater Medienbildung durch Fortbildungen und pädagogisches Begleitmaterial für Lehrkräfte intensiv begleitet.

Die Hessische Polizei vermittelt Kindern von sechs bis zehn Jahren über die programmunterlegte Sympathiefigur "Kinderkommissar LEON" ([www.polizei.hessen.de/LEON](http://www.polizei.hessen.de/LEON)) u. a. auch Präventionsinhalte "Rund ums Internet". Hierin wird auf das "sichere Chatten" und "sichere Surfen" hingewiesen. Abgerundet wird die Thematik in einer Aufzählung "sicherer Links", um weitergehende, altersgerecht aufbereitete Informationen zu erhalten.

Im Übrigen wird auf die Antworten zu den Fragen 28 und 40 verwiesen.

Frage 123. Wie werden hierbei insbesondere Soziale Netzwerke - einerseits als Kommunikationskanal, andererseits als eigenes Thema von verbraucherpolitischem Belang - einbezogen?

Die unter der Antwort zu Frage 122 genannten Maßnahmen enthalten die Aufklärung über den sicheren Umgang mit Sozialen Netzwerken.

Aktuell testet die Hessische Polizei die virale Wirkung Sozialer Netzwerke (Twitter, Facebook) in Frankfurt am Main, ohne allerdings einen speziellen Focus auf die Altersgruppe der Kinder von 6 bis 13 Jahren zu legen. Die polizeiliche Aufgabe erstreckt sich innerhalb der angefragten Altersgruppe auf die Vermittlung von Informationen über Gefahren.

Frage 124. Gibt es Kooperationen der Landesregierung mit einzelnen Betreibern von Sozialen Netzwerken zur Gewährleistung des Verbraucherschutzes von Kindern?

Die Zusammenarbeit mit Betreibern bezieht sich auf den anlassbezogenen Informationsaustausch sowie auf Datenerhebungen im Rahmen der gesetzlichen Vorgaben, insbesondere denen des Telemediengesetzes in Verbindung mit den strafverfahrens- und gefahrenabwehrrechtlichen Eingriffsbefugnissen. Beispielhaft erfolgte die Information des Betreibers einer Diskussionsplattform für Kinder über systembedingte Tatgelegenheiten, die im Zuge der umfangreichen Ermittlungen des Hessischen Landeskriminalamtes wegen sexuellen Missbrauchs über diese Plattform bekannt wurden.

Die Täter nutzten technische Schwachstellen des Systems gezielt aus, um als Kinder/Jugendliche legiert mit sexueller Zielrichtung Kontakt zu Kindern aufzunehmen. Grundsätzlich erfolgt der Informationsaustausch über die von den obersten Landesjugendbehörden eingerichtete gemeinsame Stelle "jugendschutz.net" mit Sitz in Mainz und dient in erster Linie dem Jugendschutz, nicht dem Verbraucherschutz.

Frage 125. Welche Maßnahmen ergreift die Landesregierung, um die Möglichkeiten des Internets und seine Nutzung bereits im Vorschul- und Primärbereich zu thematisieren?

Auf die Antwort zu Frage 122 wird verwiesen.

Frage 126. Welche Maßnahmen und Strukturen unterstützt die Landesregierung, um Hilfs- und Beratungsangebote für Eltern vorzuhalten, wenn ihre Kinder Probleme mit Rechtsunsicherheiten im Internet haben (bitte aufschlüsseln nach Rechtsform des Trägers, Ort sowie Form der Unterstützung)?

Das Netzwerk gegen Gewalt (Initiative der Staatskanzlei, des Ministeriums des Innern und für Sport, des Kultusministeriums, des Ministeriums für Soziales und Integration und des Ministeriums der Justiz und des Landespräventionsrates) befasst sich im Auftrag der Landesregierung seit 2007 mit dem Thema "Medienkompetenz für Erwachsene". Ein Internetauftritt und Fortbildungsangebote wurden erarbeitet, um die Zielgruppe der Erwachsenen, die beruflich oder privat mit Kindern und Jugendlichen zusammenarbeiten, besser informieren zu können. Zukünftige Fortbildungen zielen insbesondere auf die Weiterqualifizierung bereits ausgebildeter Multiplikatoren sowie auf die regionale Vernetzung im Bereich Medien ab.

Die Landesregierung unterstützt die Verbraucherzentrale Hessen und den DHB-Netzwerk Haushalt Hessen mit einer institutionellen Förderung zur Finanzierung der Verbraucherinformation und Beratung.

In ihrem Portal [www.verbraucherfenster.de](http://www.verbraucherfenster.de), das sich an Verbraucherinnen und Verbraucher richtet, informiert die Landesregierung regelmäßig auch über Risiken im Internet sowie von diesen ausgehenden Gefahren in Form von Beiträgen.

Frage 127. Welche Untersuchungen zur Erforschung des konkreten Gefährdungspotenzials für Kinder im Internet sind der Landesregierung bekannt und wie unterstützt die Landesregierung die Gewinnung weiterer Erkenntnisse (Forschungsprojekte bitte einzeln mit Art und Umfang der Unterstützung aufführen)?

Insbesondere die folgenden Studien sind der Landesregierung bekannt und werden als unterschiedlich aussagefähig eingestuft, aber nicht finanziell und anderweitig unterstützt:

KIM-Studie 2012 (Kinder, Medien, Computer + Internet) vom Medienpädagogischen Forschungsverbund Südwest, Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger in Deutschland.

JIM-Studie 2013 (Jugend, Information, (Multi-)Media)) vom Medienpädagogischen Forschungsverbund Südwest, Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland.

U25-Studie 2014 Kinder, Jugendliche und junge Erwachsene in der digitalen Welt vom Deutschen Institut für Vertrauen und Sicherheit im Internet (DIVSI).

Cyberlife - Spannungsfeld zwischen Faszination und Gefahr: Cybermobbing bei Schülerinnen und Schülern, Bündnis gegen Cybermobbing 2013.

Die Fachhochschule Frankfurt am Main verweist auf medienpädagogisch-technische Unterrichtsbegleitung ([www.unterrichtsbegleitung.de](http://www.unterrichtsbegleitung.de)), die in Zusammenarbeit mit ihrem fachbe-

reichsübergreifenden wissenschaftlichen Zentrum durchgeführt wird. Die Lehrerinnen und Lehrer werden bei der Durchführung medienpädagogischer Projekte unterstützt und mit dem Ziel begleitet, Medienkompetenz im Rahmen schulischer Medienbildung und Medienintegration zu vermitteln.

Für die o.g. Untersuchungen findet keine Einzelunterstützung statt, die Hochschulen werden seitens der Landesregierung im Rahmen des Globalbudgets finanziert.

Frage 128. Wie bewertet die Landesregierung vor dem Hintergrund der bekannten Forschungsergebnisse die vorhandenen Schutzmechanismen für Internetnutzerinnen und -nutzer im Kindesalter?

Für Nutzerinnen und Nutzer im Kindesalter stehen mehrere Webseiten und Browser unterschiedlicher Anbieter zur Verfügung, die mit Positivlisten (white lists) arbeiten. Zusammen mit auf den Geräten eingerichteten eingeschränkten Nutzerkonten für das einzelne Kind oder Gruppen von Kindern bieten diese ausreichenden Schutz. Es ist jedoch seitens der Eltern bzw. der Personen, denen Kinder anvertraut werden, darauf zu achten, dass Kinder nur auf solche Geräte Zugriff haben, die mit diesen Sicherungsmaßnahmen ausgestattet sind. Eltern, Pädagoginnen und Pädagogen sowie Sozialarbeiterinnen und Sozialarbeiter sind fortwährend zu sensibilisieren, zu informieren und fortzubilden. Hierzu gibt es seitens des Kultusministeriums zahlreiche regionale und landesweite Maßnahmen.

Zu nennen sind hier insbesondere das Projekt "Internet-ABC" an Grundschulen, das in Kooperation mit der Landesanstalt für privaten Rundfunk und neue Medien umgesetzt wird und sowohl die Fortbildung von Lehrkräften als auch die Information von Eltern umfasst, sowie die landesweite Fortbildungsreihe für Lehrkräfte zu Jugendmedienschutzberaterinnen und -beratern.

Frage 129. Wie beurteilt die Landesregierung die aktuellen gesetzlichen Regelungen zu der Frage, ob Eltern für die Kosten, die ihr minderjähriges Kind über kostenpflichtige Angebote im Netz verursacht, haften?

Frage 130. Wie beurteilt die Landesregierung die aktuellen gesetzlichen Regelungen zur Haftungspflicht der Eltern für Kosten durch vermeintlich kostenlose Online- bzw. Browser-Games, die sich insbesondere an Kinder richten und bei denen Kosten erst im Laufe des Spiels entstehen?

Die Fragen 129 und 130 werden gemeinsam beantwortet.

Bei Frage 129 wird zunächst davon ausgegangen, dass hiermit keine Sachverhalte bewertet werden sollen, bei denen ein minderjähriges Kind oder ein minderjähriger Heranwachsender sich über das Internet Inhalte herunterlädt, die - z.B. wegen einer Urheberrechtsverletzung, wie im Fall von Musiktauschbörsen - Zahlungspflichten auslösen könnten, etwa in Form eines Schadensersatzanspruchs nach § 97 Abs. 2 des Urheberrechtsgesetzes.

Für kostenpflichtige Angebote im Internet gelten grundsätzlich die allgemeinen Regelungen des Bürgerlichen Gesetzbuchs (BGB).

Dies bedeutet, dass auch im Falle der Bestellung von Dienstleistungen oder Waren uneingeschränkt die Bestimmungen über die Geschäftsfähigkeit nach den §§ 104 ff. BGB zur Anwendung gelangen. Danach sind Kinder, die das siebente Lebensjahr noch nicht vollendet haben, geschäftsunfähig mit der Folge, dass sie keine wirksame Willenserklärung abgeben können (§§ 104 Nr. 1, 105 BGB), somit auch kein Vertragsschluss zustande kommen kann.

Kinder und Jugendliche ab dem siebenten und vor Vollendung des achtzehnten Lebensjahrs sind demgegenüber beschränkt geschäftsfähig (§ 106 BGB) mit der Folge, dass die Wirksamkeit eines Vertrages von der (nachträglichen) Genehmigung des gesetzlichen Vertreters abhängt, sofern letzterer nicht bereits zuvor seine Einwilligung zur Abgabe der auf den Vertragsschluss gerichteten Willenserklärung des Minderjährigen gegeben hat (§§ 108, 107 BGB).

Eine Ausnahme bilden Willenserklärungen des Minderjährigen, durch die dieser lediglich einen rechtlichen Vorteil erlangt (§ 107 BGB). Diese Voraussetzung ist jedoch beim Abschluss kostenpflichtiger Geschäfte regelmäßig nicht gegeben.

Eine weitere Rückausnahme bildet die Bestimmung des so genannten "Taschengeldparagrafen" des § 110 BGB. Hiernach sind Geschäfte, die ein Minderjähriger mit seinem Taschengeld eigenständig tätigen kann und dies nach der Zweckbestimmung des ihm zur Verfügung gestellten Geldes auch darf, auch ohne Zustimmung des gesetzlichen Vertreters von Anfang an wirksam.

Hiernach könnte ein beschränkt geschäftsfähiger Minderjähriger auf elektronischem Weg wohl regelmäßig z.B. eine Zeichen-App für sein Tablet für 3,99 € erwerben oder einen anderen Kauf in dieser Größenordnung tätigen, sich jedoch nicht etwa zu einem Abonnement oder einem Vertrag mit einer Ratenzahlung verpflichten. Ob ein Vertrag nach Maßgabe von § 110 BGB wirksam ist, kann in Grenzfällen eine sorgfältige Einzelfallbetrachtung erforderlich machen.

Soweit der Taschengeldparagraf zur Anwendung gelangt oder eine Einwilligung vorliegt, wird der beschränkt geschäftsfähige Minderjährige und nicht sein gesetzlicher Vertreter Vertragspartner und damit auch Zahlungsschuldner.

In allen Fällen gilt, dass sich der Vertragspartner eines geschäftsunfähigen oder eines nur beschränkt geschäftsfähigen Minderjährigen auch im Bereich des elektronischen Geschäftsverkehrs nicht auf Vertrauensschutz berufen kann, wobei dies auch dann gilt, wenn der Minderjährige wahrheitswidrige Angaben über sein Alter gemacht haben sollte, da der Gesetzgeber dem Minderjährigenschutz absoluten Vorrang vor dem Vertrauens- und Verkehrsschutz eingeräumt hat (vgl. z.B. Härting, Internetrecht, 5. Aufl., 2014, RdZiff. 547, 549, m.w.N.; Ermann-Müller, BGB, 13. Aufl., 2011, Vor § 104, RdZiff. 7: Bereicherungsrechtliche Haftung nur bei Kenntnis des gesetzlichen Vertreters vom Mangel des rechtlichen Grundes).

Der Aspekt der fehlerhaften Altersangabe oder andere Formen der unerlaubten Handlung können jedoch zu einer Verantwortlichkeit nach den Vorschriften über unerlaubte Handlungen nach den §§ 823, 828 ff. BGB führen. Dies kann letztlich zu einer Haftung des Aufsichtspflichtigen oder gesetzlichen Vertreters des Minderjährigen nach Maßgabe von § 832 BGB mit der Möglichkeit des Entlastungsbeweises hinsichtlich der gehörigen Aufsicht oder der mangelnden Ursächlichkeit für den Schaden führen (Ermann-Müller, a.a.O., RdZiff. 7 und 9).

Einen zusätzlichen Schutz vor (übereilten) kostenpflichtigen Online-Bestellungen durch Verbraucherinnen und Verbraucher, ob minderjährig oder nicht, bietet seit dem 1. August 2012 die sogenannte "Button-Lösung" nach § 312g Abs. 3 und 4 BGB (seit dem 13. Juni 2014: § 312j Abs. 3 und 4 BGB). Hiernach kommt ein Vertrag im elektronischen Geschäftsverkehr nur zustande, wenn der Unternehmer seine Website so ausgestaltet hat, dass die Verbraucherin oder der Verbraucher bei ihrer/seiner Bestellung ausdrücklich bestätigen muss, dass sie/er sich zur Zahlung verpflichtet. Erfolgt die Bestellung über eine "Schaltfläche" (insbesondere über einen Button), muss die "Schaltfläche" gut lesbar mit nichts anderem als den Worten "zahlungspflichtig bestellen" oder mit einer entsprechenden eindeutigen Formulierung beschriftet sein (§ 312 g Abs. 3 Satz 2 BGB, ab dem 13.6.2014: § 312 j Abs. 3 Satz 2 BGB).

Soweit mit Frage 130 offenbar das Phänomen des sogenannten "Anfütterns" nicht zuletzt von minderjährigen Kunden angesprochen wird, gilt es, das tatsächliche Marktgeschehen weiter zu beobachten. Unabhängig davon ist vor allem auf eine Stärkung der Medienkompetenz von Eltern und Kind zu setzen.

Der Schutz der Kinder und Jugendlichen liegt grundsätzlich in der Verantwortung des Elternhauses. Wenn die Erziehungsberechtigten ihr Kind mit Bildschirmmedien, z.B. Smartphones, ausstatten, sollten sie sich auch über die möglichen Folgen und Konsequenzen einer uneingeschränkten Nutzung durch ihr Kind bewusst sein und entsprechende Vorkehrungen treffen. Hier wird z.B. ein "Nutzungsvertrag" mit den Heranwachsenden empfohlen, der genau festlegt, in welchem zeitlichen und inhaltlichen Umgang die Nutzung erfolgen darf. Z.B. sollte für ein Kind kein Administratorkonto, sondern ein eingeschränktes Benutzerkonto am Computer eingerichtet werden. Onlineaktivitäten eines Kindes sollten von den Eltern begleitet werden. In diesem Zusammenhang kann auch auf das Gefahrenpotenzial von Kostenfallen wie Online- bzw. Browser-Games von den Eltern aufmerksam gemacht werden. In fürsorglicher Kooperation mit dem Elternhaus unterstützt die Schule im Rahmen ihres Bildungs- und Erziehungsauftrags die Aufgabe der Medienerziehung.

### **Jugendliche (12- bis 19-Jährige)**

Frage 131. Welche Herausforderungen ergeben sich aus Sicht der Landesregierung, um den Verbraucherschutz im Internet speziell für Jugendliche zu verbessern?

Für Jugendliche ist die Nutzung des Internets ein integraler und selbstverständlicher Bestandteil ihres Lebensalltags. Damit verbunden sind sowohl Chancen, die das Internet bietet als auch zahlreiche Risiken, die zu Gefahren im realen Alltag werden können. Dazu zählen neben Phänomenen wie Onlinesucht, sexuellem Missbrauch, Cybermobbing u.v.m. auch alle Bereiche des Datenmissbrauchs und der Abzocke.

Die Landesregierung sieht Prävention und Information als die wichtigsten Elemente an, um Jugendliche vor Gefahren zu schützen und so Medienkompetenz im Umgang mit dem Internet zu erlangen. Des Weiteren wirkt die Landesregierung darauf hin, dass möglichst viele große Betreiber wie z.B. Google den Jugendschutz einhalten. Unter anderem geschieht dies durch die Initiative "sicher online gehen". Hier setzen sich Bund, Länder und Wirtschaft für einen besseren Schutz von Kindern im Internet ein. Gemeinsam sollen Eltern für Risiken im Netz sensibilisiert, bei der Medienerziehung ihrer Kinder unterstützt und über technische Schutzlösungen informiert werden. Der Initiative gehören fast alle großen Wirtschaftsunternehmen und Verbände, wie z.B. Google, Facebook, Telekom u.v.a. an. Diese Partner leisten ihren Beitrag, um einen

sicheren Surfraum zu entwickeln und die Wirksamkeit anerkannter Jugendschutzprogramme zu fördern.

Insbesondere im Bereich Apps gibt es verschiedene Herausforderungen. Im Juni 2013 hatte das Projekt "Verbraucherrechte in der digitalen Welt" des Bundesverbandes Verbraucherzentrale (vzbv) exemplarisch einige Apps überprüft, die sich durch die Art und inhaltliche Gestaltung speziell an Kinder richten. Dabei wurden teilweise Mängel in der verbraucherfreundlichen Anwendbarkeit festgestellt. Laut des Verbraucherzentrale Bundesverbandes sollten Eltern und Kinder/Jugendliche vor dem Herunterladen einer Kinder-App über relevante Inhalte wie Altersempfehlung, Kostenpflicht der App, Vertragslaufzeit, Abonnements, Finanzierung der App (Werbung, In-App-Käufe etc.) aber auch in Bezug auf In-App-Käufe jeweils der Zielgruppe angemessen und in verständlicher Sprache informiert werden. Zudem sollten sich die AGB und Datenschutzbestimmungen nach Auffassung der Verbraucherzentrale Bundesverband auf die für das betreffende App-Angebot relevanten Inhalte beschränken und sich sprachlich und gestalterisch an den Bedürfnissen und Fähigkeiten der Zielgruppe orientieren.

Frage 132. Erkennt die Landesregierung geschlechtsspezifische Herausforderungen für den Verbraucherschutz im Internet speziell für Jugendliche?

Die Landesregierung sieht ein unterschiedliches mediales Nutzungsverhalten von Mädchen und Jungen. Während Mädchen und junge Frauen Online-Communities bzw. Soziale Netzwerke bevorzugen, konsumieren Jungen und junge Männer deutlich mehr Computer-, Konsolen- oder Onlinespiele (vgl. JIM-Studie 2013). Dies hat Einfluss auf das jeweilige Gefährdungspotenzial.

Frage 133. Welche konkreten Maßnahmen plant oder vollzieht die Landesregierung, um diesen Herausforderungen zu begegnen?

Grundprinzip der pädagogischen Arbeit ist ein auf die Zielgruppe zugeschnittenes Angebot. In Hessen gibt es zahlreiche Angebote, die präventiv im Sinne der Erlangung von Medienkompetenz nach diesem Prinzip arbeiten, wie z.B. Angebote des Netzwerks gegen Gewalt, die Hessischen Jugendschutzmeetings sowie Angebote kommunaler und freier Träger.

Frage 134. Wie bewertet die Landesregierung das Risiko, das von speziell auf diese Altersgruppen zugeschnittenen "Abo-Fallen" ausgeht?

Das Phänomen "Abo-Fallen" wird statistisch nicht gesondert, sondern lediglich als "normaler" Betrug erfasst, so dass sich valide Aussagen anhand von Zahlenmaterial nicht treffen lassen. Durch die Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) wurde berichtet, dass die dort vorliegenden Erkenntnisse sowie der Blick in die einschlägigen Internetforen die Einschätzung zulassen, dass gerade auch die strafgerichtliche Rechtsprechung dazu geführt hat, dass die Problematik inzwischen deutlich eingedämmt erscheint. Der Bundesgerichtshof hat jüngst mit Urteil vom 5. März 2014 (Az.: 2 StR 616/12) die Revision eines wegen Betrugs verurteilten Betreibers einer "Abo-Fallen-Webseite" verworfen und ausgeführt, dass durch die auf Täuschung abzielende Gestaltung der Internetseite die Kostenpflichtigkeit der angebotenen Leistung gezielt verschleiert worden sei. Dies stelle eine Täuschungshandlung im Sinne des § 263 StGB dar. Die Erkennbarkeit der Täuschung bei sorgfältiger Lektüre schließe die Strafbarkeit nicht aus, denn die Handlung sei gerade im Hinblick darauf unternommen worden, die bei einem - wenn auch nur geringeren - Teil der Benutzer vorhandene Unaufmerksamkeit oder Unerfahrenheit auszunutzen.

Gleichwohl sind "Abo-Fallen-Angebote" nach wie vor aufzufinden, wobei diese sich nach Einschätzung der ZIT mehr in den Bereich der mobilen Endgeräte zu verlagern scheinen.

Darüber hinaus ist bedeutsam, dass Vertragsabschlüsse bis zur Volljährigkeit aufgrund der beschränkten Geschäftsfähigkeit grundsätzlich schwebend unwirksam sind und nur eingeschränkt zu einer Haftung führen. Gleichwohl sind kostenpflichtige Angebote im Internet verfügbar, die sich gezielt an Kinder, Jugendliche und/oder Heranwachsende richten. Das Risiko, Opfer einer "Abo-Falle" zu werden, sinkt erheblich mit dem Grad der Aufklärung über aktuelle Phänomene und der Darstellung von angemessenen Reaktionsmöglichkeiten.

Auf die Antworten zu den Fragen 23 und 16 wird verwiesen.

Frage 135. Welche Rolle spielt das Internet für die Landesregierung bei der Information von Jugendlichen hinsichtlich ihrer Verbraucherrechte?

Die Landesregierung stellt mit dem Verbraucherportal VerbraucherFenster ([www.verbraucherfenster.hessen.de](http://www.verbraucherfenster.hessen.de)) ein umfassendes Informationsangebot für alle Bürgerinnen und Bürgern zur Verfügung, das auch Jugendlichen zugänglich ist. Das VerbraucherFenster informiert die Verbraucherinnen und Verbraucher in verschiedenen Rubriken umfassend zu einzelnen Themen und Fragestellungen. Diese Rubriken sind: Ernährung & Lebensmittel, Finanzen & Recht, Gesundheit & Soziales, Umwelt & Energie, Internet & Telekommunikation und sicher leben. Daneben sind Basisinformationen für Verbraucherinnen und Verbraucher in leicht verständlicher Form

abrufbar. Bei der Erstellung und Qualitätssicherung von Beiträgen für das Portal besteht seit Jahren eine Kooperation mit der Verbraucherzentrale Hessen. Insbesondere werden auch die für Jugendliche interessanten Themen rund um das Internet und damit verbundene Gefahren (Kinder-Apps, Datensicherheit, etc.) sowie das Thema Ernährung aufgegriffen.

Frage 136. Wie viele Fälle von "Cyber-Mobbing" sind in Hessen in den letzten fünf Jahren bekannt und zur Anzeige gebracht worden, und in wie vielen Fällen kam es zu einer Verurteilung (bitte Opfer und Täterinnen bzw. Täter geschlechtsspezifisch und nach Jahren getrennt aufschlüsseln)?

Opfer von Cybermobbing an hessischen Schulen werden nicht systematisch erfasst, so dass keine Erkenntnisse über Fallzahlen vorliegen. Informationen liefern hierzu bisher nur unterschiedliche Studien. Da eine Abgrenzung von Vorfällen hinsichtlich der Frage, ob es sich um (Cyber-) Mobbing handelt oder nicht, z.T. sehr schwierig zu treffen ist und jeder Fall sich individuell sehr unterschiedlich darstellt, sind empirisch gesicherte Daten in diesem Feld nur schwer zu ermitteln.

Das Phänomen Cyber-Mobbing wird auch innerhalb der hessischen Justiz mangels eines speziellen Tatbestandes statistisch nicht gesondert erfasst, so dass sich valide Aussagen anhand von Zahlenmaterial hierzu nicht treffen lassen. Zur näheren Erläuterung sowie zur ergänzenden Beantwortung wird auf die Ausführungen in der Vorbemerkung Bezug genommen.

Allerdings dürften statistische Erhebungen in diesem Phänomenbereich den eigentlichen Umfang der Problematik auch nicht oder nur höchst unzureichend widerspiegeln, da von einem erheblichen Dunkelfeld ausgegangen werden muss. Mobbingopfer trauen sich aus Angst vor weiteren Übergriffen häufig nicht, Anzeige zu erstatten. Die Anonymität des Internets macht es den Tätern überdies sehr einfach, ihre Identität zu verschleiern.

Angesichts der Bedeutung des Themas hat sich auch die diesjährige Justizministerkonferenz mit dem Phänomen Cyber-Mobbing befasst. Grundtenor war, dass es zur wirksamen Bekämpfung von Cyber-Mobbing mehr als nur der strafrechtlichen Sanktionierung bedürfe und begleitende Maßnahmen, wie etwa die Stärkung der Medienkompetenzen, erforderlich sind.

In der Polizeilichen Kriminalstatistik (PKS) ist der Begriff Cyber-Mobbing nicht definiert und wird somit nicht erfasst. Eine Auswertung für die Deliktsbereiche Nötigung (Schlüssel 232200), Bedrohung (Schlüssel 232300) und Nachstellung ("Stalking") (Schlüssel 232400 im Zusammenhang mit dem Sonderkennner "Internet" ergab folgendes Ergebnis:

Jahr	2009	2010	2011	2012	2013
Erfasste Fälle	374	408	382	503	523
Oper gesamt	399	431	407	533	552
Opfer männlich	165	175	158	193	183
Opfer weiblich	234	256	249	340	369
Tatverdächtige männlich	234	269	250	318	362
Tatverdächtige weiblich	89	64	78	105	98

Zusätzlich wurde eine PKS-Auswertung Beleidigung (Schlüssel 673000) mit dem Sonderkennner "Internet" durchgeführt. Für die Beleidigung erfolgt keine Erfassung von Opferdaten. Hier sind nur Angaben zum Tatverdächtigen erfasst.

Jahr	2009	2010	2011	2012	2013
Erfasste Fälle	591	664	780	721	907
Tatverdächtige männlich	283	334	360	386	500
Tatverdächtige weiblich	208	198	238	239	319

Zu Verurteilungen liegen keine polizeilichen Statistiken vor.

Frage 137. Wie werden das Thema "Cyber-Mobbing" und weitere, damit verwandte Problemlagen bisher in Schulen behandelt und welche Maßnahmen plant die Landesregierung, um diese Thematisierung zu intensivieren?

Zunächst wird auf die Antwort des Kultusministeriums zu der Kleinen Anfrage 19/321 verwiesen.

Neben verschiedenen, vorwiegend primärpräventiven Maßnahmen (z.B. Gewaltprävention und Demokratielernen (GuD), Prävention im Team (PiT), buddy und Faustlos), die bei Bedarf auf Mobbing eingehen, hat die Landesregierung auch konkrete Projekte bzw. Initiativen umgesetzt. Die Gefahr des Cyber-Mobbing als neuartiger Variante in Verbindung mit Smartphones, Inter-

net und Sozialen Netzwerken ist zwischenzeitlich verstärkt Gegenstand der Präventionsarbeit der Landesregierung und wird vor allem im Bereich "Jugendmedienschutz" aufgegriffen. Die Prävention von Cyber-Mobbing findet auf verschiedenen Ebenen statt:

1. Aufklärung und Information - thematisiert werden z.B. Schutz der Privatsphäre im Internet, die persönlichen Folgen für die Opfer, rechtliche Konsequenzen (z.B. bei Beleidigung, Verleumdung, übler Nachrede) für die Täter sowie Verhaltenstipps für Betroffene.
2. Schaffung eines lernförderlichen und gewaltfreien Klassen- und Schulklimas - z.B. durch Angebote wie "Peer-Learning", Streitschlichterausbildung, Mediation und konstruktive Konfliktbearbeitung, Klassenrat etc.

Um Mobbing an hessischen Schulen direkt vorzubeugen, hat das Kultusministerium gemeinsam mit der Techniker Krankenkasse (TK) die Initiative "Mobbingfreie Schule - gemeinsam Klasse sein!" ins Leben gerufen. Zentraler Bestandteil der Aktion ist eine Projektwoche, in deren Verlauf sich die Schülerinnen und Schüler der Klassenstufen fünf bis sieben aller allgemeinbildenden Schulen fünf Tage intensiv mit dem Thema beschäftigen. Sie erforschen in Übungen, Rollenspielen und Gesprächen, wie sie positiv und konstruktiv miteinander umgehen können. Zudem sprechen die Schülerinnen und Schüler über die Folgen der geistigen und körperlichen Attacken und lernen, was sie selbst tun können, um Mobbing gar nicht erst entstehen zu lassen. Um die Schulen bei der Vorbereitung und Durchführung der Projektwoche zu unterstützen, erhielten sie von der TK entwickelte "Anti-Mobbing-Koffer", die Unterrichtsmaterialien unter anderem zu Rollenspielen und zum Erarbeiten von Umgangs- und Klassenregeln enthalten. Das Materialangebot des Koffers wurde im Jahr 2013 eigens um den Aspekt Cyber-Mobbing erweitert und an die weiterführenden hessischen Schulen ausgeliefert.

Zusätzlich wurde in 2013 allen hessischen Schulen die Broschüre "Mobbing - Ein Wegweiser zur Mobbingprävention und Mobbingintervention in Hessen" zugesandt. Die Broschüre wurde vom Netzwerk gegen Gewalt (NgG) in Kooperation mit dem HKM-Projekt "Gewaltprävention und Demokratie lernen" (GuD), der Schulmediation Hessen und dem Stadtjugendamt Frankfurt erarbeitet. Sie dient als Wegweiser für Schulleitungen, Lehrkräfte, sozialpädagogische Fachkräfte und Eltern, gibt Orientierung für angemessenes Verhalten bei Mobbingfällen (auch Cyber-Mobbing) und enthält Informationen über Unterstützungs- und Fortbildungsangebote in Hessen.

Im Bereich des Jugendmedienschutzes erhalten Schulleitungen gezielte Informationen zum Umgang mit Cyber-Mobbing und anderen Phänomenen im Zusammenhang mit digitalen Medien (z.B. Sexting). Für Lehrkräfte wie auch Eltern gibt es regionale Informations- und Fortbildungsveranstaltungen. Landesweit werden in mehrtägigen regionalen Fortbildungsreihen derzeit Jugendmedienschutzberaterinnen und -berater für Schulen ausgebildet. Sie sollen an ihren Schulen im Bereich des Jugendmedienschutzes die Schulleitung und das Kollegium beraten, Fortbildungen organisieren und Informationsveranstaltungen für Eltern anbieten sowie gegebenenfalls auch benachbarte Schulen unterstützen. Die Möglichkeit einer kostenlosen Online-Fortbildung zum Jugendmedienschutz besteht für alle hessischen Lehrkräfte bei dem Virtuellen Zentrum für Lehrerbildung (VLZ) der Universität Marburg auf der Grundlage einer Kooperation mit dem Landesschulamt.

Direkt für Schülerinnen und Schüler gibt es außerdem regionale Präventionsangebote wie das Frankfurter Projekt "Digitale Helden" oder die "Medienschouts" im Raum Wiesbaden und Rheingau-Taunus-Kreis, die alle einen sogenannten Peer-to-Peer-Ansatz verfolgen, indem Schülerinnen und Schüler zu Multiplikatoren/-innen ausgebildet werden, um ihre Altersgenossen zum Thema Jugendmedienschutz und in diesem Rahmen besonders auch zum Umgang mit Cyber-Mobbing zu informieren und zu unterstützen. Eine Ausweitung dieser Maßnahmen auf andere Regionen wird ausgehend von noch zu erhebenden Evaluationsergebnissen und zur Verfügung stehenden Ressourcen geprüft.

Schließlich bietet der Webauftritt zum Jugendmedienschutz auf dem Hessischen Bildungsserver aktuelle Informationen, Materialien, Fortbildungsangebote und eine Linksammlung für Lehrkräfte, Eltern sowie Schülerinnen und Schüler an. Der Bereich für Schülerinnen und Schüler sieht u.a. Notfalladressen und Informationsmaterial, das speziell für Kinder und Jugendliche geeignet ist, vor. Für Eltern stehen Informationen, Linktipps und abrufbare Informationsbroschüren, auch in mehreren Sprachen, zur Verfügung. Die Seite für Lehrkräfte stellt neben Unterrichtshilfen auch Meldestellen, kindgerechte Internetseiten, die Rechtslage sowie Schutzmöglichkeiten in der Schule vor.

Als sehr geeignet können zudem die Materialien von "klicksafe" angesehen werden ([www.klicksafe.de/materialien](http://www.klicksafe.de/materialien)), die auch seitens des Kultusministeriums im Rahmen von Fortbildungen genutzt werden.

Die bei den Organisationseinheiten "Prävention" in den Präsidien und dem Hessischen Landeskriminalamt angesiedelten Beraterinnen und Berater "Prävention Cybercrime" sowie die Jugendkoordinatorinnen und -koordinatoren unterstützen in akuten Einzelfällen die Schulen bzw. Schulklassen durch Intervention und Vortragstätigkeit bei Lehrern und Eltern zu diesem Thema. Im Rahmen der Mobbingprävention wurden durch das NgG regionale berufsübergreifende Fachtagungen abgehalten und die Broschüre "Mobbing - Ein Wegweiser zur Mobbingprävention und Mobbingintervention in Hessen" entwickelt. Geplant ist eine intensivere regionale Vernetzung zur Erhöhung der Wirksamkeit der Maßnahmen.

Frage 138. Welche Maßnahmen plant die Landesregierung, um den Jugendlichen internetspezifische Kompetenzen im Bereich der Datensicherheit und Datenschutzkompetenz zu vermitteln?

Unter Federführung des Kultusministeriums werden Lehrkräfte für die Schulen als Jugendmedienschutzberaterinnen und -berater ausgebildet. Das Netzwerk gegen Gewalt ist an einer Arbeitsgruppe beteiligt, die diese Multiplikatoren begleitet.

Auf die Antwort zu Frage 137 wird verwiesen.

Frage 139. Welche Maßnahmen werden in Hessen durchgeführt, um die Schülerinnen und Schüler selbst in die Schulung ihrer "Peer Group" im Bereich der Medienkompetenz einzubinden?

Es gibt verschiedene regionale Peer-to-Peer-Programme und Projekte zu Cybermobbing, Jugendmedienschutz und Medienkompetenz wie z.B. "Medien-Scouts" oder "Digitale Helden". Auf die Antwort zur Frage 48 und 137 wird verwiesen.

Im Übrigen wird für den Justizbereich (Landespräventionsrat) auf die Ausführungen zu Frage 140 Bezug genommen.

Frage 140. Wie werden diese Maßnahmen durch die Landesregierung unterstützt?

Die Landesregierung unterstützt unter anderem mit finanziellen Mitteln Gewaltpräventionsmaßnahmen wie z.B. PiT und buddY, den Jugendmedienschutz oder die Landesanstalt für privaten Rundfunk, die ihrerseits wiederum Maßnahmen zur Förderung der Medienkompetenz in Abstimmung mit dem Kultusministerium anbietet.

Die Vermittlung von Medienkompetenz ist auch Gegenstand der Arbeit kommunaler Präventionsgremien. Die Sachverständigenkommission für Kriminalprävention der Hessischen Landesregierung (Landespräventionsrat) unterstützt die Präventionsarbeit vor Ort durch Anregung und Beratung. Dies erfolgt sowohl über die Arbeitsgruppen des Landespräventionsrates als auch über die seit 1994 und seit 1997 jährlich an unterschiedlichen Orten stattfindenden Treffen mit den kommunalen Gremien, welche dem Informationsaustausch und der Vernetzung dienen. Konkrete kriminalpräventive Projekte, die Vorbildfunktion besitzen und von Präventionsgremien zur Bewältigung bei übereinstimmenden Problemlagen übernommen werden können, werden zudem über den alle zwei Jahre vergebenen Hessischen Präventionspreis auch finanziell unterstützt. Im Rahmen des diesjährigen Wettbewerbs erhielt das Projekt "Rheingau-Medien-Scouts" (Magistrat der Stadt Eltville, Jugendpflege, in Kooperation mit dem Staatlichen Schulamt Wiesbaden/Rheingau-Taunus-Kreis) den 1. Preis in Höhe von 2.000 Euro. Ziel dieses seit August 2011 laufenden kriminalpräventiven Projekts ist es, Defizite im Bereich Medienkompetenz zu beheben und insbesondere Schülerinnen und Schüler für einen sicheren Umgang mit dem Internet zu qualifizieren. Unter Zugrundelegung des Konzepts der peer-to-peer Education werden Jugendliche und Heranwachsende zu Medien-Scouts ausgebildet, um Personen ihrer Altersgruppe für Fragen rund um das Thema Internet mit Rat und Tat zur Seite zu stehen.

Frage 141. Welche Untersuchungen zur Erforschung des konkreten Gefährdungspotenzials für Jugendliche im Internet sind der Landesregierung bekannt und wie unterstützt die Landesregierung die Gewinnung weiterer Erkenntnisse (Forschungsprojekte bitte einzeln mit Art und Umfang der Unterstützung aufführen)?

Von den zahlreichen Untersuchungen, die es gibt und die der Landesregierung bekannt sind, werden nur einige relevante hier aufgeführt.

- JIM-Studie 2013, FIM-Studie 2011, medienpädagogischer Forschungsverbund Südwest
- Soziale Netzwerke 2013 - Dritte, erweiterte Studie, eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet, Bitkom,
- "Kinder und Jugend 3.0" - Alltag mit dem Smartphone: Studie zur Nutzung von Medien im Kinder- und Jugendalter 2014, Bitkom,
- ARD/ZDF-Onlinestudie 2013,
- DIVSI U25-Studie: Kinder, Jugendliche und junge Erwachsene in der digitalen Welt: Deutsches Institut für Vertrauen und Sicherheit im Internet,
- Studie "Jugendliche und Online-Werbung im Social Web" JFF Institut für Medienpädagogik in Forschung und Praxis,

- Cyberlife - Spannungsfeld zwischen Faszination und Gefahr, Cyber-Mobbing bei Schülerinnen und Schülern, eine empirische Bestandsaufnahme bei Eltern, Lehrkräften und Schülern/innen in Deutschland, Bündnis gegen Cyber-Mobbing, 2013,
- EU Kids Online I bis III, Hans-Bredow-Institut für Medienforschung, Koordination für Deutschland.

Bezüglich der Technischen Hochschule Darmstadt wird hier auf die Antwort zu Frage 223. verwiesen.

Hinsichtlich der Fachhochschule Frankfurt am Main wird auf die Antwort zu Frage 127 verwiesen.

Für die o.g. Untersuchungen findet keine Einzelunterstützung statt; die Hochschulen werden seitens der Landesregierung im Rahmen des Globalbudgets finanziert.

Frage 142. In welcher Hinsicht hält die Landesregierung Jugendliche im Netz für besonders schutzbedürftig?

Nach Auffassung der Landesregierung sind nicht alle Jugendlichen in gleichem Ausmaß für Gefährdungen im Internet anfällig. Vielmehr ist der Grad der Gefährdung abhängig von vielen verschiedenen Faktoren, die die Lebenswelt des Einzelnen prägen. Gerade im Umgang mit dem Internet sind soziale Faktoren wie die Anerkennung in der Peer-Group, das Selbstwertgefühl und die Atmosphäre in Familie und Schule von entscheidender Bedeutung. Jugendliche sind neugierig, versuchen sich in der Welt zu orientieren und ihre Rolle in der Gesellschaft zu finden. Dies führt dazu, dass sie auch im Internet risikobereiter sind, Unbekanntes auszuprobieren. Gleichzeitig verfügen sie über weniger Erfahrung als Erwachsene im Umgang mit ihren Daten oder im geschäftlichen Bereich und den dazu gehörigen vertraglichen und rechtlichen Bedingungen (AGB, Lizenz- oder Urheberrecht usw.). Daher sind sie anfälliger für gezielte Werbung und die Herausgabe persönlicher Daten, insbesondere in sozialen Netzwerken und jugendaffinen Foren.

Die Entwicklung von Jugendlichen in der Adoleszenzphase bedingt eine Loslösung von bisherigen sozialen Strukturen und ein Ausprobieren und Einfordern neuer Freiheiten. Gerade weil die älteren Generationen häufig weniger medienaffin sind, sind die digitalen Medien ein geeignetes Medium, um sich abzugrenzen und gewisse Freiräume zu schaffen.

Gemäß der JIM-Studie 2013 nutzen die Jugendlichen vor allem Kommunikationsmedien - hier insbesondere Soziale Netzwerke wie Facebook und Messenger-Dienste wie WhatsApp sowie E-Mail und Chatrooms, aber auch das Hören von Musik, das Schauen von Clips und Filmen, Spiele oder die Informationssuche. Dieses Nutzungsverhalten beinhaltet Gefährdungen bzgl. der Datensicherheit, entwicklungsbeeinträchtigender bzw. -gefährdender Inhalte, des Urheberrechts, Kostenfallen und sexuellen Übergriffen. In allen diesen Fällen sind Jugendliche schutzbedürftig. Dies ist z.B. auch im Jugendmedienschutzstaatsvertrag formuliert. Prävention auch durch staatliche Institutionen ist ein geeignetes Mittel, um der Schutzbedürftigkeit von Jugendlichen zu entsprechen.

Das Alter ist kein Kriterium, das per se zu einer besonderen Schutzbedürftigkeit führt. Es ist zwar einerseits zu berücksichtigen, dass Kinder wegen mangelnder Erfahrung und eingeschränkter Impulssteuerung anfälliger sind, Opfer unseriöser Angebote im Internet und von Straftaten zu werden. Die besondere Schutzbedürftigkeit nimmt mit Annäherung an das Erwachsenenalter und zunehmender Geschäftsfähigkeit grundsätzlich ab. Andererseits kann sie sich mit fortschreitender Alterung wieder verstärken. Der Aspekt der leichtfertigen Freigabe persönlicher Daten und Informationen spielt jeweils eine wesentliche Rolle. Während bei Kindern und Jugendlichen vorwiegend Gefährdungen hinsichtlich der Verletzung der Persönlichkeitsrechte und durch sexuell motivierte Handlungen bestehen, verlagern sich diese altersspezifisch zunehmend in den Bereich des E-Commerce (Internet-Banking, Betrugsofferten etc.). Junge und alte Menschen sind in dem Maße schutzbedürftig, wie sie noch nicht oder nicht mehr die Kenntnisse und Fähigkeiten eines situationsadäquat aufmerksamen, durchschnittlich informierten und verständigen Internetnutzers besitzen. Wesentliche Bedeutung - auch im Kontext der Internetnutzung - kommt dem Stand der jeweiligen Persönlichkeitsentwicklung und dem Grad der individuellen Medienkompetenz zu.

Frage 143. Wie bewertet die Landesregierung vor dem Hintergrund der bekannten Forschungsergebnisse die vorhandenen Schutzmechanismen für Internetnutzerinnen und -nutzer im Jugendalter und welche Weiterentwicklungen plant die Landesregierung?

Medienkompetenz ist eine Schlüsselqualifikation in der heutigen Gesellschaft, die sowohl für beruflichen und schulischen Erfolg als auch für private und persönliche Belange einen hohen Stellenwert hat. Die Landesregierung bemüht sich, ein höchstmögliches Schutzniveau zu erreichen, indem sie Informationen über bestehende Risiken und Aufklärung über mögliche Maßnahmen zum Schutz von Kindern und Jugendlichen einer breiten Öffentlichkeit zugänglich macht. Sie bietet Fortbildungsveranstaltungen vor allem für am Erziehungsprozess beteiligte

Personen mit dem Ziel an, durch umfassende Informationen über bestehende Risiken sowie bestehende Schutzmöglichkeiten das Gefährdungspotential für Kinder und Jugendliche zu minimieren. Dazu zählt vor allem die Information über technische Möglichkeiten der Programmierung von Kinderschutzsoftware und der Einsatz von Schutzfiltern, aber auch das Wissen über die Notwendigkeit, Kindern und Jugendlichen die nötige Medienkompetenz zu vermitteln, damit sie selbst in die Lage versetzt werden, sich zu schützen. Diese können sie aber nur erlangen, wenn Eltern und alle anderen am Erziehungsprozess beteiligten Personen sie dabei aktiv unterstützen.

Die Landesregierung hält darüber hinaus die Einbindung der Wirtschaft durch Selbstverpflichtungen, Voreinstellung von Kinderschutzprogrammen und Bereitstellen von Jugendschutzlösungen für dringend notwendig.

Gerade im Hinblick auf altersgerechte Zugänge und altersspezifisch gekennzeichnete Inhalte im Internet arbeitet die Landesregierung intensiv an allen gesetzlichen Novellierungen im Jugendmedienschutz mit und unterstützt die Arbeit der freiwilligen Selbstkontrollen sowie von jugendschutz.net. Sie steht in engem Kontakt zur Bundesprüfstelle für jugendgefährdende Medien und entsendet Mitarbeiter in deren Prüfgremien.

Der wirksamste Schutz vor Gefahren ist und bleibt die Information der breiten Öffentlichkeit und die Verantwortung aller am Erziehungsprozess beteiligten Personen, Jugendliche beim Umgang mit dem Internet zu unterstützen und vorhandene technische Lösungen, wie Kinder und Jugendschutzfilter, dabei auch einzusetzen.

Präventive Maßnahmen des Jugendmedienschutzes an den Schulen werden systematisch besser aufeinander abgestimmt und z.B. auf Basis von Evaluationsbefunden weiterentwickelt. Die technischen Schutzmaßnahmen sind Teil der IT-Ausstattung an den Schulen, die von den jeweiligen Schulträgern eingerichtet werden und auch nur von diesen eingerichtet werden können. Alle Schulträger haben Filtersoftware installiert, die auf Negativlisten (black lists) basieren.

## Erwachsene

Frage 144. Welche Herausforderungen ergeben sich aus Sicht der Landesregierung, um den Verbraucherschutz im Internet für die Gruppe der Erwachsenen zu verbessern?

Die meisten Erwachsenen nutzen das Internet täglich. Wie eine Studie des Bundesverbandes Digitale Wirtschaft (BVDW) e.V. von Ende 2012 belegt, sind 77 % aller erwachsenen Deutschen und damit insgesamt 54,1 Millionen Bundesbürger täglich online. (<http://www.bvdw.org/medien/bvdw-und-ovk-77-%-der-erwachsenen-deutschen-nutzen-das-internet?media=4178>)

Da die meisten Erwachsene tagtäglich im Berufsleben in Berührung mit dem Internet kommen, sind sie im Umgang geübt. Wie aber auch jüngere und ältere Nutzer, brauchen sie verständliche und kompetente Informationen über Gefährdungen, die vom Internet ausgehen und Chancen, die das Internet bietet.

Frage 145. Mit welchen besonderen Gefährdungslagen sind Erwachsene im Netz aus Sicht der Landesregierung konfrontiert?

Abgesehen von Delikten, deren Opfer zwangsläufig Kinder oder Jugendliche darstellen (z.B. sexueller Missbrauch von Kindern, Verbreiten kinderpornographischer Schriften), stellen Erwachsene erwartungsgemäß die weitaus größte Opfergruppe dar. Im Bereich der Delikte gegen die persönliche Freiheit (Nachstellung, Bedrohung, Nötigung), Beleidigungsdelikte, Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen weist - laut PKS - die Gruppe der Kinder, Jugendlichen und Heranwachsenden zusammen einen Anteil von 14% aus. Auffällig erscheint der verhältnismäßig hohe Anteil älterer Opfer (> 60 Jahre) in den Deliktsfeldern Schadprogramme und Ransomware.

Tabellarische Übersicht: Altersstruktur der Opfer (Jahr 2013) nach PKS.

	Nachstellung, Bedrohung, Nötigung (Tatmittel PC, Internet)	Betrugsdelikte (Tatmittel PC, Internet)	Phishing (Erlangung von Zugangs- und Transaktionsdaten)	Schadprogramme (Viren, Würmer, Trojanische Pferde)	Ransomware (Online-Erpressung Mittels Schadsoftware)
Kinder, Jugendliche, Heranwachsende	14 %	7 %	1 %	4 %	4 %
Erwachsene	86 %	93 %	99 %	96 %	96 %
Davon älter als 60 Jahre	20 %	8 %	19 %	29 %	33 %

Frage 146. In welcher Hinsicht hält die Landesregierung Erwachsene im Netz für besonders schutzbedürftig?

Auf die Antwort zu den Fragen 142 und 145 wird verwiesen.

Frage 147. Welche Maßnahmen werden seitens der Landesregierung ergriffen, um über die Gefahren für Erwachsene (insbesondere Seniorinnen und Senioren) aufzuklären und ihnen zu begegnen?

Das Internet hat sich zu einem Teil des täglichen Lebens entwickelt. Für Menschen im fortgeschrittenen Alter und vor allem in ihrer Bewegung eingeschränkte Seniorinnen und Senioren bietet das Internet Chancen, den Alltag zu erleichtern, Kontakte zu pflegen und sich Informationen zu beschaffen, die auf anderem Weg nicht zu erreichen wären. Die Vermittlung von Medienkompetenz für ältere Menschen ist deshalb der Landesregierung ein großes Anliegen. Die vom Land Hessen geförderte Landesseniorenvertretung zeigt z.B. auf der Internetseite [www.sozialnetz.de](http://www.sozialnetz.de) unter dem Stichwort "Senioren auf Draht" allen Interessierten Möglichkeiten auf, um die Welt des Internets zur eigenen Nutzung zu erschließen.

Angebote zur Förderung der Medienkompetenz sind Teil des vom Land geförderten Pflichtangebots nach § 9 Abs. 2 Hessisches Weiterbildungsgesetz (HWBG).

Auf die Antworten zu den Fragen 28 und 40 wird verwiesen.

Frage 148. Wie unterstützt die Landesregierung Projekte und Organisationen, die gezielt Erwachsene (insbesondere Seniorinnen und Senioren) mit dem Internet oder anderen digitalen Medien vertraut machen (bitte detailliert aufschlüsseln nach Art des Projekts, den unterstützten Maßnahmen, Ort/Region, Träger)?

Neben der Unterstützung der Landesseniorenvertretung (siehe Antwort zu Frage 147) werden von der Landesregierung auch einzelne Projekte unterstützt. Ein viel beachtetes Projekt ist beispielsweise die Kasseler Initiative "Erinnerungen im Netz" ([www.erinnerungen-im-netz.de](http://www.erinnerungen-im-netz.de)), das vom Stadtteilzentrum Agathof getragen und vom Hessischen Ministerium für Soziales und Integration gefördert wurde. Das Portal bietet historische Dokumente, Geschichten und Erlebtes aus und über den Kasseler Osten. Damit wird wertvolles Wissen von Zeitzeugen erhalten und nutzbar gemacht.

Im Rahmen von HESSENCAMPUS (HC) gehört der Umgang mit den sog. Neuen Medien zu den zentralen Handlungsfeldern. Seit 2010 fördert das Land im Rahmen des Aufbaus von HC landesweite Leitprojekte in diesem Handlungsfeld. Eine nach Art des Projekts, unterstützte Maßnahmen, Ort/Region und Träger aufgeschlüsselte Übersicht ist im Anhang beigefügt.

Die mit der Verbraucherzentrale Hessen e.V. abgeschlossene Kooperationsvereinbarung verfolgt u.a. die Intention, der Zielgruppe Senioren typische Tatbegehungsweisen aufzuzeigen und wirksame Schutzmöglichkeiten vorzustellen. Der durch die Kooperation erzielte größere Streuungsgrad durch den Internetauftritt des Verbraucherschutzes ([verbraucherfenster.hessen.de](http://verbraucherfenster.hessen.de)) erweist sich als probates und zielführendes Mittel, welches zukünftig verstärkt für diese Zielgruppe eingesetzt werden soll.

Frage 149. Welche Maßnahmen beabsichtigt die Landesregierung, um die Zahl der Erwachsenen mit Internetzugang zu erhöhen und so dem "Digital Divide" zu begegnen?

Auf die Antworten zu den Fragen 111 und 114 wird verwiesen.

Frage 150. Welche Maßnahmen plant die Landesregierung, um Erwachsenen (insbesondere Seniorinnen und Senioren) internetspezifische Kompetenzen im Bereich der Datensicherheit und Datenschutzkompetenz zu vermitteln?

Ergänzend zur Antwort auf Frage 40 kann bei der Präventionsarbeit auf die vielseitigen Medien des ProPK, einschließlich des Internetauftrittes "[www.polizei-beratung.de](http://www.polizei-beratung.de)" zurückgegriffen werden. Hier informiert die Polizei zielgruppenspezifisch Eltern, Lehrer, Migranten und Senioren ausführlich über die jeweiligen Kriminalitätsphänomene (z.B. Betrug, Enkeltrick, Medienkompetenz) des Internets.

Die Cybercrime-Fachberater der Hessischen Polizei bieten darüber hinaus spezielle Veranstaltungen für Seniorinnen und Senioren an und informieren über potenzielle Gefahren für diese Zielgruppe. Unter anderem wird im Rahmen der Vorträge auf den rechtlichen Aspekt des Datenschutzes bzw. die Bedeutung der Privatsphäreinstellungen in sozialen Netzwerken eingegangen, da auch immer mehr ältere Menschen dieses Medium nutzen.

Die ältere Generation steht ebenfalls im Fokus bei der Kooperation der Polizei mit der Verbraucherzentrale. Die Zielgruppe Senioren bekommt auf der Seite "[www.verbraucherfenster.de](http://www.verbraucherfenster.de)" typische Tatbegehungsweisen aufgezeigt und wirksame Schutzmöglichkeiten erläutert.

Auf die Antwort zu Frage 148 wird insoweit verwiesen.

Frage 151. Verfolgt die Landesregierung geschlechtsspezifische Maßnahmen, um die Zahl der Erwachsenen mit Internetzugang zu erhöhen?

Auf die Antwort zur Frage 150 wird verwiesen.

### **Verbraucherschutz und Datenschutz Soziale Netzwerke**

Frage 152. Welche Einschätzung vertritt die Landesregierung hinsichtlich des Datenschutzes bei der Nutzung Sozialer Netzwerke?

Die Landesregierung ist der Auffassung, dass die Nutzung von Sozialen Netzwerken einige technische und datenschutzrechtliche Fragen aufwirft. Dabei sind die Einzelheiten der Verarbeitung der Daten von Nutzerinnen und Nutzern oft nicht umfassend bekannt, insbesondere bei Anbietern aus Drittstaaten.

Die Notwendigkeit der Prüfung dieser Fragen besteht insbesondere dann, wenn die Landesregierung selbst verantwortlicher Betreiber von Webseiten mit Like-Button oder Betreiber von Fanseiten ist. Sie unterstützt daher Bemühungen, diese Fragen aufzuarbeiten, um zu belastbaren datenschutzrechtlichen Bewertungen zu kommen. Hierbei werden auch die fachlichen Einschätzungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder berücksichtigt.

Soweit Verbraucherinnen und Verbraucher sich bei Sozialen Netzwerken beteiligen wollen, sollten sie sich im Rahmen ihrer Eigenverantwortung kritisch über die datenschutzrechtlichen Risiken im Vorfeld informieren und ansonsten nach dem Grundsatz der Datensparsamkeit konsequent agieren.

Die meisten Sozialen Netzwerke werden den Verbraucherinnen und Verbrauchern kostenfrei zur Verfügung gestellt und finanzieren sich über zielgerichtete Werbung sowie den Verkauf von Benutzerprofilen bzw. von detaillierten Informationen zu seinen Benutzern. Das Geschäftsmodell der Anbieter ist deshalb einerseits auf eine hohe Vernetzung der Benutzer untereinander sowie deren stetige Interaktion und andererseits auf die Möglichkeit einer weitgehenden Auswertung der Nutzerdaten angewiesen. Beide Ziele stehen Datenschutz optimierten Verfahren und Grundeinstellungen entgegen. Der Landesregierung ist zudem bekannt, dass Verbraucherinnen und Verbraucher trotz intensiver medialer Aufklärung zu den Datenschutzproblemen in der Regel kostenfreie Dienste und Dienste mit hohen Nutzerzahlen, datenschutzfreundlichen, aber kostenpflichtigen Diensten vorziehen.

Insbesondere vor diesem Hintergrund unterstützt die Landesregierung deshalb Bemühungen, über den Datenschutz in Sozialen Netzwerken zu informieren. Soweit Bürgerinnen und Bürger die Absicht haben, sich an Sozialen Netzwerken zu beteiligen, sollten sie sich im Rahmen ihrer Eigenverantwortung über die datenschutzrechtlichen Risiken im Vorfeld informieren und konsequent auf jede unnötige Übermittlung ihrer Angaben verzichten.

Neben den Sozialen Netzwerken immanenten Datenschutzproblemen zwischen den Nutzern (beispielsweise zu freizügig gesetzte Zugriffsrechte, üble Nachrede, u.Ä.) ergeben sich laut dem Hessischen Datenschutzbeauftragten weitere Datenschutzprobleme aus diesen Geschäftsmodellen. Es ist das Ziel der Anbieter Sozialer Netzwerke, möglichst viele Daten zu den Nutzenden zu sammeln, um diese Daten beispielsweise für gezielte Werbung zu vermarkten. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder führte am 14. März 2013 im Rahmen der Ausarbeitung "Orientierungshilfe Soziale Netzwerke" dazu aus, dass Anbieter Sozialer Netzwerke sicherstellen müssen, dass die Nutzer ihrer Angebote die Profildaten und Kommunikationsinhalte anderer Nutzer nicht ohne ausdrückliche Einwilligung der Betroffenen automatisiert auslesen können.

Folgende Maßnahmen gegen den automatisierten und systematischen Abruf (z.B. durch crawler) von Profildaten und Kommunikationsinhalten sollten getroffen werden:

- Der Zugriff von Suchmaschinen oder anderen Indexierern auf die Profile der Nutzer sollten von diesen im Rahmen der Datenschutzeinstellungen festgelegt werden können und in den Standardeinstellungen deaktiviert sein.
- Betreiber von Sozialen Netzwerken sollten Maßnahmen ergreifen, die eine Massenkopie von Daten aus dem Netzwerk verhindern. Zu solchen Maßnahmen zählen z.B. die Beobachtung von auffälligen Aktivitäten im Netzwerk (Unterscheidung zwischen manuellen und maschinellen Zugriffen) oder die externe Auditierung der eigenen Infrastruktur.

Frage 153. Wie bewertet die Landesregierung die Übersichtlichkeit der Nutzungs- und Datenschutzbestimmungen von Sozialen Netzwerken mit Blick auf den Verbraucherschutz?

Kein Dienst im Netz umfasst so viele persönliche Daten wie Soziale Netzwerke. Das eigene Profil bei Facebook, Google+ und anderen ist für Millionen Nutzer inzwischen Ausweis einer neuen digitalen Identität.

Der Datenschutz in sozialen Netzwerken stellt dabei eine besondere Herausforderung dar,

- weil weltweit immer mehr Menschen diese Netzwerke nutzen,
- weil interessante und innovative Anwendungen unter Nutzung der personenbezogenen Daten denkbar sind,
- weil die Netzwerke global tätig sind, aber möglichst einheitlich betrieben werden sollten, weil auch Nichtnutzer - z.B. durch so genannte "Social-Plug-Ins" - von der großen Reichweite der Netzwerke betroffen sind,
- weil eine Erstellung von Nutzerprofilen möglich ist, in denen unterschiedliche Daten über den Nutzer zusammengefügt werden
- und weil die Netzwerke meist kostenlos zugänglich sind und sich durch (meist benutzerdefinierte) Werbung finanzieren. Durch die Vielzahl von Informationen in Sozialen Netzwerken lässt sich hier (meist benutzerdefinierte) Werbung zielgerichteter schalten.

Die Voreinstellungen in Sozialen Netzwerken werden oft sehr großzügig gehandhabt. Viele Soziale Netzwerke zwingen ihre Nutzer durch die installierten Standardeinstellungen, möglichst viele Daten öffentlich zugänglich zu machen, um so viel Persönliches preiszugeben. Sicherheitseinstellungen zum Schutz der Privatsphäre müssen oftmals nach der Anmeldung im Sozialen Netzwerk aktiv vorgenommen werden. Was also an- oder ausgeklickt werden muss, um dies oder jenes zu schützen oder abzulehnen, erfordert eine zeitintensive Auseinandersetzung und ist leider nicht immer nutzerfreundlich. Problematisch ist häufig auch, dass die Betreiber Sozialer Netzwerke die persönlichen Daten trotz Löschsens des Kontos durch den Nutzer weiter speichern und nicht vollständig entfernen. Insbesondere eine verpflichtende Löschfunktion für Diensteanbieter und verbraucherfreundliche Voreinstellungen in Sozialen Netzwerken erscheinen zwingend notwendig.

Laut dem Hessischen Datenschutzbeauftragten sind die Nutzungsbedingungen gerade von Facebook unzweifelhaft schwer verständlich und für den Nutzer kaum transparent.

Auf die Antwort auf die Frage 157 wird verwiesen.

Frage 154. Welche Maßnahmen ergreift die Landesregierung, um die Nutzerinnen und Nutzer über mögliche unklare Klauseln in den Nutzungsbestimmungen von Sozialen Netzwerken aufzuklären?

Das Engagement zur Stärkung des Datenschutzes bei der Nutzung von Sozialen Netzwerken und anderen Anwendungsprogrammen - wie bereits durch die hessische Bundesratsinitiative zur Änderung des Telemediengesetzes mit dem Ziel der Verbesserung des Datenschutzes in Sozialen Netzwerken im Internet 2011 initiiert - wird durch die Landesregierung fortgeführt.

Das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz hat im Rahmen der im vergangenen Jahr stattgefundenen VSMK einen Antrag eingebracht, in dem die Bundesregierung aufgefordert wird, sich auf europäischer Ebene für weitere Nachbesserungen der EU-Datenschutz-Grundverordnung einzusetzen, auf internationaler und europäischer Ebene die Kooperation der Regulierungsbehörden weiter zu verbessern und auf nationaler Ebene gegebenenfalls konkrete gesetzliche Änderungen im Telemediengesetz u.a. eine verpflichtende Voreinstellung auf der höchsten Sicherheitsstufe und Löschfunktionen bei Sozialen Netzwerken vorzunehmen.

Die mit Mitteln des Landes Hessen geförderte Aufklärungsarbeit durch die VZ Hessen und den DHB-Netzwerk Haushalt Hessen (auch im Hinblick auf Fragen von Verbraucherinnen und Verbrauchern zur Nutzung digitaler Medien) wird weiter fortgeführt und gestärkt.

Auf der Internetseite [www.verbraucherfenster.de](http://www.verbraucherfenster.de) wird es in den kommenden Monaten zu diesem Themenbereich verschiedene Beiträge sowie Experten-Interviews mit dem Landeskriminalamt über Gefahren und Risiken im Umgang mit Sozialen Netzwerken als Informationsangebot geben.

Frage 155. Welche Risikoeinschätzung vertritt die Landesregierung hinsichtlich der vereinfachten Verbreitung von Schadsoftware innerhalb Sozialer Netzwerke?

Die Landesregierung sieht das Risiko der Schadsoftwareverbreitung über bzw. in Sozialen Netzwerken. Die Sozialen Netzwerke sind jedoch nur ein Verbreitungskanal neben E-Mail (SPAM/Phishing, s.o.) und sogenannten "drive-by-downloads" über manipulierte Webseiten. Technische Schutzmaßnahmen gegen Schadsoftware sind dagegen weitgehend unabhängig vom

Verbreitungskanal. Tagesaktuelle Virencanaler, eine aktivierte Firewall und Softwarestände, die auch die aktuellen Sicherheitsupdates beinhalten, sind bei jeder Art der Internetnutzung dringend zu empfehlen und wirken dann auch gegen Schadsoftware, die über bzw. in Sozialen Netzwerken verteilt wird.

Frage 156. Wie beurteilt die Landesregierung die Risiken, die für Nutzerinnen und Nutzer durch interne Zusatzanwendungen von Drittanbietern innerhalb der Sozialen Netzwerke entstehen?

Zusatzanwendungen Dritter innerhalb Sozialer Netzwerke bergen grundsätzlich die gleichen Risiken wie jede andere Software. Sie können grobe Fehler in der Programmierung enthalten, die dazu führen, dass die Anwendungen angreifbar sind und sie können versteckte Funktionen enthalten. Für Nutzerinnen und Nutzer ist es praktisch unmöglich selbst feststellen, ob die Zusatzanwendungen ausschließlich die beschriebenen Funktionen beinhalten, über die sie aufgeklärt wurden und in die sie eingewilligt haben. Hinzu kommt auch, dass diese Drittanwendungen i.d.R. mit der "Einladung" oder "Empfehlung" von Freunden arbeiten und Nutzerinnen und Nutzer deshalb weniger kritisch prüfen, ob sie diese Drittanwendungen tatsächlich benötigen. In Einzelfällen sprechen diese Zusatzanwendungen die Empfehlungen bzw. Einladungen ohne Kenntnis des vermeintlichen Absenders aus.

Frage 157. Welcher Handlungsbedarf besteht aus Sicht der Landesregierung hinsichtlich der Drittanbieter in Sozialen Netzwerken mit Blick auf den Datenschutz und die Verbrauchersicherheit?

Der Landesregierung ist bekannt, dass die Nutzungs- und Datenschutzbestimmungen von Sozialen Netzwerken von den Nutzerinnen und Nutzern weitestgehend als unklar und verbraucherunfreundlich aufgefasst werden. Die Nutzungsbestimmungen von Sozialen Netzwerken enthalten datenschutzrelevante Klauseln - beispielsweise im Hinblick auf die Preisgabe personenbezogener Daten an Dritte oder die Speicherung von besuchten Seiten. Bei den Nutzungsbestimmungen handelt es sich rechtlich um Allgemeine Geschäftsbedingungen (AGB) im Sinne von § 305 BGB. Die Nutzungsbestimmungen werden dabei nur dann in den der Nutzung des Sozialen Netzwerks zugrunde liegenden Vertrag mit einbezogen, wenn der Betreiber des Sozialen Netzwerks die andere Vertragspartei - hier die Nutzerinnen und Nutzer - ausdrücklich auf die Einbeziehung der AGB hinweist und der Vertragspartei die Möglichkeit verschafft, vom Inhalt der AGB Kenntnis zu nehmen, und die andere Vertragspartei mit ihrer Geltung einverstanden ist. Zwar ist in rechtlicher Hinsicht klar geregelt, dass Zweifel bei der Auslegung von AGB zu Lasten des Verwenders gehen und der Inhalt des Vertrages sich im Falle der Unwirksamkeit - etwa bei Intransparenz - nach den gesetzlichen Vorschriften richtet, nach denen regelmäßig eine Datenverarbeitung ohne Einverständnis ausgeschlossen ist. Datenschutzrechtliche Probleme ergeben sich jedoch aus den tatsächlichen Umständen - etwa dann, wenn die Nutzungsbestimmungen unklar formuliert, unübersichtlich gestaltet, schlichtweg zu lang sind oder auf einem mobilen Endgerät nicht praktikabel dargestellt werden können. Über die AGB stimmen in diesen Fällen oftmals Nutzerinnen und Nutzer einer Verarbeitung ihrer personenbezogenen Daten zu, ohne sich der Bedeutung ihrer Erklärung und ihrer Auswirkungen bewusst zu sein. Ein typisches Beispiel hierfür sind die Fälle, in denen sich die Diensteanbieter von Sozialen Netzwerken die Nutzungsrechte an den bei ihm veröffentlichten Inhalten wie Bildern oder Videos einräumen lassen und die Nutzerinnen und Nutzer insoweit ihre alleinige Verfügungsgewalt hierüber verlieren. Derart zustande gekommene Einverständnisse widersprechen jedoch den Zielvorstellungen der Datenschutzgesetze des Landes und des Bundes. Auch nach dem europarechtlichen Verständnis sind diese Einverständnisse oftmals unwirksam. So sieht die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31 - 50; im Folgenden: Datenschutzrichtlinie) ausdrücklich vor, dass ein Einverständnis nur eine Willensbekundung des Betroffenen sein kann, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt. Außerdem muss der Betroffene über die Zweckbestimmungen der Datenverarbeitung informiert werden, woran es in einer Vielzahl von Fällen fehlt - etwa bei den Nutzungs- und Datenschutzbestimmungen des sozialen Internet-Netzwerkes "Facebook" (vgl. KG Berlin, Urteil vom 24.01.2014, Az.: 5 U 42/12 - juris).

Die Landesregierung hat den hohen Stellenwert von Sozialen Netzwerken insbesondere für die junge Bevölkerung des Landes erkannt. Sie setzt sich einerseits für eine Aufklärung der Nutzerinnen und Nutzer ein. Hierzu hat sie u.a. in Kooperation mit dem Fraunhofer-Institut für Sichere Informationstechnologie SIT eine Studie zum Daten-, Privatsphären und zur Unternehmenssicherheit in Sozialen Netzwerken herausgegeben (Poller, Andreas/Waldmann, Ulrich, SIT Technical Reports SIT-TR-2013-02 - Soziale Netzwerke bewusst nutzen, Ein Dossier zu Datenschutz, Privatsphärenschutz und Unternehmenssicherheit, Herausgeber Waidner, Michael, August 2013, im Folgenden: SIT Technical Reports SIT-TR-2013-02). Andererseits plant die Landesregierung, eine Bundesratsinitiative einzubringen, um bei Sozialen Netzwerken die höchste Sicherheitseinstellung voreinzustellen, die nur vom Nutzer individuell gelockert werden kann. Darüber hinaus begleitet und unterstützt sie das Vorhaben der europäischen Datenschutzgrundverordnung, mit der Drittanbieter auch zu einem Schutz der Verbraucherdaten durch eine entsprechende Technik ("privacy by design") bzw. zu datenschutzfreundlichen Grundeinstellungen ("privacy by default") verpflichtet werden können. Schließlich fordert die Landesregierung die

Betreiber von Sozialen Netzwerken auf, ihre AGB barrierefrei zugänglich, übersichtlich und leicht verständlich formuliert zu gestalten und so dem Transparenzgebot nachzukommen. Im Übrigen wird in diesem Zusammenhang auf die Ausführungen zum Themenblock "Weitergabe persönlicher Daten" bei den Fragen 176 bis 179 verwiesen.

Frage 158. Wie viele Fälle von Identitätsdiebstahl in Sozialen Netzwerken hat es in den letzten fünf Jahren nach Schätzungen der Landesregierung gegeben?

Auf die Antwort zur Frage 60 wird verwiesen.

Frage 159. Wie viele sind davon zur Anzeige gebracht und wie viele konnten aufgeklärt werden (bitte Opfer und Täterinnen bzw. Täter geschlechtsspezifisch aufschlüsseln)?

Auf die Antwort zur Frage 60 wird verwiesen.

Frage 160. Beurteilt die Landesregierung die Gefahr, Opfer von Belästigung, Stalking und Mobbing zu werden, in Sozialen Netzwerken anders als bei anderen Angeboten im Internet? Mit welcher Begründung?

Der Landesregierung liegen zur Fragestellung keine belastbaren Erkenntnisse vor.

Frage 161. Wie viele Fälle von Belästigung in Sozialen Netzwerken sind in den letzten fünf Jahren zur Anzeige gebracht und erfolgreich aufgeklärt worden (bitte Opfer und Täterinnen bzw. Täter geschlechtsspezifisch aufschlüsseln)?

In der Polizeilichen Kriminalstatistik (PKS) werden im Straftatenkatalog aufgeführte rechtswidrige Taten nach bundeseinheitlichen Richtlinien erfasst. Eine "Belästigung" erfüllt in der Regel keinen Straftatbestand, somit erfolgt bei diesen Fällen keine Erfassung und es kann mangels Datenbasis keine Aussage getroffen werden.

Frage 162. Wie viele Fälle von Stalking in Sozialen Netzwerken sind in den letzten fünf Jahren zur Anzeige gebracht und erfolgreich aufgeklärt worden (bitte Opfer und Täterinnen bzw. Täter geschlechtsspezifisch aufschlüsseln)?

Der Tatbestand "Stalking" wird als Fall der Nachstellung in der PKS erfasst. Eine Ausweisung von Fällen, Tatverdächtigen oder Opfern im Zusammenhang mit "Sozialen Netzwerken" ist in der Polizeilichen Kriminalstatistik (PKS) nicht möglich, da das Merkmal "Soziales Netzwerk" nicht gesondert erfasst wird.

Frage 163. Wie viele Fälle von Mobbing in Sozialen Netzwerken sind in den letzten fünf Jahren zur Anzeige gebracht und erfolgreich aufgeklärt worden (bitte Opfer und Täterinnen bzw. Täter geschlechtsspezifisch aufschlüsseln)?

In der Polizeilichen Kriminalstatistik (PKS) ist der Begriff "Mobbing" nicht definiert. Fälle des Mobbings können unter verschiedenen Straftatbeständen wie Beleidigung, Nötigung, Bedrohung oder Stalking in der PKS erfasst worden sein. Eine Auswertung dieser Fälle im Zusammenhang mit "Sozialen Netzwerken" ist in der PKS nicht möglich, da das Merkmal "Soziales Netzwerk" nicht gesondert erfasst wird.

Frage 164. Welche Maßnahmen plant oder vollzieht die Landesregierung, um die Verbraucherinnen und Verbraucher über Mobbing, Belästigung und Stalking in Sozialen Netzwerken aufzuklären?

Auf die Antworten zu den Fragen 150 und 40 wird verwiesen.

Die Landesregierung bietet hessischen Verbraucherinnen und Verbrauchern zusätzlich seit 2003 mit dem Verbraucherportal [www.verbraucherfenster.de](http://www.verbraucherfenster.de) aktuell und praxisnah umfassende Informationen rund um den Verbraucherschutz, auch im Bereich Cyber-Mobbing und Soziale Netzwerke, u.a. in den Beiträgen "Cyber-Mobbing ist kein Kinderspiel - Wie können sich Betroffene wehren?", "Modelmasche" im Internet - Hessisches Landeskriminalamt warnt Mädchen und junge Frauen vor unseriösen Angeboten", "Soziale Netzwerke - Reize und Risiken der schönen neuen virtuellen Internetwelt".

Frage 165. Berücksichtigt die Landesregierung bei Maßnahmen gegen Mobbing, Belästigung und Stalking in Sozialen Netzwerken geschlechts- und altersspezifische Herausforderungen?

Auf die Antworten zu den Fragen 28, 40 und 123 wird verwiesen.

Frage 166. Welche Maßnahmen zur besseren Information insbesondere junger Nutzerinnen und Nutzer über mögliche Risiken in Sozialen Netzwerken werden durch die Landesregierung durchgeführt oder sind angedacht?

Um für mögliche Gefahren in Sozialen Netzwerken zu sensibilisieren, stellt die Hessische Polizei verschiedene Informationsmaterialien zur Verfügung, unter anderem die Broschüre "Soziale Netzwerke". Mit dem Informationsportal VerbraucherFenster der Landesregierung steht ein weiteres Portal zur Verfügung, dass zu diesem Themenbereich Informationen bietet, u.a. in den

Beiträgen "Cyber-Mobbing ist kein Kinderspiel - Wie können sich Betroffene wehren?", "Modelmasche im Internet - Hessisches Landeskriminalamt warnt Mädchen und junge Frauen vor unseriösen Angeboten", "Soziale Netzwerke - Reize und Risiken der schönen neuen virtuellen Internetwelt", "Serie "Datenklau" (Teil V): Soziale Netzwerke, Email und Co - Wie kommuniziere ich sicher?".

Via Twitter wird zusätzlich über die wichtigsten Aspekte hinsichtlich Verbraucherschutzinformationen berichtet. Die Angebote des VerbraucherFensters [www.verbraucherfenster.de](http://www.verbraucherfenster.de) werden auf diesem Wege zusätzlich beworben.

Das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz hat in der Vergangenheit in verschiedenen Pressemitteilungen die Verbraucherinnen und Verbraucher dazu aufgerufen, in Sozialen Netzwerken datensparsam umzugehen und die eigenen Einstellungen in Sozialen Netzwerken zu prüfen. Auch wurde darauf hingewiesen, dass nicht alle persönlichen Daten der Öffentlichkeit preisgegeben werden sollten.

Weitere wichtige Aufklärung in Form von Information und Beratung in diesem Bereich führen die Verbraucherzentrale Hessen und der DHB-Netzwerk Haushalt Hessen durch.

Auf die Antworten zu den Fragen 28, 36, 40, 123 und 150 wird verwiesen.

Frage 167. Wie beurteilt die Landesregierung die Vorteile einer gesetzlichen Verpflichtung der Betreiber Sozialer Netzwerke auf den Grundsatz "Privacy by Design" bzw. "Privacy by Default"?

Angesichts des rapiden technologischen Wandels sollten die besonderen Erfordernisse des Datenschutzes bereits zu einem frühen Zeitpunkt berücksichtigt werden, da neue technologische Systeme oftmals versteckte Gefahren bergen, die sich nur schwer beseitigen lassen, wenn die Grundkonzeption erst einmal feststeht. Daher ist es umso sinnvoller, mögliche Datenschutzprobleme schon bei der Entwicklung neuer Technologien festzustellen und zu prüfen und den Datenschutz von vorneherein in die Gesamtkonzeption einzubeziehen anstatt Datenschutzprobleme im Nachhinein mühsam und mit viel Zeitaufwand durch Korrekturprogramme zu beheben.

Die Landesregierung begrüßt deshalb die Vorteile dieser Techniken und spricht sich dafür aus, dass bei der Entwicklung neuer Geräte, Programme und Anwendungen künftig noch stärker geprüft werden sollte, inwieweit Datenschutz ausreichend praktiziert und Auswirkungen auf den Schutz der Privatsphäre gegeben sind. Eine transparente, datensparsame, kontrollierbare und den Missbrauch vermeidende Technikgestaltung - Privacy by Design und Privacy by Default - gilt es in Zukunft weiter voranzutreiben und flächendeckend einzusetzen.

Die Landesregierung hat bereits im Jahr 2011 eine Initiative in den Bundesrat eingebracht (BR-Drs. 156/11), die eine Änderung des Telemediengesetzes vorsieht, durch die Anbieter von Telemediendiensten mit nutzergenerierten Inhalten, zu denen regelmäßig die Sozialen Netzwerke gehören, verpflichtet werden, die höchste Sicherheitsstufe gemäß dem Stand der Technik zum Schutz der Privatsphäre voreinzustellen.

Frage 168. Welche Sicherheitseinstellungen in Sozialen Netzwerken sind der Landesregierung bekannt?

Die Fragen 168 und 170 werden zusammen beantwortet.

Frage 169. Bewertet die Landesregierung die höchsten aktuell verfügbaren Sicherheitseinstellungen, die den Verbraucherinnen und Verbrauchern von Sozialen Netzwerken angeboten werden, in ihrer Wirksamkeit als datenschutzpolitisch ausreichend?

Die Landesregierung fördert seit 2008 im Rahmen der hessischen Landes-Offensive zur Entwicklung Wissenschaftlich-ökonomischer Exzellenz (LOEWE) das Center for Advanced Security Research Darmstadt (CASED). Wissenschaftler aus der Informatik und verwandten Fachgebieten erforschen und entwickeln am CASED Grundlagen und Anwendungen der IT-Sicherheit. Die jeweils verfügbaren Sicherheitseinstellungen sind Gegenstand dieser Forschung und werden laufend überprüft. Darüber hinaus kann die Frage nicht pauschal beantwortet werden, da der Begriff "Soziale Netzwerke" sehr viele, sehr unterschiedliche Dienste umfasst (z.B. WhatsApp, Facebook, SnapChat, Instagram, Flickr, Twitter, Xing, aber auch Foren unterschiedlichster Art).

Frage 170. Falls Frage 169 verneint wird: Welche Änderungen sollten aus Sicht der Landesregierung an den Sicherheitseinstellungen vorgenommen werden?

Die verschiedenen Netzwerke bieten dem Nutzer mehr oder weniger detaillierte Auswahlmöglichkeiten, welche der eigenen Informationen für andere zu sehen sind. Dabei sollte man sich bei keinem Anbieter auf die Voreinstellungen verlassen, sondern gezielt nachschauen, wer was sehen kann und welche Möglichkeiten man hat, Einfluss zu nehmen.

Die Voreinstellungen zum Schutz der Privatsphäre sind bei Eröffnung eines Accounts oft nicht ausreichend vorgenommen und Sicherheitseinstellungen zum Schutz der Privatsphäre müssen oftmals nach der Anmeldung im Sozialen Netzwerk aktiv durch den Nutzer vorgenommen werden. Verbindungen werden nicht immer verschlüsselt, so dass theoretisch jeder, der sich im gleichen Netzwerk befindet, diese Daten mitlesen kann. Auszüge der Profile können teilweise sogar über Suchmaschinen gefunden werden und sind dadurch allen Internetnutzern weltweit zugänglich. Daten werden häufig ohne aktive Einwilligung der Nutzer an Dritte weitergegeben. Viele Soziale Netzwerke zwingen so ihre Nutzer durch die installierten Standardeinstellungen, möglichst viele Daten öffentlich zugänglich zu machen, um so viel Persönliches preiszugeben. Um alle Funktionen, die ein Telemediendienst mit nutzergenerierten Inhalten bietet, auch nutzen zu können, geben die Nutzer so viel über sich und ihr Umfeld preis.

Die Landesregierung begrüßt grundsätzlich Regelungen zu datenschutzfreundlichen Voreinstellungen. Sie unterstützt die Zielsetzung, verstärkt technische Schutzkonzepte als Beitrag zur Gewährleistung der informationellen Selbstbestimmung in das bestehende System formaler sowie materieller Anforderungen an die Zulässigkeit der Datenverarbeitung aufzunehmen. Grundsätzlich ist mehr Transparenz für den Nutzer eines Internetangebots zu schaffen, indem der Anbieter verpflichtet wird, klarer als bisher über die beabsichtigte Verarbeitung und Nutzung der erhobenen Daten zu informieren.

Frage 171. Welchen Handlungsbedarf sieht die Landesregierung, dass erhöhte Sicherheitseinstellungen von Betreibern Sozialer Netzwerke umgesetzt werden?

Auf die Antworten zu den Fragen 167 bis 169 wird verwiesen.

Frage 172. Welche Position vertritt die Landesregierung zur Möglichkeit der anonymen oder pseudonymen Nutzung Sozialer Netzwerke?

Nach § 13 Abs. 6 Telemediengesetz haben Diensteanbieter grundsätzlich im Geltungsbereich des Gesetzes die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

Die Landesregierung hat die Entscheidungen des Oberverwaltungsgerichts Schleswig-Holstein zur Kenntnis genommen, nach der der Betreiber des Sozialen Netzwerkes "Facebook" Konten von Nutzerinnen und Nutzern sperren darf, wenn diese nicht ihre Echtdateien ("Klarnamen") angeben (OVG Schleswig-Holstein, Beschlüsse vom 22. April 2013, Az.: 4 MB 10/13 und 4 MB 11/13 - juris). Das Gericht führte als wesentliche Begründung an, hinsichtlich der Verarbeitung von Nutzerdaten sei von einer Tätigkeit der irischen Niederlassung von "Facebook" auszugehen. Nach der Datenschutzrichtlinie sowie dem Bundesdatenschutzgesetz sei ausschließlich irisches Datenschutzrecht anwendbar; der Antragsteller habe nicht dargelegt, dass die Möglichkeit pseudonymer Nutzung - wie sie § 3a des Bundesdatenschutzgesetzes vorsehe - auch nach irischem Datenschutzrecht gewährleistet sein müsse.

Die Landesregierung sieht in der Pseudonymisierung und Anonymisierung Methoden, mit denen gerade auch in Sozialen Netzwerken ein effektiver Schutz des informationellen Selbstbestimmungsrechts erreicht werden kann. Für sie erleichtert die Anonymität im Internet die Ausübung der Meinungsfreiheit. Diese Sichtweise wurde bisher auch von anderen Gerichten im Ergebnis geteilt, die darauf abstellten, dass die anonyme Kommunikation ebenso schutzwürdig wie die Kommunikation unter "Klarnamen" sei (vgl. OLG Frankfurt, Urteil vom 8. März 2012, Az.: 16 U 125/11 - juris). Daher will sich die Landesregierung in Vorhaben wie dem einer Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (im Folgenden: Datenschutz-Grundverordnung) dafür engagieren, die Betreiber von Sozialen Netzwerken zu verpflichten, dass ihre Nutzerinnen und Nutzer in den Sozialen Netzwerken auch unter einem Pseudonym agieren können. Darüber hinaus sollen Aufklärungsmaßnahmen der Landesregierung bei den Nutzerinnen und Nutzern Sozialer Netzwerke zu einer Sensibilisierung im Hinblick auf die Preisgabe von personenbezogenen Daten sowohl an die Betreiber als auch ggf. an Dritte beitragen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder führt in ihrer im März 2013 erschienen Orientierungshilfe "Soziale Netzwerke" hierzu Folgendes aus:

"Das TMG fordert in §13 Abs. 6 von Betreibern Sozialer Netzwerke, die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzende ist über diese Möglichkeit zu informieren. Den Nutzenden muss jedenfalls ermöglicht werden, in dem Sozialen Netzwerk unter Pseudonym zu agieren. Eine Offenlegung der tatsächlichen Identität des Nutzers gegenüber dem Betreiber des Sozialen Netzwerkes kann dagegen zur Erschwerung von Missbrauch insbesondere dann hingegenommen werden, wenn die Nutzer das Netzwerk nicht nur passiv (Herunterladen von Informationen), sondern auch aktiv (Einstellen von Informationen) nutzen können. Betreiber Sozialer Netzwerke für Privatnutzung sollten die Nutzung von Pseudonymen aktiv fördern.

Bei Netzwerken, die im beruflichen Kontext genutzt werden, ist es in der dortigen Zielgruppe zwar eher unüblich, anonym bzw. unter Pseudonym aufzutreten. Trotzdem gilt die Verpflichtung aus §13 Abs. 6 TMG zur Eröffnung einer optionalen Möglichkeit, in dem Netzwerke unter Pseudonym zu handeln, auch für solche Netzwerke. Bei entsprechenden Vorgaben zur Gestaltung der Pseudonyme muss die Qualität des Netzwerks nicht leiden, so dass eine Unzumutbarkeit für den Anbieter nicht anzunehmen ist."

In dem Urteil des VI. Zivilsenats vom 1. Juli 2014 hat der BGH (AZ.VI ZR 345/13) noch einmal ausdrücklich die Möglichkeit der anonymen der pseudonymen Nutzung bei Internetdiensten bestätigt, wie sie im Telemediengesetz verankert ist.

Frage 173. Welche Ansätze gibt es, um die langfristige Speicherung von Profildaten durch den Anbieter, auch nach dem vermeintlichen Löschen, zu unterbinden, und wie werden diese durch die Landesregierung bewertet und ggf. verfolgt?

Im Rahmen der aktuellen Verhandlungen zur Europäischen Datenschutz-Grundverordnung ist das "Recht auf Löschung" vorgesehen. Die Verbraucherin oder der Verbraucher soll damit in Zukunft die Löschung der Daten von den Unternehmen und auch unmittelbar von Dritten verlangen, solange nicht festgelegte Gründe dagegen sprechen. Die Unternehmen müssen nun nicht mehr bei Dritten für die Löschung der Daten sorgen, wenn diese von ihnen rechtmäßig veröffentlicht wurden (wogegen auch das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz sich ausgesprochen hatte), sondern nur noch wenn die Daten unrechtmäßig veröffentlicht wurden. Die Landesregierung begrüßt diesen Ansatz. Wichtig scheint auch, durch die Aufklärung über die Risiken der Veröffentlichung persönlicher Daten, sowohl der eigenen als auch dritter Personen, die Nutzer in Bezug auf mögliche Gefahren zu sensibilisieren.

Auf die Antwort auf Frage 175 wird verwiesen.

Frage 174. Welchen Handlungsbedarf sieht die Landesregierung hinsichtlich der Anwendbarkeit des deutschen Datenschutzrechts insbesondere gegenüber den Anbietern Sozialer Netzwerke?

Die vorrangigen Probleme, die Gefahren für das Persönlichkeitsrecht der Internetnutzer bereiten, sind mangelnde Transparenz bei der Erhebung, Verarbeitung oder Nutzung persönlicher Daten durch die Internet-Anbieter, nicht ausreichende Aufklärung über die Risiken für das Persönlichkeitsrecht, wenn persönliche Daten im Internet preisgegeben werden und schließlich der Verbleib der persönlichen Daten, die einmal ins Internet gestellt wurden.

Die Reform des Europäischen Datenschutzrechts und die parallel dazu in den Vereinigten Staaten von Amerika angelaufene Debatte über einen neuen Rechtsrahmen für den Datenschutz in der Informationsgesellschaft eröffnen die Chance, diese Forderungen in umfassend verbindlicher und zeitgemäßer Gewährleistung der informationellen Selbstbestimmung umzusetzen. Diese gilt es zu nutzen, um sich auf europäischer und internationaler Ebene für eine proaktive Kooperation zwischen den entsprechenden EU- und US-Behörden auszusprechen, um eine bessere Durchsetzung der bestehenden rechtlichen nationalen und europäischen Regelungen und des Schutzes personenbezogener Daten zu erreichen.

Frage 175. Welche Vollzugsdefizite sieht die Landesregierung bei der Durchsetzung des deutschen Datenschutzrechts gegenüber den Anbietern Sozialer Netzwerke?

Das nationale Datenschutzrecht sieht vor, dass personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, grundsätzlich zu löschen sind, wenn ihre Speicherung unzulässig ist oder ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Das allgemeine Datenschutzrecht definiert "löschen" als das "Unkenntlich machen gespeicherter personenbezogener Daten". Die Betreiber von Sozialen Netzwerken sind demnach verpflichtet, Profildaten umgehend und vollständig zu löschen, wenn Nutzerinnen und Nutzer ihre Mitgliedschaft in dem Sozialen Netzwerk beenden. Trotzdem kommt es vor, dass Betreiber von Sozialen Netzwerken die Profildaten ihrer ehemaligen Mitglieder vorhalten - beispielsweise werden bei "Facebook" von den Nutzerinnen und Nutzern gelöschte Postings und Nachrichten auch nach dem "Entfernen" weiter gespeichert (vgl. SIT Technical Reports SIT-TR-2013-02, S. 14 f.). Dieser datenschutzrechtliche Missstand lässt sich u.a. damit erklären, dass einerseits die Datenschutzrichtlinie europaweit nicht zu einer vollständigen Harmonisierung des Datenschutzniveaus geführt hat und am Maßstab des in Deutschland erreichten Datenschutzniveaus Defizite in anderen Mitgliedstaaten bestehen. So findet das Bundesdatenschutzgesetz grundsätzlich keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegende verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dies hat u.a. zur Folge, dass beispielsweise der Betreiber des Sozialen Netzwerks "Facebook" dem irischen Datenschutzrecht sowie der Aufsicht der staatlichen Stellen in Irland unterliegt. Andererseits haben oftmals die Betreiber von Sozialen Netzwerken ihren Sitz nicht im Geltungsbereich der europäischen oder nationalen

Datenschutzvorschriften, weswegen europäisches oder deutsches Datenschutzrecht nach geltender Rechtslage nicht zur Anwendung kommt.

Die Landesregierung unterstützt deshalb auf europäischer Ebene das Vorhaben der Datenschutz-Grundverordnung. Der Verordnungsvorschlag sieht in Artikel 3 vor, dass auch Unternehmen mit Sitz außerhalb der EU dann das europäische Datenschutzrecht zu beachten haben, wenn sich ihre Dienstleistungsangebote bzw. Verkaufsaktivitäten an den europäischen Binnenmarkt richten und dabei personenbezogene Daten erhoben werden (Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr - KOM (2012) 11 final). Mit der Datenschutz-Grundverordnung wird für alle Mitgliedstaaten unmittelbar geltendes Recht gesetzt und ein einheitliches Schutzniveau erreicht - auch im Hinblick auf die Löschung von Profildaten. Die Landesregierung sieht darüber hinaus im globalen Zusammenhang die alternative Möglichkeit, mit völkerrechtlichen Verträgen die datenschutzrechtliche Verantwortung von Betreibern der Sozialen Netzwerke, die ihren Sitz außerhalb der EU haben, zu regeln. Auf nationaler Ebene wird die von der Landesregierung beabsichtigte Bundesratsinitiative für höchste Sicherheitseinstellungen bei Sozialen Netzwerken dazu beitragen, dass im Vorhinein weniger Profildaten erhoben werden, deren Löschung ggf. von den Diensteanbietern widerrechtlich unterbleibt.

Für den darüber hinausgehenden Vollzug der datenschutzrechtlichen Vorschriften durch die Anbieter Sozialer Netzwerke ist die Landesregierung nicht zuständig.

### **Weitergabe persönlicher Daten**

Frage 176. Wird die Verwendung personenbezogener Daten von Privatpersonen durch Unternehmen im Internet aus Sicht der Landesregierung ausreichend kenntlich gemacht und den Verbraucherinnen und Verbrauchern die Möglichkeit gegeben, dies zu unterbinden?

Aus Sicht der Landesregierung ist die Verwendung von personenbezogenen Daten von Verbraucherinnen und Verbrauchern im Internet häufig nicht ausreichend transparent gestaltet. Das nationale Recht setzt ein hohes Datenschutzniveau, indes treten unbefriedigende Zustände oftmals aus tatsächlichen Gründen auf.

Auch nach Meinung der Verbraucherzentralen wird die Verwendung personenbezogener Daten durch Unternehmen im Internet nicht ausreichend kenntlich gemacht. So sei für einen Großteil der Verbraucherinnen und Verbraucher nicht ersichtlich, wie es zu der immer persönlicher werdenden Werbeansprache und der passgenauen Artikelauswahl komme. Anbieter stellen in der Regel nicht ausreichend sicher, dass der Nutzer in verständlicher Form über Art, Zweck und Umfang des Einsatzes von Cookies (Datei, die der zeitlich beschränkten Archivierung von Informationen dient) informiert wird. Fehlende Hinweise zur Lebensdauer der Cookies und zu Cookies von Drittanbietern oder das Fehlen von Einwilligungserklärungen beim Einsatz von Permanent-Cookies lassen den Schluss zu, dass kein tatsächliches und wirtschaftliches Interesse an einem aufgeklärten, informierten Internetnutzer besteht. Auch Pixeltracking (Graphik, die beim Aufruf einer Website geladen wird), Network Targeting (Erhebung darüber, mit wem Nutzer verbunden sind), Packet Sniffing (Untersuchung von Datenströmen im Internet) oder Mousetracking (Aufzeichnung und Untersuchung der Mausbewegung, d.h. Aufzeichnung welche Inhalte der Nutzer anklickt) lassen - ohne ausreichende Kenntnis der Nutzer - zu, deren Internetverhalten zu erkunden. Auch wenn der Nutzen vieler dieser Programme unbestritten ist, fehlt es oftmals an Transparenz und Information über deren Einsatz.

Darüber hinaus sei es eine gängige Methode, Verbraucherinnen und Verbraucher z.B. im Rahmen von Gewinnspielen zur Freigabe ihrer persönlichen Daten aufzufordern und ihnen erst mit dem entsprechenden Einverständnis die Teilnahme am Losverfahren zu ermöglichen. Auch hier werde der eigentliche Zweck des Gewinnspiels, das Abgreifen eben dieser Daten zwecks späterer Werbebearbeitung den Verbraucherinnen und Verbraucher nicht transparent dargestellt. Über das Setzen von "Cookies", das "Tracking" oder aber das Betätigen eines "Like-Buttons" werden personenbezogene Daten der Verbraucherinnen und Verbraucher zu Werbezwecken erhoben. Aus diesen Daten wird ein Profil erstellt und die Nutzerinnen und Nutzer mit individualisierter Werbung zu einem Kauf animiert. Oftmals tätigen Verbraucherinnen und Verbraucher daraufhin vorschnelle Interneteinkäufe, wobei geltende Widerrufsrechte nicht die Lösung dieses Problems sein können. In all diesen Fällen bestehen Zweifel, ob noch tatsächlich von einer wirksamen Einwilligung der Nutzerinnen und Nutzer an den Diensteanbieter zur Erhebung und Verwendung der Daten - wie sie das Datenschutzrecht nach § 12 des Telemediengesetzes vorsieht - ausgegangen werden kann, oder ob sich nicht vielmehr die Nutzerinnen und Nutzer mit den grundsätzlich unerwünschten Folgen aus anderen Gründen wie etwa schlicht aus Bequemlichkeit abfinden.

Faktisch hat die Verbraucherin bzw. der Verbraucher daher schon wegen Unkenntnis der Abläufe wenig Handhabe, wenn sie oder er auf bestimmte Leistungen und Angebote nicht verzichten will.

Die Landesregierung spricht sich dafür aus, dass die Werbewirtschaft und die Plattformbetreiber die Verbraucherinnen und Verbraucher in angemessener und verständlicher Weise über die eingesetzten Techniken und die Nutzung der Daten informieren. Zudem sind Transparenz fördernde Maßnahmen (privacy by design) aus Sicht der Landesregierung eine Option für mehr Nutzerfreundlichkeit in diesem Bereich. Ferner wird eine Verpflichtung befürwortet, die aus Sicht des Datenschutzes höchste Sicherheitsstufe gemäß dem Stand der Technik voreinzustellen (siehe Antwort zu Frage 177).

Nach Aussage des Hessischen Datenschutzbeauftragten sollte die ausreichende Kenntnisnahme gesetzgeberisch näher konkretisiert werden und ein einheitlicher Standard angestrebt werden.

Frage 177. Hält die Landesregierung den Schutz der Verbraucherinnen und Verbraucher vor einer unbefugten Weitergabe ihrer persönlichen Daten hinsichtlich des Schutzniveaus und der Durchsetzungskraft der einschlägigen Regelungen für angemessen?

Unternehmer, die mit Verbraucherinnen und Verbrauchern über Verträge verhandeln oder mit Verbraucherinnen und Verbrauchern Verträge schließen, erheben, verarbeiten und nutzen in immer größerem Umfang personenbezogene Daten der Verbraucherinnen und Verbraucher. Diese Daten werden nicht nur für die Abwicklung des Schuldverhältnisses zwischen dem Unternehmer und Verbraucherinnen und Verbraucher erhoben, verarbeitet und genutzt, sondern immer häufiger auch vom Unternehmer kommerziell verwertet. Viele Leistungen, die Verbraucherinnen und Verbrauchern insbesondere im Internet unentgeltlich angeboten werden, wie z.B. die Nutzung von Sozialen Netzwerken, Internetsuchmaschinen, Apps für mobile Endgeräte oder Kundenkarten, lassen sich die Anbieter durch die Daten der Verbraucherinnen und Verbraucher bezahlen, die sie dann für andere Geschäftszwecke verwenden, insbesondere immer öfter auch für eine gewinnbringende Weitergabe an andere Unternehmer. Aufgrund des stetigen Fortschritts in der Informationstechnik ist es so möglich, immer mehr personenbezogene Daten immer schneller zu sammeln, zu systematisieren und auszuwerten, insbesondere auch für Profilbildungen zu nutzen. Deshalb können Verstöße gegen Datenschutzgesetze beim Erheben, Verarbeiten und Nutzen von personenbezogenen Daten einer Verbraucherin oder eines Verbrauchers zu erheblichen Persönlichkeitsrechtsverletzungen bei den betroffenen Verbraucherinnen und Verbrauchern führen.

Das datenschutzrechtliche Schutzniveau im Internet wird maßgeblich durch die bundesgesetzlichen Regelungen im Telemediengesetz bestimmt und muss an die aktuellen technischen Entwicklungen angepasst werden. Hessen hat schon 2011 einen Gesetzentwurf in den Bundesrat eingebracht, in dem eine deutliche Anhebung des gesetzlichen Schutzniveaus gefordert wird. Diese dort aufgeführten Bestrebungen zur Erhöhung des Datenschutzniveaus auf nationaler Ebene sind vom Bundestag innerhalb der 17. Legislaturperiode leider nicht aufgegriffen worden.

Die Landesregierung begrüßt in diesem Zusammenhang den Gesetzentwurf des Bundes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts. Mit der darin enthaltenden Erweiterung der Verbandsklagebefugnis für Verbraucherschutzverbände besteht die Chance, gemeinsam mit den Datenschutzaufsichtsbehörden die Durchsetzungskraft gegen Unternehmen, die gegenüber Verbraucherinnen und Verbrauchern gegen datenschutzrechtliche Vorschriften verstoßen, zu erhöhen.

Frage 178. Wie bewertet die Landesregierung bestehende datenschutzrechtliche Regelungen auf Landes-, Bundes- und Europaabene bezüglich der Weitergabe persönlicher Daten?

Hierzu wird auf die Antwort zu Frage 179 verwiesen.

Frage 179. Welchen Verbesserungsbedarf sieht die Landesregierung bezüglich bestehender datenschutzrechtlicher Regelungen auf Landes-, Bundes- und Europaabene und inwieweit wird sie sich für Verbesserungen einsetzen?

Die vorrangigen Probleme, die Gefahren für das Persönlichkeitsrecht der Internetnutzer bereiten, sind mangelnde Transparenz bei der Erhebung, Verarbeitung oder Nutzung persönlicher Daten durch die Internet-Anbieter, nicht ausreichende Aufklärung über die Risiken für das Persönlichkeitsrecht, wenn persönliche Daten im Internet preisgegeben werden und schließlich der Verbleib der persönlichen Daten, die einmal ins Internet gestellt wurden.

Die Informationspflichten der für die Datenverarbeitung verantwortlichen Stellen sind gesetzlich geregelt - etwa in § 4 Abs. 3 des Bundesdatenschutzgesetzes oder im Telemediengesetz. Nach § 13 des Telemediengesetzes haben die Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren,

das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten, wobei der Inhalt der Unterrichtung für den Nutzer jederzeit abrufbar sein muss. Die konkrete Ausgestaltung der Unterrichtung ist jedoch nicht geregelt. Dies hat zur Folge, dass viele Diensteanbieter zwar ihrer Unterrichtungspflicht nachkommen, aber die maßgeblichen Informationen wenig offensichtlich in ihren Allgemeinen Geschäftsbedingungen unterbringen. Nutzerinnen und Nutzer stoßen dann - wenn überhaupt - erst zufällig nach vielen Klicks auf die Nutzungsbedingungen.

Zudem sind viele Nutzerinnen und Nutzer im Hinblick auf die Preisgabe ihrer personenbezogenen Daten im Internet nicht ausreichend sensibilisiert. Ihnen ist oftmals nicht bewusst, wem sie welche persönlichen Informationen über das Internet offenbaren, wobei dieses Problem umso erheblicher ist, als das Internet "nichts vergisst" und die Diensteanbieter häufig eine Löschung einzelner Daten oder eine Anonymisierung der Nutzerkonten nicht vorsehen oder durchführen. Gerade in Sozialen Netzwerken wie "Facebook" geben Nutzerinnen und Nutzer Vieles über sich und ihr Umfeld bekannt und unterschätzen dabei oftmals die Risiken für sich und Dritte. Gefährdet sind nicht nur die Persönlichkeitsrechte der Betroffenen. Durch die leichtfertige Preisgabe von persönlichen Informationen wie der Veröffentlichung privater Fotos an eine unbestimmte Zahl von anderen Nutzerinnen und Nutzern oder unbedachter Äußerungen wird Problemen wie Pädophilie im Internet, Stalking, Identitätsdiebstahl, Betrug oder der Verlust des Arbeitsplatzes Vorschub geleistet.

Die Landesregierung befürwortet zur Lösung der oben aufgezählten Probleme, die Informationspflichten des Diensteanbieters gegenüber den Nutzern zu stärken. Die Nutzer müssen jederzeit und auch ohne technisches Hintergrundwissen die Möglichkeit haben, datenschutzrechtliche Informationen zu erhalten. Wegen der besonderen Gefahren müssen Diensteanbieter von nutzergenerierten Inhalten, z.B. Sozialen Netzwerken, bei denen die Nutzer viele sehr persönliche Daten ins Internet einstellen können, zusätzliche Pflichten erfüllen. Standardmäßig soll der Diensteanbieter bei der Neuanschaffung eines Nutzers zunächst die höchste von ihm angebotene Sicherheitsstufe voreinstellen, die von dem Nutzer dann gelockert werden kann, wenn er dies möchte. Eine besonders wichtige Voreinstellung, die Verhinderung der Auffindbarkeit und Auslesbarkeit mittels externer Suchmaschinen, wird vorgegeben. Auch durch die Aufklärung über die Risiken der Veröffentlichung persönlicher Daten soll der Nutzer sensibilisiert werden. Schließlich sollen Nutzerinnen und Nutzer immer die Möglichkeit haben, selbst zu veranlassen, dass die in dem Telemediendienst veröffentlichten Daten wieder gelöscht bzw. zumindest gesperrt oder anonymisiert werden. Um diese Ziele zu verwirklichen, hatte die Landesregierung bereits 2011 einen entsprechenden Gesetzesantrag betreffend eines Gesetzes zur Änderung des Telemediengesetzes in den Bundesrat eingebracht (BR-Drucks. 156/11), der allerdings in der 17. Legislaturperiode des Deutschen Bundestages nicht berücksichtigt wurde. Die Landesregierung nimmt von dem im Gesetzesantrag formulierten Zielen keinen Abstand. Sie fühlt sich auch weiterhin ihren Bürgerinnen und Bürgern verpflichtet, im Bereich der IT-Produkte die Rechte der Verbraucherinnen und Verbraucher zu stärken und für eine weitere Erhöhung des Datenschutzniveaus zu sorgen. Entsprechend des Koalitionsvertrages der die Regierungskoalition tragenden Parteien für die 19. Wahlperiode des Hessischen Landtags wird sich die Landesregierung bei der Nutzung personenbezogener Daten, insbesondere auch im Internet, für einen Einwilligungsvorbehalt und praxismgerechte Widerspruchsrechte sowie Löschungsmöglichkeiten für die Verbraucherinnen und Verbraucher einsetzen. Deshalb spricht sie sich für das Vorhaben der Datenschutz-Grundverordnung aus, mit der insbesondere auch die Diensteanbieter verpflichtet werden, durch eine entsprechende Technik ("privacy by design"), datenschutzfreundlichen Grundeinstellungen ("privacy by default") und dem jeweiligen Stand der Technik entsprechende Voreinstellungen der höchsten Sicherheitsstufe die Datenschutzrechte der Verbraucherinnen und Verbraucher zu wahren. Neben den datenschutzrechtlichen Bestimmungen des Telemediengesetzes gewinnen im Hinblick auf die Weitergabe persönlicher Daten die Vorschriften des Bundesdatenschutzgesetzes sowie des Hessischen Datenschutzgesetzes Bedeutung. In einem globalen und europäischen Vergleich garantieren diese Vorschriften ein hohes Schutzniveau, das nationale Datenschutzrecht nimmt eine Vorreiterstellung ein. Die Vorschriften des Bundesdatenschutzgesetzes sowie des Hessischen Datenschutzgesetzes überzeugen durch ihre Bestimmtheit und sind für den Rechtsanwender gut zu vollziehen. Nach den Datenschutzgesetzen des Bundes und des Landes dürfen personenbezogene Daten von öffentlichen wie auch nicht-öffentlichen Stellen, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen, an Dritte nur dann weitergegeben werden, wenn eine Einwilligung des Betroffenen in die Datenverarbeitung vorliegt oder eine spezialgesetzliche Rechtsgrundlage die Datenweitergabe ausdrücklich erlaubt. Im Weiteren sehen die Datenschutzgesetze des Bundes und des Landes die Befugnis vor, nach einer Abwägung Dritten personenbezogene Daten zu übermitteln. Zugunsten des von der Datenverarbeitung Betroffenen wird diese dritte Möglichkeit der Datenweitergabe restriktiv gehandhabt. Bußgeldvorschriften scheinen den Schutz der Verbraucherinnen und Verbraucher vor unbefugter Datenweitergabe hinreichend zu sichern. Auf europäischer Ebene garantiert die Datenschutzrichtlinie Mindeststandards für die Weitergabe personenbezogener Daten. Die Landesregierung begrüßt darüber hinaus das Vorhaben einer Europäischen Datenschutz-Grundverordnung. Sie setzt sich dafür ein, dass auch die im Hinblick auf das Verhältnis zwischen Staat und Bürger

geltenden Maßstäbe der Datenschutzgesetze des Bundes sowie des Landes im Verhältnis zwischen privaten Akteuren gelten und insbesondere auch datenverarbeitende Stellen, die ihren Sitz außerhalb der EU haben und in der EU agieren, diese Maßstäbe achten und einhalten.

Darüber hinaus ist es eine wichtige Aufgabe des Landes, Verbraucherinnen und Verbraucher auf Gefahren und Risiken in Zusammenhang mit diesen Techniken aufmerksam zu machen und mögliche Schutzmechanismen aufzuzeigen. Die Landesregierung spricht sich dafür aus, dass die Forschung in technischen Jugendschutzprogrammen auf Bundesebene z.B. zum "Digitalen Vergessen" vorangetrieben wird.

Frage 180. Wie bewertet die Landesregierung die Weitergabe von Nutzungsdaten an ausländische und außer-europäische Sicherheitsbehörden?

Bestands- und Nutzungsdaten nach dem Telemediengesetz (TMG) stellen ebenso wie Bestands- und Verkehrsdaten nach dem Telekommunikationsgesetz (TKG) wesentliche Ermittlungsansätze zum Nachweis von Tat und Täterschaft dar. Die Erhebung und Verwertung sind in den Vorschriften des TMG und des TKG jeweils in Verbindung mit den einschlägigen Eingriffsbefugnissen des Strafverfahrens- und Gefahrenabwehrrechts geregelt. Internetkriminalität weist per se internationale bis globale Züge auf. Strafverfahren lassen sich häufig nur erfolgreich durch eine wirksame und zeitnahe internationale Zusammenarbeit führen. Vor diesem Hintergrund ist die Datenerhebung durch deutsche Behörden im Ausland und die Datenerhebung durch ausländische Behörden im Inland im Rahmen der geltenden landesspezifischen Regelungen und zwischenstaatlichen Vereinbarungen eine unabdingbare Voraussetzung zur Bekämpfung des Cybercrime oder der Internetkriminalität.

Konkrete Erfahrungen mit der Übermittlung von Internet-Nutzungsdaten an ausländische Behörden liegen dem Hessischen Landeskriminalamt nicht vor.

Das Landesamt für Verfassungsschutz darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- oder zwischenstaatliche Stellen nur übermitteln, wenn die Übermittlung zur Erfüllung seiner Aufgaben oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist. Die Übermittlung hat zu unterbleiben, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Belange der betroffenen Person entgegenstehen. Dabei ist die Übermittlung nur im Einvernehmen mit dem Bundesamt für Verfassungsschutz zulässig. Sie ist aktenkundig zu machen. Der Empfänger ist darauf hinzuweisen, dass die übermittelten personenbezogenen Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden und das Landesamt für Verfassungsschutz sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

Frage 181. Wie bewertet die Landesregierung den aktuellen Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei und welche Ausnahmen sieht der Gesetzentwurf nach Auffassung der Landesregierung vor?

Die Landesregierung bewertet den aktuellen Gesetzentwurf (BR-Drs. 70/14) durchweg positiv. Der Gesetzentwurf geht auf eine hessische Initiative zurück und wurde von Hessen in den Bundesrat eingebracht, um die bestehenden Strafbarkeitslücken im Bereich der Datenhehlerei zu schließen.

Die Tatbestandsausschlussregelung in § 202d Absatz 5 StGB-E lautet:

"Die Absätze 1 bis 4 gelten nicht für Handlungen, die ausschließlich der Erfüllung gesetzlicher Pflichten durch Amtsträger oder deren Beauftragte dienen. Die Absätze 1 bis 4 gelten ebenfalls nicht für Handlungen von Amtsträgern oder deren Beauftragten, um Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zuzuführen."

Frage 182. Gab es Änderungen an dem am 14.03.2014 aufgrund der Diskontinuität erneut in den Bundesrat eingebrachten Gesetzentwurf zur Strafbarkeit der Datenhehlerei im Vergleich zu dem im Mai 2013 eingebrachten Entwurf?

Der am 3. Mai 2013 von Hessen in den Bundesrat eingebrachte Gesetzesantrag zur Strafbarkeit der Datenhehlerei (BR-Drs. 284/13) wurde auf Vorschlag des Finanzausschusses des Bundesrates mit Beschluss des Bundesrates vom 7. Juni 2013 wie folgt ergänzt:

In Artikel 1 Nummer 4 wurde dem § 202d Absatz 5 folgender zweiter Satz angefügt:

"Die Absätze 1 bis 4 gelten ebenfalls nicht für Handlungen von Amtsträgern oder deren Beauftragten, um Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zuzuführen."

Aufgrund dieser Ergänzung kam es zu den im Weiteren aufgeführten Folgeänderungen:

- a) Im Vorblatt Abschnitt B wurde Absatz 1 Satz 3 wie folgt gefasst:  
 "Nach § 202d Absatz 5 werden Handlungen eines Amtsträgers oder seiner Beauftragten nicht vom Tatbestand der Datenhehlerei erfasst, wenn diese in Erfüllung gesetzlicher Pflichten handeln bzw. die Daten ausschließlich in einem Besteuerungs-, Straf- oder Ordnungswidrigkeitenverfahren verwertet werden."
- b) In der Einzelbegründung zu Artikel 1 Nummer 4 (§ 202d StGB-E) wurde die Begründung zu Absatz 5 wie folgt geändert:
- aa) Dem zweiten Absatz wurde folgender Satz angefügt:  
 "Hierzu enthält § 202d Absatz 5 Satz 2 StGB-E eine ausdrückliche Klarstellung des gesetzgeberischen Willens, dass Amtsträger beim Ankauf von Datenmaterial zur ausschließlichen Verwendung in einem Besteuerungsverfahren nicht mit Strafe bedroht werden dürfen."
- bb) Dem vierten Absatz wurden folgende Sätze angefügt:  
 "Durch den Zusatz in § 202d Absatz 5 Satz 2 StGB-E soll sichergestellt werden, dass unabhängig von der Diskussion über die Zulässigkeit des Datenankaufs unter verwaltungsrechtlichen Gesichtspunkten solche Handlungen von Amtsträgern bzw. ihrer Beauftragten jedenfalls im Strafrecht nicht relevant sind. Die im Schrifttum geäußerten Zweifel, ob in der Abgabenordnung bzw. der Strafprozessordnung eine Rechtsnorm existiert, die den Datenankauf ermöglicht oder ggf. sogar zum Ankauf von Daten verpflichtet, sind damit für das Strafrecht nicht relevant."

Mit diesen vorgenannten Ergänzungen zum ursprünglichen hessischen Gesetzesantrag vom 3. Mai 2013 wurde der Gesetzentwurf dann vom Bundesrat am 7. Juni 2013 beschlossen (BR-Drs. 284/13 (B)). Dieser vom Bundesrat am 7. Juni 2013 beschlossene Gesetzentwurf wurde - mit den beschlossenen Ergänzungen - dann am 14. März 2014 erneut von Hessen in den Bundesrat eingebracht und unverändert vom Bundesrat beschlossen.

Frage 183. Welche Maßnahmen plant oder ergreift die Landesregierung, um die Verbraucherinnen und Verbraucher über ihr Recht, die Nutzung ihrer eigenen Daten durch Dritte zu verbieten, aufmerksam zu machen?

Das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz hat in der Vergangenheit Verbraucherinnen und Verbraucher in Form von verschiedenen Pressemitteilungen auf ihr Recht, die Nutzung eigener Daten durch Dritte zu verbieten, aufmerksam gemacht. Das Thema "Datenschutz im Internet" wird zudem in verschiedenen Beiträgen des Verbraucherportals [www.verbraucherfenster.de](http://www.verbraucherfenster.de) aufgegriffen.

Weitere wichtige Aufklärung in Form von Information und Beratung in diesem Bereich führen die Verbraucherzentrale Hessen und der DHB-Netzwerk Haushalt Hessen durch, die vom Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz zur Wahrnehmung ihrer Aufgaben eine institutionelle Förderung erhalten. Die Verbraucherzentrale hat zum Thema "Datenschutz" zudem den Ratgeber "Meine Daten gehören mir" aufgelegt, welcher Verbraucherinnen und Verbraucher für den Umgang mit Daten sensibilisiert.

Frage 184. Wie beurteilt die Landesregierung das Risiko, dass persönliche Daten von Verbraucherinnen und Verbrauchern zu Werbezwecken durch Anbieter genutzt werden?

Voreingestellte Werbezustimmungen, die per Klick, also durch das Entfernen eines bereits gesetzten Häkchens, erst wieder ungültig gemacht werden müssen, sind oftmals zuungunsten der Verbraucherin oder des Verbrauchers gängige Praxis und machen ein aktives Handeln des Nutzers notwendig. Was also an- oder ausgeklickt werden muss, um dies oder jenes zu schützen oder abzulehnen, erfordert eine zeitintensive Auseinandersetzung und ist leider nicht immer nutzerfreundlich. Im Rahmen der VSMK 2014 hat sich das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz in diesem Zusammenhang dafür ausgesprochen, dass die Datenerhebung, -verarbeitung und -nutzung für Werbezwecke nur mit ausdrücklicher Einwilligung durch die Nutzer erfolgen sollte (opt-in).

Frage 185. Verfügen die Verbraucherinnen und Verbraucher aus Sicht der Landesregierung über ausreichende Möglichkeiten, eine Nutzung ihrer persönlichen Daten zu unterbinden?

Die Verbraucherzentralen sehen deutliche Gefahren in der gängigen Nutzung der persönlichen Daten von Verbraucherinnen und Verbrauchern zu Werbezwecken. Häufigstes Problem ist, dass die Nutzung der Daten bzw. der hieraus zusammengestellten Profile nicht transparent offen gelegt und den Verbraucherinnen und Verbrauchern gegenüber auch nicht verständlich und nachvollziehbar kommuniziert wird. Gängige Praxis ist oftmals, dass das Einverständnis zur Nutzung der Daten mit dem Akzeptieren der Nutzungsbedingungen als gegeben vorausgesetzt wird,

ohne das auch ein Fortführen des Einkaufs nicht möglich ist. Nur teilweise gibt es eine Möglichkeit, zu widersprechen oder per opt-out das Einverständnis nicht zu erteilen. In welchem Umfang und welcher Professionalität die Verarbeitung und Weitergabe der Daten dann im Weiteren erfolgt, ist für den durchschnittlichen Nutzer bzw. die durchschnittliche Nutzerin schon aufgrund der häufig zwischen den Unternehmen bestehenden, oft auch branchenübergreifenden Verbindungen nicht ersichtlich.

Von den Verbraucherzentralen wird es zudem als kritisch eingeschätzt, dass Dienstleistungen und Internetdienste sich über den Geldwert der bereit gestellten persönlichen Daten der Nutzer und Nutzerinnen finanzieren. In diesem Fall ist die Bereitstellung der Daten und das Einverständnis zur Nutzung in der Regel grundlegende Vertragsbedingung, ohne die es gar nicht erst zu einem Vertragsverhältnis kommt. Aktuell ist das sogenannte Kopplungsverbot normiert in § 28 Abs. 3b BDSG. Nach dieser Regelung ist es zwar grundsätzlich untersagt, den Abschluss eines Vertrages von der Einwilligung der Nutzerinnen und Nutzer zur Datennutzung abhängig zu machen. Dieses Kopplungsverbot wird allerdings eingeschränkt, denn es soll nur gelten, wenn "dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist". Das Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz sieht diese Einschränkung des Kopplungsverbotes kritisch.

Soweit mit der Frage die Möglichkeit von Verbraucherinnen und Verbrauchern angesprochen ist, die Nutzung ihrer Daten zu Werbezwecken und die Zusendung unrechtmäßiger Werbung zu unterbinden, ist zwischen juristischen und technischen Mitteln zu unterscheiden. Gegenüber Angeboten in Deutschland und im Europäischen Wirtschaftsraum (EWR) gelten die Vorschriften des BDSG und die Vorgaben der Europäischen Datenschutzrichtlinie (RL 95/46). Allgemein sind die Erhebung, Verwendung und Nutzung personenbezogener Daten zum Zweck der Werbung nur dann zulässig, wenn die Person ihre Einwilligung hierzu erteilt hat oder dies aufgrund eines Gesetzes erlaubt ist (§ 4 Abs. 1 BDSG). Im Anwendungsbereich des Bundesdatenschutzgesetzes ist die Werbung anhand listenmäßig erfasster Daten auch ohne Einwilligung von Gesetzes wegen erlaubt, soweit die in § 28 Abs. 3 BDSG genannten Voraussetzungen beachtet werden. Die Verbraucherinnen und Verbraucher haben jedoch das Recht zum Widerspruch, um die Verwendung ihrer Daten für Werbezwecke zu unterbinden (§ 28 Abs. 4 S. 1 BDSG). Darüber hinaus können Empfängerinnen und Empfänger unerwünschter Werbung Auskunft, Berichtigung, Sperrung und Löschung ihrer personenbezogenen Daten verlangen (§§ 34, 35 BDSG).

Die Aufsicht über die Einhaltung der Datenschutzgesetze fällt in die Zuständigkeit unabhängiger Datenschutzaufsichtsbehörden (§ 38 BDSG). Gegenüber Anbietern, für die das BDSG oder vergleichbare Regelungen in den EU-Mitgliedsstaaten nicht gelten, sind die Verbraucherinnen und Verbraucher auf Mittel des technischen Selbstschutzes angewiesen. Sie können etwa Filterprogramme gegen Spam-E-Mails auf ihren Rechnern installieren oder auf den Mail-Servern ihrer Provider installieren lassen.

## Cloud Computing

Frage 186. Wie schätzt die Landesregierung mögliche Gefahren für die Datensicherheit der Nutzerinnen und Nutzer ein, die von Cloud Computing ausgehen können?

Wer Cloud Computing-Dienste nutzen möchte, sollte sich der damit verbundenen Gefahren und Risiken bewusst sein, da hier sensible private Daten Dritten zur Aufbewahrung oder Weiterverarbeitung gegeben werden. Die Gefahren für die Sicherheit der Daten sind vielfältig. Der Anbieter könnte die Daten einsehen. Der Nutzer sollte deshalb seine Daten selbst verschlüsseln und diese erst dann an den Anbieter übermitteln. Der Anbieter des Cloud Computing sollte nicht in der Lage sein, diese Daten zu entschlüsseln. Die Verschlüsselung spielt auch bei der Datenübertragung eine wichtige Rolle. Vor allem beim Datentransfer außerhalb Deutschlands besteht die Gefahr, dass Daten unberechtigt gelesen werden. Für den Nutzer ist oft nicht ersichtlich, auf welchem Weg Datenpakete ihren Weg zum Anbieter nehmen. Ausländische Nachrichtendienste verfügen teilweise über technische und rechtliche Möglichkeiten, Daten bei der Übertragung auszulesen. Das unverschlüsselte Übermitteln der Daten an einen Cloud Computing-Anbieter vereinfacht deren Auslesen. Je nachdem in welchem Staat die Daten gespeichert werden oder in welchem Staat der Anbieter seinen Sitz hat, können die dortigen Sicherheitsbehörden einen gesetzlich geregelten Zugriff auf diese Daten haben oder sich diesen verschaffen.

Die Datensicherheit muss bei diesen Diensten oberste Priorität haben. Dies gilt für die Verschlüsselung der Daten auf dem Übertragungsweg zwischen dem Rechner und dem Cloud Computing-Dienst-Anbieter genauso wie für den Schutz der Daten im Onlinespeicher selbst.

Auch nach Auffassung des Hessischen Datenschutzbeauftragten erfordert Cloud Computing eine sorgfältige Abwägung der Chancen und Risiken. Die Risiken hängen davon ab, in wessen Verantwortungsbereich das Cloud Computing fällt. Zu echten Gefahren werden die Risiken erst,

wenn das Cloud Computing dem Kontrollzugriff der Bundesrepublik Deutschland entzogen ist. Ob das der Fall ist, hängt von den jeweiligen konkreten Umständen ab.

Frage 187. Wie beurteilt die Landesregierung die Nutzung persönlicher Daten durch Cloud-Anbieter zum Zwecke der personalisierten Werbung?

Das Ministerium des Innern und für Sport unterscheidet in seiner Beurteilung zwischen einer einvernehmlich zwischen Anbieter und Nutzer vereinbarten Vorgehensweise, die als unkritisch angesehen wird, und einer nicht einvernehmlichen Nutzung. Hier greift der im Koalitionsvertrag der die Regierungskoalition tragenden Parteien verankerte Leitsatz: "Was außerhalb des Netzes verboten ist, muss auch im Netz verboten sein".

Nach § 28 Abs. 3 des Bundesdatenschutzgesetzes ist die Nutzung personenbezogener Daten für Zwecke der Werbung unter den im Gesetz genannten Voraussetzungen allerdings auch ohne die Einwilligung des Betroffenen zulässig.

Die Nutzung persönlicher Daten zum Zwecke personalisierter Werbung ohne ausdrückliche Zustimmung der Verbraucherin oder des Verbrauchers (opt-in) wird vom Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz kritisch bewertet. Auf die Antworten zu den Fragen 184 und 185 wird verwiesen.

Frage 188. Welche Maßnahmen zur Aufklärung der Verbraucherinnen und Verbraucher über die Risiken von Cloud Computing plant oder ergreift die Landesregierung, insbesondere hinsichtlich des Datenschutzes?

In ihrem Portal [www.verbraucherfenster.de](http://www.verbraucherfenster.de), das sich an Verbraucherinnen und Verbraucher richtet, informiert die Landesregierung regelmäßig auch über neue Entwicklungen im Bereich des Internets sowie von diesen ausgehenden Gefahren und Risiken in Form von Beiträgen oder Experten-Interviews.

In einer Reihe des VerbraucherFensters zum Thema Datenklau und in Form eines Interviews mit einem IT-Experten in Sachen "Daten im Cloud-Speicher: Heiter bis wolkig", ([http://verbraucherfenster.hessen.de/irj/VF\\_Internet?rid=HMULV\\_15/VF\\_Internet/nav/485/48553a3c-a9ee-611a-eb6d-f144e9169fcc,7563057e-d065-8041-79cd-aa2b417c0cf4,,11111111-2222-3333-4444-100000005003%26overview=true.htm&uid=48553a3c-a9ee-611a-eb6d-f144e9169fcc](http://verbraucherfenster.hessen.de/irj/VF_Internet?rid=HMULV_15/VF_Internet/nav/485/48553a3c-a9ee-611a-eb6d-f144e9169fcc,7563057e-d065-8041-79cd-aa2b417c0cf4,,11111111-2222-3333-4444-100000005003%26overview=true.htm&uid=48553a3c-a9ee-611a-eb6d-f144e9169fcc)), wurden die Risiken und Gefahren des Cloud Computing vorgestellt. Via Twitter wird über die wichtigsten Aspekte hinsichtlich Verbraucherschutzinformationen sowohl der Landesregierung als auch überregional zusätzlich berichtet. Zudem wird auf wissenswerte Neuigkeiten in Verbraucherschutzfragen aufmerksam gemacht. Die Angebote des VerbraucherFensters [www.verbraucherfenster.de](http://www.verbraucherfenster.de) werden auf diesem Wege zusätzlich beworben.

Weitere wichtige Aufklärung in Form von Information und Beratung in diesem Bereich führen die Verbraucherzentrale Hessen und der DHB-Netzwerk Haushalt Hessen durch, die vom Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz zur Wahrnehmung ihrer Aufgaben eine institutionelle Förderung erhalten.

Im Rahmen von Sensibilisierungsgesprächen und in zusammen mit den hessischen Industrie- und Handelskammern veranstalteten Vorträgen zum Themenkomplex "Abwehr elektronischer Angriffe", "Cyberspionage" etc. informiert das Landesamt für Verfassungsschutz regelmäßig über die Risiken des Cloud Computing und über Möglichkeiten der Datensicherung.

Frage 189. Wie beurteilt die Landesregierung die Sicherheit von in der Cloud abgelegten Daten mit Blick auf Zugriffe durch ausländische Behörden?

Hierzu wird auf die Antwort zu Frage 186 verwiesen.

Frage 190. Auf welcher Rechtsgrundlage und durch welche Behörden können derartige Zugriffe erfolgen?

Es existiert keine Rechtsgrundlage für den unmittelbaren Zugriff ausländischer Behörden auf Daten, die in einer Cloud abgelegt sind. § 4b des Bundesdatenschutzgesetzes erfasst lediglich Fälle der Übermittlung von personenbezogenen Daten an ausländische Behörden, die bei öffentlichen oder ihnen datenschutzrechtlich gleichgestellten nicht-öffentlichen Stellen in einer Cloud gespeichert sind. Die Vorschrift regelt jedoch nicht die Fälle, in denen personenbezogene Daten durch (juristische) Personen des Privatrechts ohne öffentlichen Auftrag in einer Cloud gespeichert werden.

Frage 191. Wie bewertet die Landesregierung das Safe-Harbour-Abkommen zwischen der EU und den USA?

Frage 192. Wie schätzt die Landesregierung die Zertifizierung von Unternehmen durch das Safe-Harbour-Abkommen ein?

Die Fragen 191 und 192 werden zusammen beantwortet.

Die Reform des Europäischen Datenschutzrechts und die parallel dazu in den Vereinigten Staaten von Amerika angelaufene Debatte über einen neuen Rechtsrahmen für den Datenschutz in der Informationsgesellschaft eröffnen die Chance, diese Forderungen in umfassend verbindlicher und zeitgemäßer Gewährleistung der informationellen Selbstbestimmung umzusetzen. Diese gilt es zu nutzen, um sich auf europäischer und internationaler Ebene für eine proaktive Kooperation zwischen den entsprechenden EU- und US-Behörden auszusprechen, um eine bessere Durchsetzung der bestehenden rechtlichen nationalen und europäischen Regelungen und des Schutzes personenbezogener Daten zu erreichen.

Die Entscheidung der Kommission vom 26.07.2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des "sicheren Hafens" und der diesbezüglich "Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (ABl. L 215 vom 25. August 2000, S. 7 - 47; im Folgenden: Safe-Harbour-Abkommen) ist vor dem Hintergrund der Datenschutzrichtlinie zu würdigen. Nach der Datenschutzrichtlinie ist eine Übermittlung personenbezogener Daten aus den Mitgliedsstaaten an Drittstaaten wie den USA, die über kein in der EU verwirklichtes Datenschutzniveau verfügen, ausgeschlossen. Von diesem Grundsatz ausgehend stellt die Entscheidung der Europäischen Kommission eine Ausnahme für den transatlantischen Datenverkehr dar. Sie ist gleichermaßen als (politischer) Kompromiss und als (rechtliches) Abwägungsergebnis zwischen dem Interesse an einem möglichst hohen Schutzniveau einerseits und zwingenden wirtschaftlichen Notwendigkeiten andererseits zu verstehen.

Die Landesregierung hat die Entscheidung des Europäischen Parlaments vom 12. März 2014, das Safe-Harbour-Abkommen auszusetzen, zur Kenntnis genommen. Die freiwillige Safe-Harbour-Zertifizierung hat sich nicht als nachhaltiges Instrumentarium erwiesen, welches im transatlantischen Datenverkehr ein innerhalb der EU bestehendes Datenschutzniveau gewährleisten kann. So sind der Landesregierung beispielsweise eine Vielzahl von durch "Facebook" begangenen Verstöße gegen das Safe-Harbour-Abkommen bekannt (Poller, Andreas/Waldmann, Ulrich, SIT Technical Reports SIT-TR-2013-02 - Soziale Netzwerke bewusst nutzen, Ein Dossier zu Datenschutz, Privatsphärenschutz und Unternehmenssicherheit, Herausgeber Waidner, Michael, August 2013, im Folgenden: SIT Technical Reports SIT-TR-2013-02; [https://www.sit.fraunhofer.de/fileadmin/dokumente/studien\\_und\\_technical\\_reports/Soziale-Netzwerke-2013.pdf](https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Soziale-Netzwerke-2013.pdf)). "Facebook" hat u.a. Daten über Pokes (Anstupsen) nach dem "Entfernen" nicht gelöscht, Schattenprofile erstellt, (vermeintlich) gelöschte Postings, Markierungen auf Fotos und Nachrichten nach dem "Entfernen" weiterhin gespeichert und keine Vorkehrungen dafür getroffen, dass Nutzerinnen und Nutzer auch ohne vorherige Zustimmung zu Gruppen hinzugefügt werden. Außerdem bietet das Zertifizierungsverfahren, das im Wesentlichen aus einer formalen Beitrittserklärung gegenüber dem US-Handelsministerium besteht, keine Gewähr für ein aus europäischer Sicht hinreichendes Datenschutzniveau. Bei der Selbstzertifizierung entfallen die staatliche und damit eine unabhängige Überprüfung, ohne eine staatliche Kontrolle aber fehlt der Anreiz, auch nach der Zertifizierung die proklamierten Datenschutzabreden einzuhalten. Daher setzt sich die Landesregierung auf Europaebene im Rahmen der EU-Datenschutzreform für die Einführung einer Datenschutz-Grundverordnung ein. Mit dieser Verordnung soll auch die datenschutzrechtliche Verantwortung von solchen Unternehmen festgelegt werden, die ihren Sitz außerhalb der EU haben und in der EU agieren. Darüber hinaus teilt die Landesregierung die Auffassung der Bundesregierung, die sich wiederholt für eine Verbesserung der Safe-Harbor-Regelung ausgesprochen hat, die schnellstmögliche Vorlage des Kommissionsberichts zu Safe Harbor fordert und in der EU auf Nachverhandlungen des Safe-Harbor-Abkommens drängt. Safe-Harbor soll mit der geplanten Datenschutz-Grundverordnung in Einklang stehen. Daher befürwortet die Landesregierung den entsprechenden Vorschlag der Bundesregierung, mit der Datenschutz-Grundverordnung einen rechtlichen Rahmen zu schaffen, in dem festgelegt wird, dass von Unternehmen, die sich Modellen wie Safe-Harbor anschließen, angemessene Garantien zum Schutz personenbezogener Daten als Mindeststandards übernommen werden müssen und dass diese Garantien wirksam kontrolliert und Verstöße gebührend sanktioniert werden.

Frage 193. Welche Auffassung vertritt die Landesregierung hinsichtlich des möglichen Verlusts der Kontrolle von Nutzerinnen und Nutzern über ihre Daten bei der Nutzung von Cloud-Diensten?

Die Landesregierung ist der Auffassung, dass Nutzerinnen und Nutzer bei Cloud-Diensten keine Möglichkeit haben, die Zusicherungen des Anbieters hinsichtlich des Ortes der Verarbeitung und Speicherung der Daten zu überprüfen und deshalb grundsätzlich davon ausgehen müssen, dass die Nutzung von Cloud-Diensten die Möglichkeit des Verlustes der Kontrolle über ihre Daten einschließt. Wenn die Nutzerinnen und Nutzer dies bei informierter Abwägung akzeptieren und keine Rechte Dritter verletzen, hält die Landesregierung dies für unkritisch.

Im Übrigen wird auf die Antwort zu den Fragen 186 und 187 verwiesen.

Frage 194. Welche Daten von Nutzerinnen und Nutzern werden durch öffentliche Stellen des Landes Hessen in einer Cloud gespeichert und welche Sicherungsmaßnahmen erfolgen?

Dem Ministerium des Innern und für Sport sind keine Verfahren der Hessischen Landesregierung bekannt, die Daten der Nutzerinnen und Nutzer oder Daten der Bürgerinnen und Bürgern in einer Public-Cloud speichern. Zur Optimierung der Rechenzentren der öffentlichen Hand werden Cloud-Technologien eingesetzt, Verarbeitung und Speicherung erfolgt dabei jedoch vollständig unter eigener Kontrolle (sogenannte private cloud).

Frage 195. Werden Nutzerinnen und Nutzer oder öffentliche Stellen, wie Fraktionen des Hessischen Landtages, darüber informiert, dass ihre Daten in einer Cloud gespeichert werden?

Auf die Antwort zur Frage 194 wird verwiesen.

### **Analyse des Surfverhaltens**

Frage 196. Welche Position vertritt die Landesregierung zu der Erstellung von persönlichen Nutzungsprofilen/Bewegungsprofilen von Internetnutzerinnen und -nutzern durch Internetanbieter, Smartphones oder Suchmaschinen?

Anbieter von Waren und Dienstleistungen haben ein nachvollziehbares Interesse, Informationen über das Nutzerverhalten auf der jeweiligen Webseite zu generieren. Die Analyse des Nutzerverhaltens dient nicht nur dazu, den eigenen Internetauftritt und die Angebote zu verbessern, sondern auch dazu, dem Nutzer individuelle, auf seine Bedürfnisse zugeschnittene Angebote zu präsentieren. Die Erstellung von Nutzungs- und Bewegungsprofilen erhöht die Absatzchancen für die Anbieterseite und kann für den Nutzer eine gute Orientierungshilfe in einem vielfältigen Produktmarkt sein.

Mit der in der Vergangenheit deutlich verbesserten Technik sind aber nicht nur die Möglichkeiten zur Analyse des Nutzerverhaltens, sondern auch die Voraussetzungen für die Zusammenführung der an verschiedenen Stellen gesammelten Nutzerdaten weiterentwickelt worden. Kritisch zu bewerten sind insbesondere webseitenübergreifende Auswertungen, die auf eine gezielte Person zurückzuführen sind und somit zu einer individualisierten Profilbildung genutzt werden können. Nutzerinnen und Nutzer sollten daher von technischen Schutzmöglichkeiten Gebrauch machen. Die Installation von Schutzprogrammen allein ist jedoch nicht ausreichend, um Nutzer wirksam zu schützen.

Die Landesregierung erachtet in diesem Zusammenhang die Datensparsamkeit als wichtiges Ziel. Daten sollten nur im Einverständnis der Verbraucherin oder des Verbrauchers erhoben werden. Für die Verbraucherinnen und Verbraucher muss klar ersichtlich werden, für welchen Zweck und vor welchem Hintergrund die Daten erhoben werden. Klare und transparente Informationen sind oberstes Gebot.

Frage 197. Unterstützt die Landesregierung die Einführung einer sog. "Don't track me"-Option bei Programmen, die es den Nutzerinnen und Nutzern ermöglicht, einzustellen, nicht in ihrem Surfverhalten protokolliert zu werden?

Viele Webseiten und Anzeigen-Netzwerke messen das Verhalten von Internetbenutzern, da dies wertvolle Informationen liefert, die für Re-Targeting oder für die Erstellung eines Profils benutzt werden. Diese Nutzerinformationen werden allerdings nicht nur für kommerzielle Zwecke benutzt. Das Speichern eines von Produkten einer früheren Surfrunde im Einkaufswagen kann allerdings auch die Nutzung vereinfachen.

Do Not Track (DNT) ist ein so genanntes HTTP-Header-Feld und signalisiert einer Webseite oder Webanwendung den Wunsch, dass diese über die Aktivitäten des Besuchers kein Nutzungsprofil erstellt. Firefox war der erste Browser der dieses Feld unterstützte, später folgten Internet Explorer (ab Version 9), Safari, Opera und Chrome.

DNT bietet Internetbenutzern die Möglichkeit, zu verhindern, dass Informationen über ihr Nutzerverhalten ohne Zustimmung an Dritte weitergegeben werden. Grundsätzlich wird der Ansatz von DNT unterstützt, da der Wunsch des Nutzers, keine Aktivitäten von ihm zu speichern, an eine Webseite übermittelt wird. Die Landesregierung setzt sich dafür ein, dass die Anbieter von Internetseiten nur Daten speichern, die für die Verwendung der Webseite notwendig sind und nur Daten erhoben werden, wenn die Verbraucherin oder der Verbraucher informiert ist und in die Erhebung dieser Daten einwilligen kann.

Die mit DNT verbundenen Programme setzen zur Sicherstellung ihrer Funktionsfähigkeit eine Technik ein, die eine individuelle Erfassung und Auswertung des Surfverhaltens ermöglicht. Die Landesregierung ist daher skeptisch, dass die mit dem Einsatz solcher Programme verbundenen technischen Lösungen einen in jeder Hinsicht zufriedenstellenden Schutz vor einer ungewollten Analyse des Surf-Verhaltens darstellen - insbesondere weil die Analyse des Surfver-

haltens in der Regel vom Nutzer nicht bemerkt wird und somit die Wirkung eines Schutzprogramms schwer nachprüfbar ist.

Frage 198. Wie steht die Landesregierung zu der Idee einer "Don't track me"-Datenbank, in die sich Internetnutzerinnen und Internetnutzer eintragen lassen können, um eine strafrechtliche Handhabe gegen Internetseitenbetreiber zu haben, die dennoch Daten über die Nutzerin oder den Nutzer sammeln (angelehnt an die "Don't call me"-Methode in den USA)?

Inwieweit eine so genannte DNT-Datenbank den Ermittlungsbehörden die Bekämpfung der Informations- und Kommunikationskriminalität erleichtern könnte, vermag die Landesregierung nicht zu beurteilen.

Frage 199. Welche weiteren Möglichkeiten sieht die Landesregierung, um das Protokollieren des Surfverhaltens von Internetnutzerinnen und Internetnutzern zu unterbinden?

Da sich die technischen Möglichkeiten sehr schnell weiterentwickeln, müssen Internetnutzer vom Kindes- bis zum Seniorenalter über den Umgang mit dem Internet, die von diesem ausgehenden Risiken, Gefährdungen sowie Fallstricke informiert werden. Die Initiative "Deutschland sicher im Netz", die unter Schirmherrschaft des Bundesministerium des Innern steht, arbeitet durch das Verbreiten nützlicher Informationen und konkreter Hilfestellungen täglich daran, dass Verbraucherinnen und Verbraucher und Unternehmen ein stärkeres Bewusstsein für einen sicheren Umgang mit dem Internet entwickeln. Auch die Landesregierung sensibilisiert die Bürger über verschiedene Kanäle wie u.a. dem VerbraucherFenster für ein bewusstes Surfverhalten.

Frage 200. Inwiefern hat die Landesregierung datenschutzrechtliche Bedenken hinsichtlich der automatischen Analyse von Zugriffen auf Webseiten?

Eine automatische Analyse von Zugriffen auf Webseiten ist im Rahmen des Telemediengesetzes abschließend geregelt. Im Wesentlichen ist danach eine automatische Analyse datenschutzrechtlich zulässig, wenn sie zu Abrechnungszwecken erfolgt. Zwar ist die Erhebung von Nutzungsdaten auch für andere Zwecke wie der Werbung oder der Marktforschung unter einem Widerspruchsvorbehalt des von der Datenerhebung Betroffenen erlaubt. Jedoch sind für die Erstellung der Nutzungsprofile in diesen Fällen Pseudonyme zu verwenden. Ferner hat der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

Verstößt der Diensteanbieter bei der automatischen Analyse von Zugriffen auf Webseiten gegen diese Maßstäbe, indem er etwa Daten seiner Nutzerinnen und Nutzer nicht (nur) zu Abrechnungszwecken erhebt oder ein Nutzungsprofil mit Daten über den Träger des Pseudonyms zusammenführt, so handelt er ordnungswidrig. Die Ordnungswidrigkeit kann in diesen Fällen mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden. Zuständig für die Verfolgung und Ahndung dieser Ordnungswidrigkeiten ist der Hessische Datenschutzbeauftragte.

Der beschriebene datenschutzrechtliche Standard kann jedoch dann nicht gewährleistet werden, wenn der Diensteanbieter seinen Sitz außerhalb der EU hat. Auch insofern begrüßt die Landesregierung das Vorhaben einer Datenschutz-Grundverordnung, mit der auch die datenschutzrechtliche Verantwortung von solchen Unternehmen, die ihren Sitz außerhalb der EU haben, verwirklicht wird.

Laut dem Hessischen Datenschutzbeauftragten gibt es auch die Möglichkeit, Zugriffe von Nutzern über die Grenzen eines Angebots hinaus zu analysieren. Für dieses Tracking kommen neben Cookies auch weitere Techniken wie Flash-Cookies, LSO (Local Shared Object) oder HTML5 Client Side Storage zum Einsatz. Bei anbieterübergreifenden Analysen können detaillierte Surfprofile gebildet werden, aus denen sich Aussagen über Verhalten und Interessen gewinnen lassen. Sobald diese Informationen einer bestimmten Person zugeordnet werden können, bedarf es laut dem Hessischen Datenschutzbeauftragten regelmäßig der Einwilligung des Nutzers.

Frage 201. Falls datenschutzrechtliche Bedenken bestehen, welche Möglichkeiten sieht die Landesregierung, diese auszuräumen?

Bei Beurteilung der datenschutzrechtlichen Zulässigkeit einer automatischen Nutzeranalyse durch Diensteanbieter auf Webseiten sind insbesondere die Vorschriften des TMG zu berücksichtigen.

sichtigen, z.B. die in § 15 TMG geregelten Vorgaben zur Erhebung, Verwendung und Zusammenführung von Nutzungsdaten.

Auf die Antwort zur Frage 200 wird verwiesen.

Es wird auch auf den Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 8. Dezember 2011) zum Thema "Datenschutz in sozialen Netzwerken" verwiesen.

([https://www.ldi.nrw.de/mainmenu\\_Service/submenu\\_Entschliessungsarchiv/Inhalt/Beschluesse\\_Duesseldorfer\\_Kreis/Inhalt/2011/index.php](https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2011/index.php))

Frage 202. Hält die Landesregierung die von verschiedenen Anbietern bereitgestellten Opt-out Browser-Add-ons für ausreichend, um datenschutzrechtlichen Bedenken hinsichtlich der Analyse von Zugriffen auf Webseiten zu begegnen?

Mithilfe von Opt-out-Browser-Add-ons können Verbraucherinnen und Verbraucher eine unberechtigte bzw. unerwünschte Analyse ihres Surfverhaltens verhindern. Die technisch einwandfreie Einrichtung solcher Programme wird jedoch von der Verbraucherin/dem Verbraucher nicht zu erwarten sein. Deshalb setzt sich die Landesregierung dafür ein, dass die datenschutzrechtliche Verantwortung bei dem Diensteanbieter verbleibt. Ein effektiver Schutz vor unberechtigter bzw. ungewollter Analyse des Surfverhaltens kann nur erreicht werden, wenn das mit den Voraussetzungen des Telemediengesetzes erzielte Schutzniveau auch auf europäischer Ebene verwirklicht ist und hierbei ebenso Diensteanbieter mit Sitz außerhalb der EU verpflichtet werden. Auch insoweit wird das Vorhaben einer Datenschutz-Grundverordnung von der Landesregierung befürwortet.

Frage 203. Ist die aktuelle Gesetzgebung aus Sicht der Landesregierung ausreichend, um im Bereich mobile Werbung und mobiles Profiling (hauptsächlich durch Apps auf Smartphones) den Datenschutz der Verbraucherinnen und Verbraucher in ausreichendem Maß zu gewährleisten?

Die Bestimmungen des Telemediengesetzes bieten den Nutzerinnen und Nutzern im Hinblick auf mobile Werbung und mobiles Profiling ein hohes Schutzniveau. Die Landesregierung strebt jedoch eine weitere Erhöhung dieses Schutzniveaus an.

Nach der aktuellen Gesetzeslage dürfen Diensteanbieter für Zwecke der (mobilen) Werbung Nutzungsprofile unter der Verwendung von Pseudonymen erstellen, sofern die Verbraucherinnen und Verbraucher dem nicht widersprechen. Mobiles Profiling ist darüber hinaus nur bei einer vorherigen Einwilligung des Betroffenen zulässig. Die Landesregierung berücksichtigt jedoch auch die sich gerade im Bereich der Nutzung von mobilen Endgeräten stetig ergebenden Änderungen technischer und tatsächlicher Art. Sie vertritt daher die Auffassung, dass ein effektiver Schutz vor unerwünschter mobiler Werbung bzw. unerwünschtem mobilen Profiling nur über eine verbraucherfreundliche Gestaltung der Nutzungs- und Datenschutzbedingungen sichergestellt werden kann. Zu denken ist in diesem Zusammenhang außerdem an eine Regelung, nach der eine Analyse des Surfverhaltens grundsätzlich nur nach einer einzelfallbezogenen Einwilligung zulässig ist. Ferner sollen die Diensteanbieter zu datenschutzfreundlichen Grundeinstellungen ("privacy by default") sowie zu einer dem jeweils höchstmöglichen Sicherheitsstandard entsprechenden Technik ("privacy by design") verpflichtet werden.

Auf die Antwort zur Frage 196 wird verwiesen.

Frage 204. Sind aus Sicht der Landesregierung in diesem Bereich eher freiwillige Vereinbarungen mit den Anbietern von Internetdienstleistungen oder gesetzliche Regulierungen zielführend, um Abhilfe zu schaffen?

(Freiwillige) Selbstverpflichtungen der Diensteanbieter sind aus Sicht der Landesregierung zu begrüßen. Die Landesregierung geht jedoch von der grundsätzlichen Notwendigkeit einer gesetzlichen Regulierung aus. Ein effektiver wie ebenso nachhaltiger Schutz der Verbraucherinnen und Verbraucher vor einer unerwünschten Analyse ihres Surfverhaltens wird nur durch verbindliche Vorgaben zu erreichen sein, die von den Aufsichtsbehörden kontrolliert und bei Verstößen sanktioniert werden können. Für die Landesregierung ist es daher erstrebenswert, sich im Rahmen ihrer Tätigkeit bei der EU-Datenschutzreform für einen Einwilligungsvorbehalt bei der Analyse der Webaktivitäten von Verbraucherinnen und Verbrauchern einzusetzen. Hierbei müssen insbesondere auch in den jeweiligen Mitgliedstaaten agierende Diensteanbieter mit Sitz außerhalb der EU mit in den Regelungsgehalt einbezogen werden.

Generell sollte ein Schutzniveau, das nicht unterschritten werden darf, möglichst in verbindlichen gesetzlichen Vorgaben geregelt werden. Ansonsten fehlt der rechtliche Orientierungsmaßstab, der eine Einhaltung der Verbraucherrechte gewährleistet.

## "Recht auf Vergessenwerden"

Frage 205. Wie beurteilt die Landesregierung die Vor- und Nachteile eines "Rechts auf Vergessenwerden"?

Die Vorteile des Internets liegen auf der Hand: Nutzer sparen Zeit, Aufwand und Kosten. Die Schattenseite dieser Entwicklung: Jeder hinterlässt Spuren im Netz. Jede Äußerung im Internet wird potenziell weltweit öffentlich, was in Internetforen steht, ist öffentlicher als das, was in der Schule am Schwarzen Brett hängt, Konsumprofile für die Werbung führen zur "gläsernen Verbraucherin" oder zum "gläsernen Verbraucher" und auch Mobbing-Attacken durch virtuelle Netzwerke steigen ständig an. Das Internet "vergisst nichts". Dies sollten sich Nutzer bewusst machen, denn solche Nutzerkonten sind dann für alle Zeiten im Internet, selbst wenn sie jahrelang nicht mehr aktiv genutzt worden sind. Eine Löschung des einmal angelegten Nutzerkontos und der darin enthaltenen persönlichen Daten bieten die Diensteanbieter oftmals nicht an, ebenso wenig eine Löschung bzw. Anonymisierung weiterer Daten, die gegebenenfalls mit dem Nutzerkonto in Verbindung stehen.

Das aktuelle Urteil des Europäischen Gerichtshofs, den Suchmaschinenbetreiber Google dazu zu verpflichten, Verweise auf Webseiten mit sensiblen persönlichen Daten aus seiner Ergebnisliste zu streichen, zeigt den Handlungsbedarf in diesem Bereich: Dienste-Anbieter sollten künftig verpflichtet werden, eine deutlich erkennbare Löschfunktion bereit zu halten, die es dem Nutzer ermöglicht, die Löschung seines Nutzerkontos jederzeit selbst zu veranlassen und das Verfallsdatum seiner Daten selbst zu bestimmen. Das Gericht weist darauf hin, dass bereits die Ergebnislisten bei Suchanfragen im Internet erhebliche Eingriffe in die Persönlichkeitsrechte einer Person darstellen können. Ergebnislisten liefern einen strukturierten Überblick über alle zu einer Person im Internet verfügbaren Informationen, die ohne die betreffende Suchmaschine nicht oder nur sehr schwer hätten miteinander verknüpft werden können.

Frage 206. Wie beurteilt die Landesregierung die technische Realisierbarkeit eines solchen Rechts?

Frage 207. Wie beurteilt die Landesregierung die Möglichkeit der Durchsetzung eines "Rechts auf Vergessenwerden"?

Frage 208. Plant oder realisiert die Landesregierung Maßnahmen, um die weitere technische und rechtliche Ausgestaltung eines "Rechts auf Vergessenwerden" zu unterstützen?  
Falls die Frage bejaht wird: Bitte Maßnahmen nennen und erläutern.

Die Fragen 206, 207 und 208 werden gemeinsam beantwortet.

Die Datenschutzgesetze des Bundes und des Landes verpflichten derzeit zuvorderst öffentliche Stellen und nicht-öffentliche Stellen, soweit sie Aufgaben öffentlicher Stellen erfüllen, zur Einhaltung der Datenschutzprinzipien. Personenbezogene Daten sind von diesen Stellen zu löschen, wenn der Betroffene seine Einwilligung zur Erhebung und Verarbeitung zurückzieht, die Daten nicht mehr gebraucht werden oder spätestens definierte Aufbewahrungsfristen abgelaufen sind. Seitens der öffentlichen und den ihnen gleichgestellten Stellen ist damit schon jetzt ein Recht auf Vergessenwerden verwirklicht. Jedoch besteht auf Landes-, Bundes- und Europaebene kein allgemein verbindliches Recht auf Vergessenwerden. Die Vorschriften der Datenschutzrichtlinie genügen nicht den Anforderungen an das inzwischen erreichte Maß technisch möglicher Datenerhebung und Datenverarbeitung einerseits sowie der steigenden Sozialadäquanz von Veröffentlichungen privater Daten andererseits. Ein explizites Recht auf Vergessenwerden sieht diese Richtlinie nicht vor. Die Landesregierung erachtet es als erforderlich, dass insbesondere auch von privatrechtlich agierenden Internetdiensteanbietern die Datenschutzprinzipien der Datensparsamkeit und Datenvermeidung im Vorfeld der Datenerhebung sowie die Löschung von Daten nach ihrer Erhebung beachtet werden. Ein Recht auf Vergessenwerden muss als Ausfluss des informationellen Selbstbestimmungsrechts des Einzelnen verstanden werden. Für einen effektiven Schutz dieses Grundrechts ist es zwingend erforderlich, dem Einzelnen ein bisher fehlendes einklagbares und damit auch durchsetzbares Recht auf Vergessenwerden zuzusprechen - der Rahmen dieses Rechts wird unter Berücksichtigung der neuesten EuGH-Rechtsprechung (Urteil vom 13.05.2014, Az.: C-131/12) zu bestimmen sein. Die Landesregierung begrüßt das Vorhaben einer verbindlichen Europäischen Datenschutz-Grundverordnung, welche auch einen erweiterten Löschungsanspruch enthält. Der Betroffene soll nicht nur vom datenverarbeitenden Diensteanbieter verlangen können, dass sämtliche bei diesem über ihn vorhandenen Daten gelöscht und nicht weiter verarbeitet werden. Wenn der Datenverarbeiter unterdessen die persönlichen Daten an Dritte weitergegeben oder im Internet veröffentlicht hat, soll der Betroffene zudem beanspruchen können, dass der Datenverarbeiter alle vertretbaren Schritte unternimmt, um sämtliche Personen, die diese Daten verarbeiten, darüber zu informieren, dass die Daten samt aller Querverweise und Kopien zu löschen sind. Das Recht auf Vergessenwerden kann nach dem heutigen Stand der Technik jedoch nur ansatzweise umgesetzt werden. Bei Daten, die zu einem Zeitpunkt mit Wissen und Einwilligung der betroffenen Person öffentlich angeboten wurden, ist es praktisch unmöglich, die Weiterverwertung durch andere Dienste nachzuverfolgen und so zu einer vollständigen Löschung aller (legitim erzeugten) digitalen Kopien zu gelangen. Auch die Löschung der Daten in ausgelagerten Datensicherungen stellt Diensteanbieter vor gro-

ße technische Herausforderungen und würde immense Kosten verursachen. Aktuelle Ansätze beschränken sich deshalb in der Regel darauf, die öffentliche Auffindbarkeit der Daten zu verhindern. Die Schwierigkeiten selbst bei diesem eingeschränkten Ansatz werden in der Reaktion der Firma Google auf das angesprochene EuGH-Urteil deutlich. Die vom Betroffenen beantragte Löschung von Fundstellen wird von Google nur durch eine Unterdrückung der tatsächlichen Suchergebnisse in der Anzeige für Suchanfragen aus Europa umgesetzt. Suchanfragen außerhalb Europas erhalten weiterhin die vollständigen Suchergebnisse, und damit auch die "gelöschten Verweise" angezeigt. Die Durchsetzung des Rechts gegenüber jedem einzelnen Diensteanbieter wird den individuellen Nutzer regelmäßig überfordern.

Die Landesregierung stellt Internetnutzerinnen und -nutzern über das Internetangebot VerbraucherFenster Informationen zum Recht auf Vergessenwerden bereit.

### **Personensuchmaschinen**

Frage 209. Wie steht die Landesregierung speziell zu Personensuchmaschinen, die Daten von Menschen aggregieren und diese für alle im Internet frei zugänglich machen?

Frage 210. Wie beurteilt die Landesregierung das sog. "eReputation-Management", das durch Personensuchmaschinen ermöglicht werden soll?

Frage 211. Sind Maßnahmen seitens der Landesregierung geplant, um das Sammeln und Bereitstellen von Daten über Internetnutzerinnen und -nutzer durch Suchmaschinen aus verschiedenen, mitunter auch nicht öffentlichen Quellen, zu regulieren?

Die Fragen 209 bis 211 werden zusammen beantwortet.

Die Aggregation frei im Internet verfügbarer Informationen durch hochspezialisierte Suchmaschinen ist der Kern zahlreicher Dienstleistungen im Internet. Die so bereitgestellten Ergebnisse werden sowohl in der Kreditwirtschaft als auch bei der Personalgewinnung sowie im Marketing vielfältig genutzt. Die Landesregierung empfiehlt den Nutzerinnen und Nutzern, das durch diese Anbieter erzeugte Bild ihrer Person aktiv zu überwachen, um bei fehlerhaften oder unrechtmäßigen Darstellungen gezielt eingreifen zu können. Das reicht je nach individuellem Bedürfnis von gelegentlichem "Googlen" des eigenen Namens über die regelmäßige Kontrolle der wichtigsten Personensuchmaschinen bis hin zur Inanspruchnahme von e-Reputation-Diensten, die die dafür notwendigen Einzelschritte gegen Entgelt abwickeln und konsolidierte Berichte erstellen.

Die Landesregierung wird hier die weiteren Entwicklungen beobachten und auf dieser Grundlage den Bedarf an weiteren Aufklärungsmaßnahmen sowie den Regelungsbedarf analysieren. Problematisch könnte aus Verbrauchersicht hierbei sein, dass für den Nutzer oder die Nutzerin nicht auf den ersten Blick erkennbar ist, dass sein oder ihr Verhalten als Einwilligung gedeutet werden könnte. Das Auffinden durch externe Suchmaschinen sollte erst dann möglich sein, wenn der Nutzer hierin ausdrücklich, z.B. durch das freiwillige und bewusste Setzen eines Häkchens, einwilligt.

### **DeMail**

Frage 212. Wie bewertet die Landesregierung grundsätzlich die Bestrebungen, eine rechtsverbindliche E-Mail-Kommunikation zu ermöglichen?

Die Landesregierung begrüßt eine rechtsverbindliche E-Mail-Kommunikation. Mit De-Mail können elektronische Nachrichten verschickt werden, bei denen die Identität der Kommunikationspartner sowie der Versand und der Eingang von De-Mails zweifelsfrei nachgewiesen werden können. Die Inhalte einer De-Mail werden auf ihrem Weg durch das Internet transportverschlüsselt und können nicht mitgelesen oder verändert werden. De-Mail erhöht so die Sicherheit der elektronischen Kommunikation im Vergleich zur herkömmlichen E-Mail und hilft, unerwünschte und gefälschte Mails (wie Spam und Phishing), mit denen u.a. Zugangsdaten ausgepäht werden können, zu vermeiden. Vor dem Hintergrund der berechtigten Erwartungen der Bürgerinnen und Bürger an eine zeitgemäße Verwaltung sind Bestrebungen in diesem Zusammenhang alternativlos und tragen zu mehr Bürger- und Wirtschaftsfreundlichkeit bei.

Frage 213. Welche konkreten Initiativen, die diesem Ziel dienen sollen, unterstützt oder unternimmt die Landesregierung?

Nachdem sich die Landesregierung auf Bundesebene in das Gesetzgebungsverfahren unterstützend eingebracht hat, wurden mit dem Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften vom 25. Juli 2013 (BGBl. I S. 2749) zusätzliche Möglichkeiten geschaffen, mit Behörden über E-Mail rechtsverbindlich in Kontakt zu treten. Art. 1 des Gesetzes enthält das E-Government-Gesetz (EGovG), das für die Behörden des Bundes einschließlich der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie für die Behörden der Länder, der Gemeinden und Gemeindeverbände und sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts,

wenn sie Bundesrecht ausführen, gilt. Die Behörden des Landes setzen die Vorgaben des Gesetzes um, die nicht auf Bundesbehörden beschränkt sind. Eine dieser für alle Behörden geltenden Vorgaben ist, dass nach § 2 Abs. 1 EGovG jede Behörde verpflichtet ist, den elektronischen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifizierten elektronischen Signatur versehen sind, zu eröffnen. Durch Art. 3 des Gesetzes ist das Verwaltungsverfahrensgesetz des Bundes (VwVfG) geändert worden. Maßgeblicher Inhalt der Änderung ist, dass in einem neuen Satz 4 des § 3a Abs. 2 VwVfG Regelungen geschaffen wurden, die es zulassen, das Schriftformerfordernis neben einem elektronischen Dokument mit einer qualifizierten elektronischen Signatur (§ 3a Abs. 2 Satz 2 VwVfG) durch andere technische Verfahren als die qualifizierte elektronische Signatur zu ersetzen. Die Gründe, die im Verwaltungsverfahrensgesetz des Bundes zur Zulassung weiterer technischer Verfahren zur Ersetzung der Schriftform geführt haben, gelten auch für Hessen. Ebenso wie seinerzeit im Bund besteht in Hessen ein wesentliches Hindernis für e-Government-Angebote der öffentlichen Verwaltung darin, dass als elektronisches Äquivalent der Schriftform allein die qualifizierte elektronische Signatur zugelassen ist. Die Vielzahl der verwaltungsrechtlichen Schriftformerfordernisse und die Tatsache, dass diese in der elektronischen Welt - zwar nicht mehr im Bund, aber noch in Hessen - allein durch die sehr wenig verbreitete qualifizierte elektronische Signatur ersetzt werden kann, führt dazu, dass in schriftformbedürftigen Verwaltungsverfahren letztlich keine ausreichend praktikable Alternative zur Papierform für die Unternehmen, Bürgerinnen und Bürger und für die Verwaltung existiert. Daher ist es sinnvoll, so wie im Bund auch in Hessen weitere sichere technische Verfahren zur elektronischen Ersetzung der Schriftform zuzulassen. Eine unterschiedliche Rechtslage wäre für die Unternehmen und für die Bürgerinnen und Bürger, die mit der Verwaltung rechtsverbindlich kommunizieren wollen, nicht vermittelbar. Für sie ist es nicht nachvollziehbar, dass bei Verwaltungsverfahren, die sich nach Bundesrecht richten, weitere Möglichkeiten zur Ersetzung der Schriftform zur Verfügung stehen, nicht aber bei Verwaltungsverfahren, die nach dem Hessischen Verwaltungsverfahrensgesetz durchzuführen sind. Eine einheitliche Rechtslage ist daher auf allen und für alle Verwaltungsebenen geboten. Sie dient den Zielen des IT-Staatsvertrages (Gesetz zum Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern - Vertrag zur Ausführung von Artikel 91c GG vom 27. Mai 2010, BGBl. I, S. 662), nach denen aufgrund der wachsenden Herausforderungen als Folge der Entwicklungen in der Informationstechnik der reibungslose und sichere Betrieb informationstechnischer Systeme für geordnete Abläufe in den Verwaltungen nur durch eine gemeinsame Strategie des Bundes und der Länder - hier in Gestalt der Simultangesetzgebung - aufrechterhalten werden kann (vgl. BT-Drucks. 17/427).

Gegenwärtig liegt ein Referentenentwurf des Ministeriums des Innern und für Sport zur Änderung des Hessischen Verwaltungsverfahrensgesetzes und anderer Vorschriften vor. In diesem wird eine Änderung des § 3a Abs. 2 des Hessischen Verwaltungsverfahrensgesetzes (HVwVfG), so wie in § 3a Abs. 2 VwVfG des Bundes bereits geregelt, vorgeschlagen (wortgleiche Übernahme). Die im VwVfG des Bundes neben einem elektronischen Dokument mit einer qualifizierten elektronischen Signatur (§ 3a Abs. 2 Satz 2 VwVfG) in § 3a Abs. 2 Satz 4 VwVfG zugelassenen anderen technischen Verfahren zur elektronischen Ersetzung der Schriftform sind folgende: Das erste Verfahren regelt die unmittelbare Abgabe einer Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird (§ 3a Abs. 2 Satz 4 Nr. 1 VwVfG). Bei einer Eingabe über öffentlich zugängliche Netze ist ein sicherer elektronischer Identitätsnachweis durch die eID-Funktion des neuen Personalausweises nach § 18 des Personalausweisgesetzes oder des elektronischen Aufenthaltstitels nach § 78 Abs. 5 des Aufenthaltsgesetzes zu erbringen. Das zweite dieser Verfahren ist die De-Mail in Ausgestaltung der Versandart nach § 5 Abs. 5 des De-Mail-Gesetzes (§ 3a Abs. 2 Satz 4 Nr. 2 und 3 VwVfG). Der Sender der Nachricht ist dabei durch ein sicheres Anmeldeverfahren identifiziert, die Nachricht einschließlich aller Metadaten durch eine vom De-Mail-Provider aufgebrachte dauerhafte qualifizierte elektronische Signatur (des De-Mail-Providers) gegen Veränderungen geschützt. Die dritte Möglichkeit ist, dass durch Rechtsverordnung auch andere sichere Verfahren zugelassen werden können (§ 3a Abs. 2 Satz 4 Nr. 4 VwVfG). Die Zulassung anderer sicherer Verfahren ist im Vorfeld zwischen Bund und Ländern im IT-Planungsrat (§ 10 EGovG) abzustimmen.

Frage 214. Wie bewertet die Landesregierung die bisherigen Regelungen zur DeMail?

Frage 215. Welche Anforderungen hinsichtlich der Datensicherheit hat die Landesregierung an ein rechtsverbindliches Mailsystem?

Frage 216. Welchen Stellenwert hinsichtlich der Datensicherheit nimmt aus Sicht der Landesregierung eine verbindliche Ende-zu-Ende-Verschlüsselung im Rahmen eines rechtsverbindlichen Mailsystems ein?

Frage 217. Welche konkreten Anforderungen zur Sicherung der Rechtsverbindlichkeit (bspw. hinsichtlich der Zugangsfiktion) hat die Landesregierung an ein rechtsverbindliches Mailsystem?

Die Fragen 214 bis 217 werden zusammen beantwortet.

Das Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften vom 28. April 2011 (BGBl. I S. 666, im Folgenden: De-Mail-Gesetz) setzt Vorgaben der europäischen Dienstleistungsrichtlinie um. Es trägt im Bereich der E-Mail-Kommunikation zu mehr Integrität und Authentizität bei. Zum einen garantiert das Zertifizierungsverfahren die Zuverlässigkeit der De-Mail-Diensteanbieter. Zum anderen führt der De-Mail-Standard im Bereich der E-Mail-Kommunikation aus datenschutzrechtlicher Sicht zu einer Erhöhung des Schutzniveaus, da Signatur- und Verschlüsselungstechniken verbindlich festgelegt werden. Für den Bereich der rechtsverbindlichen E-Mail-Kommunikation gewährleistet das De-Mail-Gesetz damit aus Sicht der Landesregierung einen hinreichenden Sicherheitsstandard. Denn in technischer Hinsicht unterscheidet sich eine De-Mail von der Versendung herkömmlicher E-Mails durch eine Transportverschlüsselung entsprechend der vom Bundesamt für Sicherheit in der Informationstechnik für den Bereich der De-Mail festgelegten Technischen Richtlinie. Zwar zwingt das De-Mail-Gesetz nicht zu einer sog. Ende-zu-Ende-Verschlüsselung, sondern ermöglicht den De-Mail-Diensteanbietern zu Zwecken der Überprüfung von Schadsoftware eine automatisierte Entschlüsselung der E-Mail. Nach der Überprüfung wird die De-Mail wieder transportverschlüsselt und dann verschlüsselt beim Provider abgespeichert. Die Landesregierung kann sich jedoch auch eine weitere Erhöhung dieses Standards durch eine Pflicht zu einer sog. Ende-zu-Ende-Verschlüsselung vorstellen. Bereits im Gesetzgebungsverfahren zum De-Mail-Gesetz drängten die Länder auf eine Ende-zu-Ende-Verschlüsselung (vgl. BT-Drucks. 17/4145), die indes nicht durchgesetzt werden konnte. Hintergrund war, dass einerseits bei einer Ende-zu-Ende-Verschlüsselung eine automatisierte Überprüfung auf Schadsoftware nach dem Stand der Technik unmöglich gewesen wäre; andererseits befürchtete die Bundesregierung, dass eine Ende-zu-Ende-Verschlüsselung das Ziel einer einfachen und ohne spezielle Softwareinstallation möglichen Nutzbarkeit durch die Bürgerinnen und Bürger gefährden würde (vgl. BT-Drucks. 17/4145). Diese Besorgnis teilte auch der Bundestag und beschloss das Gesetz ohne das Erfordernis einer Ende-zu-Ende-Verschlüsselung (vgl. BT-Drucks. 17/4893), wobei er hervorhob, dass eine Ende-zu-Ende-Verschlüsselung weiterhin optional gewählt werden könne. Nachdem der Bundesrat im Gesetzgebungsverfahren zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften das Problem einer pflichtigen Ende-zu-Ende-Verschlüsselung nicht mehr aufgegriffen und im Rahmen von § 3a Abs. 2 Satz 4 Nr. 2 und 3 VwVfG nicht zur Bedingung gemacht hat (vgl. BT-Drucks. 17/11473), ist davon auszugehen, dass auch im Rahmen der Simultangesetzgebung eine Ende-zu-Ende-Verschlüsselung im Hinblick auf eine rechtsverbindliche Kommunikation mit und von den Behörden nicht notwendigerweise Einzug in das Hessische Verwaltungsverfahrensgesetz finden muss. Der Landesregierung ist überdies bekannt, dass bereits einige Länder die gleichen Regelungen in ihr Verwaltungsverfahrensgesetz übernommen haben bzw. andere Länder eine entsprechend wortgleiche Übernahme des § 3a Abs. 2 Satz 4 Nr. 2 und 3 VwVfG in ihr Verwaltungsrecht beabsichtigen. Für die Bürgerinnen und Bürger und für die Verwaltung besteht nach § 3a Abs. 2 Satz 4 Nr. 2 und 3 VwVfG keine Verpflichtung, elektronische Dokumente mit einer De-Mail zu versenden. Die Verwaltung hat hierüber nach pflichtgemäßem Ermessen zu entscheiden, so dass bei besonders sensiblen Daten, wie beispielsweise bei Gesundheitsdaten, die Ermessensentscheidung dazu führen müsste, die Versandart einer De-Mail nicht zu wählen oder aber eine Ende-zu-Ende-Verschlüsselung mit einer hierfür erforderlichen Mail-Software vorzunehmen. Letzteres setzt voraus, dass auch der Empfänger eine entsprechende Kryptografiesoftware besitzt.

Nach dem Hessischen Verwaltungszustellungsgesetz, das auf das Verwaltungszustellungsgesetz des Bundes verweist, können Zustellungen per De-Mail nur dann wirksam vorgenommen werden, wenn der Empfänger hierfür einen Zugang eröffnet hat. Die De-Mail gilt erst dann als zugestellt, wenn sich der Bürger an seinem Postfach beim Diensteanbieter anmeldet (vgl. BT-Drucks. 17/4893).

### **Maßnahmen in Schulen und Bildungsinstitutionen**

Frage 218. Welchen Stellenwert misst die Landesregierung der Förderung des Verbraucherschutzes im Bereich Medien- bzw. Datenschutzkompetenz insgesamt bei?

Alle hessischen Schulen vermitteln "Medienerziehung" als Teil von Medienbildung im Unterricht und im Rahmen des Schullebens. Darüber hinaus setzen einzelne Schulen in Abhängigkeit vom Schulprofil individuelle Schwerpunkte für Medienbildung.

In ihrer Unterrichtsentwicklung werden die Schulen dabei durch die Fachberater/-innen Medienbildung an den Staatlichen Schulämtern (SSÄ), durch externe Medienpädagogen, die mit dem Kultusministerium und dem Hessischen Rundfunk kooperieren sowie durch Schulprojekte mit Modellcharakter unterstützt.

Im Rahmen der Medieninitiative "Schule@Zukunft" unterstützt das Land Hessen gemeinsam mit den kommunalen Schulträgern die Schulen durch eine moderne IT-Ausstattung, durch Lehrerfortbildungen und durch Onlinedienste, um Medienerziehung für alle Schülerinnen und Schüler sicherstellen zu können.

Durch eine umfassende finanzielle Unterstützung über die Medieninitiative Schule@Zukunft sowie personelle Ressourcen im Bereich Fachberatung Medienbildung an den SSÄ und landesweiten Projektmaßnahmen sowie die Unterstützungsleistungen des Sachgebiets Medienbildung im LSA wird eine Vielzahl von Projekten und Fortbildungsmaßnahmen umgesetzt, die die Vermittlung von Medienkompetenz an Schülerinnen und Schüler und an Lehrkräfte sowie den Einsatz neuer Medien im Unterricht fördert. Auch die Medienzentren bieten regionale Fortbildungsangebote für Lehrkräfte rund um das Thema Medienbildung an.

Frage 219. Welche Herausforderungen für die Verbesserung der Förderung der Medien- und Datenschutzkompetenz, insbesondere für Kinder und Jugendliche, sieht die Landesregierung?

Die schulische Medienbildung sollte die Umsetzung einer angemessenen und umfassenden Vermittlung von Medienkompetenz im Unterricht und im Schulleben gewährleisten. Über die bestehenden Maßnahmen zur Medienkompetenzvermittlung hinaus, die regelmäßig hinsichtlich ihrer Aktualität anzupassen sind, ist das Ziel die Entwicklung und Implementierung eines Mediencurriculums als Orientierungshilfe für die Schulen.

Frage 220. Wie ist die Förderung der Medien-, Informations- und Datenschutzkompetenz derzeit in den Lehrplänen verankert?

In Hessen gilt der Grundsatz, der nachwachsenden Generation in der Schule den Zugang zu einer handlungsorientierten Medienbildung zu ermöglichen, damit sie sich Chancen und Risiken der Medien- und Informationsgesellschaft erschließen kann. Im § 6 Absatz 4 des Hessischen Schulgesetzes wird Medienerziehung als fachübergreifende Bildungs- und Erziehungsaufgabe aufgeführt, die in Aufgabengebieten erfasst wird. Aufgabengebiete werden fachübergreifend unterrichtet. Sie können in Form themenbezogener Projekte unter Berücksichtigung der fachbezogenen Lernziele und Methoden auch jahrgangs- und schulformübergreifend unterrichtet werden. Über die inhaltliche und unterrichtsorganisatorische Umsetzung entscheidet die Gesamtkonferenz auf der Grundlage einer Konzeption der jeweils zuständigen Konferenz der Lehrkräfte.

Medienbildung bündelt medienerzieherische, medienpädagogische, medienkundliche und informatorische Anteile und umfasst damit auch die Vermittlung von Datenschutzkompetenz.

In den Lehrplänen und Bildungsstandards ist die Vermittlung von Medienkompetenz als überfachliche Kompetenz dahin gehend verankert, dass neben der gestalterisch und technisch sachgerechten Anwendung von Medien zur Information und Präsentation von Lerninhalten eine kritisch-reflektierte Mediennutzung die Voraussetzung dafür schaffen soll, um in der heutigen Informations- und Mediengesellschaft kompetent und verantwortungsvoll zu handeln.

Frage 221. Wie ist die Förderung der Medien-, Informations- und Datenschutzkompetenz derzeit in der Lehrerbildung und -fortbildung verankert?

In der Vermittlung von Kompetenzen zur didaktisch fundierten Nutzung digitaler Medien in Schule und Unterricht und zum kritisch-reflektierten Umgang mit diesen Medien wird eine wesentliche Aufgabe zukunftsorientierter Lehrerbildung gesehen. Damit der Erwerb von Medienkompetenz und Medienbildungskompetenz phasenübergreifend in der Lehrerbildung sichergestellt werden kann, erhalten Lehrkräfte in allen drei Ausbildungsphasen Angebote zur Förderung ihrer Medienkompetenz sowie ihrer Medienbildungskompetenz. Im Bereich der ersten Ausbildungsphase bestehen dafür auf Ebene des Landesschulamtes mit allen hessischen Universitäten Kooperationen. Im Rahmen einer Steuergruppe aus Mitgliedern des Hessischen Kultusministeriums, des LSA und Vertretern der Universitäten findet ein regelmäßiger Austausch über die universitären Projekte und Maßnahmen sowie deren Weiterentwicklung statt.

In der zweiten Ausbildungsphase ist die Vermittlung von Medienbildungskompetenz als Bestandteil der fachdidaktischen Module verankert. Darüber hinaus werden Fortbildungen im Bereich der Studienseminare im Rahmen des Projekts "Medien und Module" angeboten, die eine Unterstützung für Ausbilderinnen und Ausbilder bei der Umsetzung der fachdidaktischen Module umfassen.

Im Rahmen der Lehrerfortbildung bietet das LSA eine Vielzahl von Fortbildungsangeboten für Lehrkräfte im Bereich der Medienbildung an, die unter anderem Fragen des sicheren Umgangs mit dem Internet und den Datenschutz umfassen.

Um die in den verschiedenen Aus- und Fortbildungskontexten in den einzelnen Phasen der Lehrerbildung erworbenen Kenntnisse und Fähigkeiten der Medienkompetenz und der Medienbildungskompetenz nachvollziehbar abbilden zu können, befindet sich derzeit ein Portfolio Medienbildungskompetenz für Lehrkräfte in der Umsetzung.

An der Technischen Universität Darmstadt werden Medienkompetenz, Informationskompetenz und Datenschutz umfassend im Modul Informationspädagogik der Grundwissenschaften themati-

siert. Dieses Modul ist ein Wahlpflichtmodul, d.h. die Studierenden können es wählen, könnten aber auch Alternativmodule belegen. Erfahrungsgemäß wird dieses Modul aber von sehr vielen Lehramtsstudierenden belegt. Medienkompetenz und Informationskompetenz werden darüber hinaus in geringerem Umfang in der Vorlesung "Pädagogik der Neuen Medien" im Pflichtmodul "Didaktik, Methodik, Medien" thematisiert. Allerdings spielen die Themen naturgemäß in der allgemeinbildenden und berufsbildenden Lehrerbildung Informatik eine große Rolle. In Zusammenarbeit mit der Hessischen Film- und Medienakademie lernen Lehramtsstudierende zusammen mit Schülerinnen und Schülern anhand filmischer Arbeit didaktische Konzepte mit Medien wie Film umzusetzen. In den integrierten Veranstaltungen Fachdidaktik 1 und Fachdidaktik 2 werden Datenschutz und Datensicherheit didaktisch aufbereitet und unter verschiedenen Gesichtspunkten analysiert. Im Zentrum stehen jeweils aus Schülerinnen- und Schülersicht insbesondere die Anleitung zum kritischen Vernunftgebrauch, die Entfaltung von Verantwortungsbereitschaft und vor allem die Stärkung des Schüler-Ich in allen Fragen der Medien- und Informationskompetenz sowie des Datenschutzes.

Die Fragen stellen auch für die Lehrerfort- und -weiterbildung eine zentrale Rolle, die im Rahmen des Projektes "Abenteuer Technik" des Fachbereichs Informatik nicht nur für Lehrerinnen und Lehrer mit Informatik als Fach, sondern offen für alle Fächer und Schulformen durchgeführt wird. Neben den anderen Beiträgen ist dies ein ganz wesentlicher Aspekt, der die Notwendigkeit allgemeinbildenden Informatikunterrichts an Schulen unterstreicht.

An der Goethe-Universität Frankfurt am Main wird seit dem Jahr 2005 das Medienkompetenzzertifikat für Lehramtsstudierende angeboten. Das Medienkompetenzzertifikat ist als ein 11 Credits umfassendes teilintegriertes Studienprogramm umgesetzt, das sich an Studierende aller Lehrämter und Fächer richtet. Für den Erwerb des Zertifikates können die Studierenden aus Veranstaltungen des regulären Lehramtsstudiums bestimmte Seminare mit Medienswerpunkt auswählen, die von der Akademie für Bildungsforschung und Lehrerbildung für das Zertifikat akkreditiert wurden. Im Rahmen des Zertifikatserwerbs sind die Lehramtsstudierenden darüber hinaus verpflichtet, eine einmal im Jahr angebotene Ringvorlesung mit Tutorium zu besuchen. Die Ringvorlesung beinhaltet wechselnde Themen, so dass jeweils aktuelle Entwicklungen und Trends im Bereich Medien und Schule aufgegriffen werden. Im Wintersemester 2013/2014 stand die Ringvorlesung beispielsweise unter dem Titel "Kinder und Jugendliche im Web 2.0: Neue Medien und Soziale Netzwerke". Referentinnen und Referenten der Goethe-Universität sowie externe Experten aus dem Bereich Medienbildung trugen hierzu ihre Expertise bei und hielten Vorträge zu Themen wie "Tablets in der Schule", "Computersucht - Pathologische Mediennutzung", "Cybercrime", "Beziehung, Kommunikation und Partizipation im Zeitalter von Social Media" usw.

Neben dem Medienkompetenzzertifikat für Lehramtsstudierende bietet die Akademie für Bildungsforschung und Lehrerbildung auch Veranstaltungen zum Thema Medien-, Informations- und Datenschutzkompetenz im Rahmen der Reihe PRO-L an. PRO-L ist ein kostenloses Workshopprogramm, das speziell zur Professionalisierung von Lehramtsstudierenden eingerichtet wurde. Weitere Veranstaltungen und Förderprogramme zum Thema Medien-, Informations- und Datenschutzkompetenz werden über die zentrale eLearning Einrichtung der Goethe-Universität, studiumdigitale, angeboten. Diese Veranstaltungen richten sich an Studierende aller Fachrichtungen und Abschlüsse und richten sich daher natürlich auch an Lehramtsstudierende. Die Förderung der Medien-, Informations- und Datenschutzkompetenz ist in der Ausbildung der künftigen Lehrerinnen und Lehrer für das Unterrichtsfach "Politik und Wirtschaft" nicht explizit curricular verankert. Allerdings wird in den fachdidaktischen Grundlagen- und Vertiefungsveranstaltungen, in denen die digitalen Medien nicht nur zum Einsatz kommen, sondern auch Gegenstand der Veranstaltungen sind, immer wieder auf Fragen des Datenschutzes und des Urheberrechts eingegangen, um die Studierenden für einen verantwortungsbewussten Umgang mit den Medien zu sensibilisieren. Im Zeitalter des digitalen Wandels fällt die intensive Auseinandersetzung mit Fragen der Informationsgewinnung, -weitergabe und -speicherung in den Kernbereich sozialwissenschaftlicher Bildung.

Weiter bietet die Goethe-Lehrerakademie Veranstaltungen explizit zum Thema Datenschutz an. So existiert ein dreiwöchiges eLearning-Seminar "Schule und Datenschutz in Hessen - Die Aufgaben der Datenschutzbeauftragten in der Schule". Es stellt die täglichen und praxisbezogenen Aufgaben der Datenschutzbeauftragten in den Schulen in den Mittelpunkt. Die Inhalte der Seminarangebote zum Thema "Datenschutz in Hessischen Schulen" sollen immer den aktuellen Stand des Datenschutzrechts mit einem besonderen Blick auf die Schulen reflektieren. Daher gibt es im Rahmen der Weiterentwicklung der Kursangebote auf der fachlichen Ebene eine enge Kommunikation zwischen dem HDSB (Hessischen Datenschutzbeauftragten) und den Tutoren der Veranstaltung mit dem Ziel, die Qualität der Inhalte zu prüfen und weiterzuentwickeln.

Die Ausbildung von Medienkompetenz von Lehrerinnen und Lehrern ist in vierfacher Weise im Aufbaumodul "Lehren und Lernen mit Medien" im Rahmen des Lehramtsstudiums an der Justus-Liebig-Universität Gießen (JLU) verankert: Erstens lernen Studierende hier die Potentiale

kennen, die Medien im Hinblick auf die Gestaltung von Schule und Unterricht sowie das Lernen zu Hause und/oder in sozialen Gruppen haben. Zweitens lernen die Studierenden die instruktionswissenschaftlichen sowie methodisch-didaktischen Prinzipien kennen, die bei der Gestaltung von Lehrmedien berücksichtigt werden sollten, um lernwirksame und in der jeweiligen Alterszielgruppe gut akzeptierte Lehrmedien zu erhalten. Drittens lernen Studierende das selbstständige Gestalten von Lehrmedien mit Hilfe von Autorenwerkzeugen. Hierzu hat eine Arbeitsgruppe umfangreiches und hoch performantes Schulungsmaterial sowie Coaching-Guidelines entwickelt. Viertens lernen die Studierenden das Entwerfen von Lehr-Lern-Szenarien unter Nutzung digitaler Medien.

Darüber hinaus realisiert ein Großteil der Grundwissenschaften und Fachdidaktiken in den Lehramtsstudiengängen an der JLU eine Vielzahl von Lehrangeboten für eine gezielte Förderung von fachübergreifender und/oder fachdidaktisch fundierter Medienkompetenz (Reflexion relevanter Medientheorien, Medienerziehung, gesellschaftspolitische Bedeutung neuer Medien, Nutzung von Interaktiven Whiteboards (IWBs), lerntheoretisch und/oder fachdidaktisch fundierte Produktion von WBTs (web-based Trainings), Podcasts, Wikis oder Filmen).

Um das Angebot an Lehrveranstaltungen, die den Aufbau und die Entwicklung von Medienkompetenz der Lehramtsstudierenden an der Universität zum Ziel haben, auszubauen und sich mit den anderen hessischen Universitäten sowie den weiteren Phasen der Lehrerbildung diesbezüglich abzustimmen, ist die JLU über das Zentrum für Lehrerbildung in einer Steuergruppe "Medien in der Lehrerausbildung" vertreten. Das Zentrum für Lehrerbildung wirbt unter anderem beim Projekt Schule@Zukunft Mittel ein, um konkrete Veranstaltungen zu Medienkompetenz angemessener und in Kooperation mit den weiteren Phasen der Lehrerbildung realisieren zu können.

Die Fortbildungen des Zentrums für Lehrerbildung richten sich unter anderem an die Beauftragten im Rahmen der Schulpraktischen Studien, also diejenigen Dozentinnen und Dozenten, die die Praxisphasen in den Schulen mit den Studierenden vorbereiten, sie begleiten und die Praktika nachbereiten. Über deren Multiplikatorenfunktion wird eine erhebliche Anzahl von Studierenden erreicht.

Darüber hinaus bestehen Angebote zur konkreten Entwicklung und Nutzung von Medien in einzelnen Fächern.

Frage 222. Welche dauerhaften Maßnahmen und Projekte zur Förderung der Medien- und Datenschutzkompetenz unterstützt die Landesregierung bei nicht schulischen öffentlichen Bildungsträgern?

Das Kultusministerium kooperiert eng mit den Medienanstalten LPR und dem HR im Bereich der Medienbildung und unterstützt im Rahmen dieser Kooperationen finanziell, personell und durch fachliche Beratung vielfältige schulische Medienkompetenzprojekte sowie Fortbildungsmaßnahmen für Lehrkräfte.

Im Bereich der Erwachsenenbildung wird auf die Antwort der Frage 148 verwiesen.

Die Technische Universität Darmstadt verweist für das Lehramt am Gymnasium (LAG) im Bereich der Grundwissenschaften auf folgende Modulbeschreibung: [http://www.zfl.tu-darmstadt.de/media/zfl/lagpdf/lag\\_grundwissenschaften\\_module\\_end\\_april2009.pdf](http://www.zfl.tu-darmstadt.de/media/zfl/lagpdf/lag_grundwissenschaften_module_end_april2009.pdf).

Im Kontext der entsprechenden Studienordnung wird sichtbar, dass die Vorlesung "Pädagogik der Neuen Medien" ein Bestandteil des Pflichtmoduls ist. Gemäß Studienordnung wird darin insbesondere auch das Ziel "Den Einsatz neuer Medien pädagogisch begründen und argumentativ vertreten" verfolgt. Das Wahlpflichtmodul "Informationspädagogik" (sowohl für LAG als auch für Master of Education /M.Ed.) enthält die "Informationspädagogik" als Vorlesung; die "Neuen Medien in der Bildung" als Seminar und das E-Learning-Projekt als Projektseminar. Gemäß Studienordnung werden dabei folgende Ziele - insbesondere für eine spätere Medienkompetenz - verfolgt:

- Einsatzbereiche für Neue Medien in Bildungsprozessen hinsichtlich ihrer unterschiedlichen lernfördernden Potenziale differenzieren und begrenzen;
- die Modellierungsfunktion der Neuen Medien beurteilen und an Beispielen aus den Studienfächern demonstrieren oder illustrieren;
- Neue Medien in Bildungsprozessen so einsetzen, dass neue Möglichkeiten der Veranschaulichung und der Verständnisförderung erschlossen werden;
- den Einsatz Neuer Medien in Bildungsprozessen so organisieren, dass die Lernenden zu erhöhter Selbsttätigkeit und eigenverantwortlichem Lernen angeregt werden;
- für die pädagogische Sinnhaftigkeit selbst entwickelter Formen des Medieneinsatzes argumentativ (auch in Bezug auf kritische Nachfrage) eintreten;
- Heterogenität in Lerngruppen für kooperative Arbeit mit Neuen Medien fruchtbar werden lassen;

- eigene Kenntnisse und Fähigkeiten auf dem Gebiet der Neuen Medien so weitergeben, dass andere davon lernen können;
- die Entwicklungen auf dem Gebiet der Neuen Medien so beurteilen, dass daraus der eigene Weiterbildungsbedarf abgeleitet werden kann.

An der Goethe-Universität Frankfurt werden folgende e-Learning-Zertifikate/Workshops angeboten:

- **Veranstaltungen der Goethe-Lehrerakademie:**
  - MedienBildungsMesse 2013,
  - Neue Medien im Unterricht,
  - Schule und Datenschutz in Hessen: Die Aufgaben der Datenschutzbeauftragten in der Schule.
- **Universität des 3. Lebensalters e.V.:**
  - Übung Literaturrecherche im Internet,
  - AG Internetkommunikation - Technische und gesellschaftliche Entwicklungen. Projektgruppe Enigma.
- **Hochschulrechenzentrum (HRZ):**
  - Seminar: Studieren mit dem PC,
  - Lunch Time Lectures über PC-Benutzung für Studierende der Naturwissenschaften,
  - Schulungen zum Umgang mit Lernplattformen:
    - OLAT-Workshops,
    - LON-Capa über naturwissenschaftliche Lernnetzwerke.
  - Schulungen zum Umgang mit Content Management Systemen.
- **Innerbetriebliche Weiterbildung:**
  - Diverse Seminare zu PC-Programmen und e-Learning,
- Kompetenzzentrum für Neue Medien in der Lehre.
- Im Rahmen der Lehrerausbildung an der ABL: Möglichkeit des Erwerbs eines Medienkompetenzzertifikats für Lehramtsstudierende.

Im Rahmen des Innovations- und Strukturentwicklungsprogramms 2012 bis 2015 fördert das Ministerium für Wissenschaft und Kunst an der Technischen Hochschule Mittelhessen (THM), initiiert vom Datenschutzbeauftragten der Hochschule, mit jährlich 90.000 € das Projekt "Modellhafte Datenschutzrevision einer hessischen Hochschule und Entwicklung eines Awareness- und Compliance-Programms und -Katalogs für Datenschutz und -sicherheit an Hochschulen - DACH". Ziel des Projekts ist die Schaffung eines umfassenden Awareness- und Compliance-Programms und -Katalogs für Datenschutz- und Datensicherheit in einer hoch differenzierten IT-Hochschul-Infrastruktur sowie die Realisierung von Datenschutz und Datensicherheit durch praxistaugliche Hilfestellungen für die Hochschulmitglieder und hochschulweite Zugriffsmöglichkeiten auf entsprechende Informationen (Datenschutzportal). Die Sensibilisierung und Weiterbildung der Hochschulbeschäftigten für Fragen des Datenschutzes und der Datensicherheit ist dabei eine zentrale Aufgabe.

Abgesehen von dem o.g. Projekt der Technischen Hochschule Mittelhessen, das im Rahmen des Innovations- und Strukturentwicklungsprogramms gefördert wird, findet für die weiteren Maßnahmen keine Einzelunterstützung statt; die Hochschulen werden seitens der Landesregierung im Rahmen des Globalbudgets finanziert.

Frage 223. Welche Kooperationen von Schulen und Hochschulen mit außerschulischen Akteuren auf dem Gebiet der Förderung der Medien- und Datenschutzkompetenz sind der Landesregierung bekannt und welche werden von ihr unterstützt?

Für den schulischen Bereich wird auf die Antwort der Frage 222 verwiesen.

Für die Technische Universität Darmstadt ist das Forschungsprojekt Generation "Gefällt mir" - Wie die Jugend klickt, Fachgebiet (FG) Professor Dr. Peter B. und HR-INFO, zu nennen. Für diese Studie bat das FG Wirtschaftsinformatik etwa 200 Schülerinnen und Schüler, eine Woche lang ein Social-Media Tagebuch zu führen.

Die Jugendlichen dokumentieren unter anderem, was sie posteten, was ein "Gefällt mir" wert war und was sie nervte. Dem Forscherteam war es auch wichtig herauszufinden, wie ernst die jugendlichen Nutzerinnen und Nutzer den Schutz ihrer persönlichen Daten und der Privatsphäre nahmen.

In der Studie wurden insbesondere zwei Themenbereiche adressiert: zum einen die Frage wie Erwachsene das Verhalten von Jugendlichen in Sozialen Netzwerken einschätzen. Ein Schwer-

punkt waren hierbei wahrgenommene Privatsphäre-Risiken. Zum anderen war die Nutzung von Facebook im Schulunterricht Gegenstand der Untersuchung.

Der Hessische Rundfunk dokumentierte und begleitete das Projekt und ließ Jugendliche, Eltern, Lehrkräfte, Internetexperten und Verantwortliche aus der Politik zu Wort kommen.

Im Rahmen der Seminarangebote zum Thema "Datenschutz in Hessischen Schulen" der Goethe-Lehrerakademie der Goethe-Universität Frankfurt findet eine enge Abstimmung zwischen dem Hessischen Datenschutzbeauftragten und den Tutoren/-innen der Veranstaltung statt.

Bei der Fachhochschule Frankfurt am Main (FH FFM) sind zu nennen:

- fraLine (Stadt Frankfurt am Main und FH FFM/Frankfurter Technologiezentrum [:Medien] - FTzM),
- Unterrichtsbegleitung (staatl. Schulamt/HKM und FH FFM/FTzM),
- Seminare für IT-Beauftragte (staatl. Schulamt/HKM und FH FFM/FTzM),
- fraMediale (FH FFM/FTzM).

Das Projekt "Kinderperspektiven zu Kinderrechten in pädagogischen Arrangements" ist eine Kooperation zwischen der Hochschule RheinMain, Fachbereich Sozialwesen, dem Verein "Makista e.V. - Bildung für Kinderrechte und Demokratie" und Grundschulen in Hessen.

Einzelne Mitglieder der Hochschule RheinMain sind im Chaos Computer Club organisiert und führen im bundesweiten Projekt "CCC macht Schule" gelegentlich Beratung in Schulen durch.

Für die o.g. Kooperationen findet keine Einzelunterstützung statt; die Hochschulen werden seitens der Landesregierung im Rahmen des Globalbudgets finanziert.

Frage 224. In welcher Weise wird der Trend zur immer stärkeren mobilen Internetnutzung im Rahmen der Arbeit der Bildungsinstitutionen berücksichtigt?

Schulen entscheiden sich im Rahmen ihrer eigenverantwortlichen pädagogischen Konzeption für den Einsatz von Tablets und anderen mobilen Endgeräten und neuen Medien im Unterricht, so dass in diesem Zusammenhang auch eine zunehmende mobile Internetnutzung im Rahmen des unterrichtlichen Einsatzes in Abhängigkeit von den technischen Voraussetzungen an der Schule in der Entscheidung der jeweiligen Schule liegt.

Darüber hinaus startete mit Beginn dieses Schuljahres das Landesprojekt "Mobiles Lernen" an sechs hessischen Grundschulen, das den Einsatz und die Wirkung von Tablets im Unterricht unterschiedlicher Fächer erproben soll. Im Rahmen dieses Projekts erfolgt u.a. die Internetnutzung der Schülerinnen und Schüler unter Anleitung und enger Begleitung der Lehrkräfte. Das Projekt wird von der Universität Frankfurt am Main wissenschaftlich begleitet.

Die Landesregierung hat im letzten Jahrzehnt den Einsatz neuer Medien durch die Förderung innovativer Projekte an den hessischen Hochschulen unterstützt, insbesondere Maßnahmen, die den Zugriff auf Lehrmaterialien der Hochschule über das Internet durch mobile Endgeräte erlauben. Beispielsweise wurden in den Jahren 2009 bis 2011 insgesamt 2 Mio. € in die Förderung solcher Projekte investiert. In den Jahren 2012 bis 2013 flossen 8 Mio. € aus Mitteln des Hochschulpaktes 2020 in Maßnahmen, die unter anderem den mobilen Zugriff auf Ressourcen der hessischen Hochschulen zum Ziel hatten.

Daneben unterstützt die Landesregierung das Kompetenznetz E-Learning Hessen ([www.e-learning-hessen.de](http://www.e-learning-hessen.de)), in dem sich hochschulübergreifend die Multimedia-Kompetenzzentren der hessischen Hochschulen über den Einsatz der neuen, insbesondere der mobilen Technologien verständigen.

"OpenLearnWare" wird die Web-Plattform der Technischen Universität Darmstadt (TUD) für die Veröffentlichung und den weltweit freien Zugang von digitalen Lehr- und Lernmaterialien genannt. Über die Plattform lassen sich Videos, Folien-Präsentationen, Skripte und Podcasts von Veranstaltungen sowohl der TUD als auch von anderen Hochschulen finden. Die Plattform richtet sich an Studierende, Lehrende, Gastwissenschaftler/-innen der TUD sowie die interessierte Öffentlichkeit. Die Plattform ist eine Eigenentwicklung mit Hilfe von Open-Source-Komponenten. Lehrende können mittels des eingebauten Administrations-Tools ihr Lehrmaterial auf OpenLearnWare hochladen und nach Vergabe von Metadaten zur Veröffentlichung freigeben. Zur Materialrecherche können eine Volltextsuche sowie diverse miteinander kombinierbare Filter genutzt werden. Ca. 2.000 Einzelmaterialien aus neun Fachbereichen können bereits über diese Plattform abgerufen werden. Zwischen April und Oktober 2013 wurden auf der Plattform 50.000 Besucher und 190.000 Suchanfragen registriert.

"Moodle" ist die zentrale Lernplattform der TUD. Mit dem Learning Management System (LMS) Moodle können Lehrende ihre Lehrveranstaltungen durch einen virtuellen Kursraum im Web ergänzen und alle digitalen Angebote einer Lehrveranstaltung zentral anbieten. Moodle zeichnet sich in erster Linie durch die aktive Einbindung der Studierenden in die Lehrveranstaltung aus. Den Anforderungen des kollaborativen Lernens stellt sich Moodle sowohl mit synchronen (Chat-Funktion) als auch asynchronen Instrumenten (z.B. Foren, Wikis, Glossar, FAQ).

Moodle ist auf virtuelle Lern- und Arbeitsräume ausgelegt, in denen Lehr- und Selbstlernmöglichkeiten angeboten werden. Mit Hilfe von Online-Tests überprüfen Studierende ihr Wissen und werden in der Prüfungsvorbereitung unterstützt. Moodle wird seit 2009 mit stark steigender Nutzung an der TUD eingesetzt. Die Konfiguration der Plattform wird eng mit dem Datenschutzbeauftragten der TUD abgestimmt. Die E-Learning-Arbeitsgruppe des Hochschulrechenzentrums an der TUD fördert nachhaltig die Bildungsinitiative Open Educational Resources (OER) und betreut die beiden o.g. Plattformen.

Die Goethe-Universität Frankfurt ist bestrebt, die mobile Internetnutzung für Studierende und Mitarbeitende auszubauen und auch die Nutzung neuer Geräteformate zum Abruf der digitalen Inhalte und Dienste zu ermöglichen. In einzelnen werden folgende Ziele verfolgt:

- W-LAN: Die Goethe-Universität baut seit 2003 die Versorgung mit WLAN kontinuierlich aus. Mit der Fertigstellung des Seminarhauses zum Sommersemester 2015 werden insgesamt ca. 1.500 Access Points an der Goethe-Universität in Betrieb sein. Alle Hörsäle, Seminarräume und die Verkehrsflächen werden dann mit WLAN versorgt sein, die Freiflächen zwischen den Gebäuden weitgehend. Es wird angestrebt, zukünftig auch alle Bürobereiche mit WLAN zu versorgen.
- Drahtloser Internetzugang an anderen Universitäten und Forschungseinrichtungen: Im Eduroam-Verbund können sich Mitglieder und Angehörige der beteiligten Hochschulen und Forschungseinrichtungen an den anderen Standorten mit ihrem Heimataccount drahtlos mit dem Internet verbinden. Es nehmen praktisch alle Universitäten in Europa sowie zahlreiche amerikanische Einrichtungen teil.
- Vorlesungsaufzeichnungen: Zahlreiche Vorlesungen und Veranstaltungen werden an der Goethe-Universität aufgezeichnet und stehen dann unmittelbar als Videostream und anschließend online zum Abruf zur Verfügung. Federführend sind hier das Hochschulrechenzentrum und studiumdigitale, die zentrale eLearning-Einrichtung der Goethe-Universität.
- Lernplattform (Learning Management System): Mit OLAT steht eine zentrale Lernplattform zur Verfügung, auf der aktuell mehr als 1.200 curriculare Kurse gehostet werden: <https://olat.server.uni-frankfurt.de>. Die Kursinhalte und Lernbausteine sind auf der Lernplattform für Mitglieder und Angehörige der GU ständig und weltweit abrufbar.
- E-Mail-Abruf per Webclient: E-Mails können mobil über einen Webclient abgerufen und versandt werden.
- Ausrüstung des Otto-Stern-Zentrums und der Seminarräume im PEG-Gebäude mit Videokonferenzeinrichtungen: Im Rahmen der zentral gesteuerten Medientechnik der GU können ad hoc in allen Hörsälen und Seminarräumen des Otto Stern Zentrums - Infrastrukturzentrum am Campus Riedberg, bestehend aus naturwissenschaftlicher Bereichsbibliothek, Cafeteria und Hörsälen - und des Gebäudes der Psychologie, Erziehungswissenschaften, Gesellschaftswissenschaften (PEG) Videokonferenzschaltungen vorgenommen werden.
- Online verfügbare Selbstbedienungsfunktionen: Im Rahmen des Studierenden Life Cycle im Campus Management wird, wo immer persönliche Identitätsüberprüfungen etc. nicht notwendig sind, auf online verfügbare Selbstbedienungsfunktionen zurückgegriffen.
- Darstellung der Web-Präsenz der Goethe Universität im sogenannten "responsive design": Layout und Anordnung auf der Webseite werden den Möglichkeiten des aufrufenden Endgeräts (Laptop, Tablet, Smartphone) automatisch angepasst. Diese befindet sich in unmittelbarer Vorbereitung.

Systematische Zahlen zur didaktischen Nutzung von mobilem Internet in Lehrveranstaltungen liegen an der Justus-Liebig-Universität Gießen derzeit nicht vor. Entsprechende Erhebungen sind im Rahmen geplanter Forschungsvorhaben zur Bereitschaft der Nutzung innovativer Medien vorgesehen.

Ab dem Wintersemester wird in einer Studie der Einsatz von mobilen Endgeräten (Smartphones, Tablets) als Classroom Response System ("Clicker", "TED") in der Lehre auf ihre Einsetzbarkeit und Lernwirksamkeit hin untersucht werden.

Eine Studie zur Erhebung von studentischen Lehrveranstaltungsevaluationen per mobilen Endgeräten (vs. Papier bzw. Online-Fragebogen am PC) läuft derzeit und wird bis Herbst erste Ergebnisse liefern.

Ein entsprechendes Forschungsprojekt ist derzeit am Frankfurter Technologiezentrum [:Medien] - FTzM der Fachhochschule Frankfurt am Main (multiperspektivisch: Medienintegration/Bildungsinformatik/Lehr-Lern-Forschung) in Planung bzw. Verhandlung.

Grundsätzlich wird bei der Gestaltung digitaler Angebote für Studierende und Dozenten darauf geachtet, dass diese auch über mobile Endgeräte nutzbar sind.

Im Rahmen des Datenschutzprojekts DACH an der Technischen Hochschule Mittelhessen wurde Anfang 2013 für die Beschäftigten in der neu aufgelegten Broschürenreihe "Arbeitshilfe Datenschutz" ein Heft zum Thema "Datenschutzgerechter Umgang mit E-Mails" veröffentlicht. Das Heft ist auch über die Homepage der Hochschule abrufbar.

Ein weiteres Heft der Reihe behandelt das Thema "Bildrechte, Fotos und Lizenzen in der Praxis", u.a. den Umgang mit Bildveröffentlichungen in Sozialen Netzwerken.

Ferner wurde in enger Kooperation mit der Abteilung ITS und dem Datenschutzbeauftragten der Hochschule eine neue "Benutzungsordnung für die IT-Services der Technischen Hochschule Mittelhessen" entwickelt, die sich aktuell im personalvertretungsrechtlichen Mitbestimmungsverfahren befindet.

Das Projekt "Kinderperspektiven zu Kinderrechten in pädagogischen Arrangements" stellt den Beginn der Arbeit mit digitalen, mobilen Medien an der Hochschule Rhein Main im Fachbereich Sozialwesen dar.

Mobile Internetnutzung einschließlich Fragen der Sicherheit werden in verschiedenen Lehrveranstaltungen im Bachelor-Studiengang Angewandte Informatik sowie im Master-Studiengang Informatik behandelt (z.B. Mobile Anwendungen, Web-basierte Anwendungen, Security).

Frage 225. Welche Schulen, Hochschulen und weitere Bildungsinstitutionen in Hessen sind auf dem Gebiet Vorreiter und können als Beispielprojekte für andere Einrichtungen dienen?

Auf die Antwort zur Frage 224 wird verwiesen. Ergänzend ist zu erwähnen, dass im Rahmen des Landesprojekts "Mobiles Lernen" ein Austausch mit anderen Tablet-Projekten im Land angeboten und mit den bekannten Projekten gepflegt wird. Ein Informationsaustausch findet auch auf der Ebene der Fachberaterinnen und Fachberater Medienbildung der Staatlichen Schulämter statt.

Die Technische Universität Darmstadt (TUD) beansprucht für sich eine Vorreiterrolle für virtuelle Lehre. Insbesondere die Entwicklung und Umsetzung didaktischer Konzepte für eine digitalisierte Lehre unter Berücksichtigung der mobilen Internetnutzung ist ein Schwerpunkt an der TUD. Gleichzeitig wird auf die Antwort zur Frage 224 verwiesen.

Die Goethe-Universität Frankfurt sieht sich im Vergleich mit den anderen hessischen Universitäten durchaus als richtungsweisend, insbesondere beim Konzept zur zentralen Medientechnik.

Das Frankfurter Technologiezentrum [:Medien] - FTzM der Fachhochschule Frankfurt am Main kooperiert seit nunmehr zwölf Jahren mit der Stadt Frankfurt in einer Reihe von Projekten z.B. fraLine, fraMediale. Weitere Projekte laufen mit dem Staatlichen Schulamt.

Im Rahmen des Datenschutzprojekts DACH an der Technischen Hochschule Mittelhessen (THM) wird auf die Weiterbildung zum Thema Datenschutz und Medienkompetenz besonderes Augenmerk gelegt. Aktuell wird ein Weiterbildungsprogramm entwickelt, das ab dem Jahr 2015 den Beschäftigten angeboten wird. In den Jahren 2013 und 2014 wurden erste Angebote durchgeführt. So wurde z.B. im Herbst 2013 eine ganztägige Inhouse-Schulung unter der Überschrift "Beipackzettel Internet - digitale Medienkompetenz" speziell für die Auszubildenden der Hochschule angeboten. Von den 24 Auszubildenden nahmen an der Schulung 22 teil. Aufgrund der hohen Nachfrage und positiven Bewertung der Veranstaltung durch die Teilnehmerinnen und Teilnehmer werden weitere Schulungen für Auszubildende der THM zum Thema Medienkompetenz in 2015 angeboten.

In Kooperation mit zwei weiteren hessischen Hochschulen wurden durch den Datenschutzbeauftragten der THM zwei Weiterbildungsveranstaltungen zum Thema Datenschutz und Internetnutzung mit insgesamt 50 Teilnehmerinnen und Teilnehmern durchgeführt.

Mit dem THM-Datenschutztag wurde 2013 eine Halbtagesveranstaltung mit drei Vorträgen ins Leben gerufen, auf der zentrale Problemstellungen des Datenschutzes an Hochschulen intensiv dargestellt und diskutiert werden. Die Themen des THM-Datenschutztages am 28. Januar 2013 waren: Professionelles E-Mail-Management und Datenschutz, Datensicherheit und Social Engineering sowie richtiger Umgang mit Social Media in Hochschule und Unternehmen.

Da die Veranstaltung großen Anklang fand und sehr positive Rückmeldungen sowie sehr positive Presseberichterstattung erbrachte, wird der THM-Datenschutztag nunmehr in jährlichem Turnus stattfinden. Am 25. Februar 2014 fand daher der 2. THM-Datenschutztag mit rund 250 Teilnehmerinnen und Teilnehmern zu den Themen Urheberrecht, Foto- und Lizenzrecht und Recht am eigenen Bild und zum Thema BYOD (Bring your own device) aus rechtlicher und technischer Sicht sowie einer Vorführung zum Live-Hacking statt. Von den Teilnehmerinnen und Teilnehmern waren jeweils über die Hälfte Beschäftigte der Hochschule.

Die Hochschule Rhein Main verweist bezüglich der Thematisierung mobiler Anwendungen und Internet-Sicherheit auf ihren Bachelor-Studiengang "Angewandte Informatik" sowie den Master-Studiengang "Informatik".

Frage 226. Welche Forschungsprojekte gibt es an hessischen Hochschulen zur Förderung der Medien- und Datenschutzkompetenz sowie zum Verbraucherschutz im Internet?

Für die Technische Universität Darmstadt (TUD) sind hier zu nennen:

- **Nutzerfreundliche, sichere E-Mail-Kommunikation**

Das Projekt zielt darauf ab, die Nutzerfreundlichkeit von sicherer E-Mail-Kommunikation zu verbessern. Es werden zwei unterschiedliche Bereiche untersucht: Senden und Empfangen von vertraulichen und authentischen E-Mails: Wie kann die Lücke zwischen Ende-zu-Ende-Verschlüsselung und Lösungen wie dem De-Mail-Konzept geschlossen werden? Welche Vorstellung haben Nutzer von Schlüsseln, Schlüsselpaaren oder Public Key-Infrastrukturen (PKI)? Wie kann ein nutzerfreundlicheres Konzept für PKI und sichere E-Mail-Systeme aussehen, das Nutzer besser verstehen als existierende Lösungen und daher auch akzeptieren?

Warnmeldungen bei potenziell gefährlichen Anhängen und Phishing-Seiten: Es sollen neue Warnmeldungen entwickelt werden, die auf Informationen zur Sicherheit sowie zur Identität des Absenders und dem Datentyp des E-Mail-Anhangs basieren. Die Warnmeldungen sollen Nutzerinnen und Nutzer eine konkretere Entscheidungsgrundlage dafür bieten, ob sie einen Anhang öffnen oder besser ignorieren sollten. Die Horst Görtz Stiftung fördert das Projekt über LOEWE CASED mit einem Doktorandenstipendium in der Forschungsgruppe SecUSo.

- **Browser-Erweiterung**

Facebook Privacy Watcher ist eine Erweiterung für Mozilla Firefox und Google Chrome, die am Center for Advanced Security Research Darmstadt (CASED) in Zusammenarbeit mit der TUD entwickelt wurde. Sie bietet eine neue und sehr einfache Schnittstelle, um die Privatsphäre-Einstellungen auf Facebook zu verwalten.

- **InUse-Benutzerunterstützung zur Bewertung der Vertrauenswürdigkeit von Webseiten und Webshops:**

Die Bandbreite der im Internet auf Webseiten angebotenen Dienste steigt beständig und damit einhergehend auch die Bedrohungen für die Nutzer von Online-Banking, Online-Shopping oder Sozialen Netzwerken. Technische Sicherheitsmechanismen, wie verschlüsselte Verbindungen (HTTPS) mit der verbundenen Überprüfung des Webservers (PKI), haben sich als unzulänglich erwiesen, den Bedrohungen angemessen zu begegnen. Die Mechanismen benötigen die Unterstützung des Anwenders, nicht nur wenn auf ungewöhnliche Situationen reagiert werden muss ("ungültiges Zertifikat"), sondern auch weil Menschen bereit sind, je nach Situation unterschiedlich hohe Risiken einzugehen. Aktuell ist für eine angemessene Interaktion mit den Sicherheitsmechanismen allerdings ein hohes Maß an Sicherheitsbewusstsein und Expertise notwendig, so dass die Mechanismen mit ihren Warnungen mehr als zu umgehende Störung denn als Unterstützung wahrgenommen werden. Es fehlt eine umfassende Einbindung der Mechanismen in das "Ökosystem Web", das Anwender genauso einschließt wie die Dienstbetreiber und die technischen Mechanismen.

InUse begegnet diesen Herausforderungen mit einem multidisziplinären Forschungsansatz: Die Expertise der Projektpartner im Bereich benutzbare Sicherheit (TUD), Rechtswissenschaft (Universität Kassel), IT-Auditierung (usd) und digitaler Identität (Kobil) ermöglicht eine umfassende Herangehensweise an die Verringerung der Bedrohung: Auf der einen Seite soll die Unterstützung für die Anwender präzisiert und die Kommunikation durch höhere Verständlichkeit effektiver werden. Gleichzeitig werden rechtliche und organisatorische Aspekte von den entwickelten Sicherheitsmaßnahmen und -mechanismen betrachtet, wie dem Schutz der Privatsphäre und der Überprüfung von Webseiten zur Vergabe von Prüf-siegeln.

- **PersoApp - Sichere und benutzerfreundliche Internet-Anwendungen Nutzerorientierte Anforderungsanalyse:**

Das Team aus Sozialwissenschaftlerinnen und -wissenschaftlern sowie Informatikerinnen und Informatikern wird bundesweit Bürgerinnen und Bürger sowie Unternehmen befragen, welche Anforderungen sie an die Benutzbarkeit und Sicherheit von Internet-Dienstleistungen stellen. Mit den Ergebnissen wird das Projekt entsprechende Anwendungsszenarien für die Online-Ausweisfunktion des neuen Personalausweises erarbeiten. Unternehmen und Behörden können sich an diesen orientieren, um eigene IT-Anwendungen mit der Online-Ausweisfunktion zu entwickeln.

An der Goethe-Universität Frankfurt wird aktuell das BMBF-Projekt "Computergestützte, adaptive und verhaltensnahe Erfassung Informations- und Kommunikationstechnologie-bezogener Fähigkeiten (ICT-Skills) in PISA (CavE-ICT-PISA)" durchgeführt.

Inhalt des Projekts: Ein kompetenter Umgang mit Informations- und Kommunikationstechnologien (ICT) stellt aufgrund der alltäglichen Nutzung von Computern die Voraussetzung für eine erfolgreiche Teilnahme in modernen Wissensgesellschaften und damit ein wichtiges Bildungsziel dar. Im Rahmen des Verbundprojektes soll ein Instrument entwickelt werden, mit dem die ICT-Fähigkeiten von 15-jährigen Schülerinnen und Schülern computerbasiert gemessen werden können.

Die Vorgabe authentischer und adaptiver (d.h. an das individuelle Kompetenzniveau angepasster) Testaufgaben in verhaltensnaher Umgebung ermöglicht dabei eine valide und effiziente Messung der ICT-Fähigkeiten.

Weiter werden am Lehrstuhl für Öffentliches Recht, Informationsrecht, Umweltrecht, Verwaltungswissenschaft der Goethe-Universität durch die Lehrstuhlinhaberin als Leiterin der Forschungsstelle Datenschutz Projekte aus dem Bereich des Datenschutzrechts, des Informationsrechts und zu IT-Sicherheit sowie zur Gestaltung der Informationsgesellschaft durchgeführt. Auch wird die Reihe "Frankfurter Gespräche zum Informationsrecht" von Frau Professor Spiecker ausgerichtet. Die Frankfurter Gespräche zum Informationsrecht richten sich an Wissenschaft, Wirtschaft und Praxis. Sie bieten ein Forum sowohl für den Austausch über aktuelle Problemstellungen als auch für Grundsatzfragen aus allen Bereichen des Öffentlichen Informationsrechts. Behandelt werden daher Spezialgebiete wie Datenschutzrecht, Verbraucherinformationsrecht, Telekommunikationsrecht oder Medienrecht. Darüber hinaus bieten die Gespräche auch ein Forum für rechtstheoretische Themen wie die rechtliche Gestaltung der Informationsordnung, Rationalitätsfragen oder Entscheidungsverhalten. Die Veranstaltung ist intra- und interdisziplinär ausgerichtet, so dass die Frankfurter Gespräche zum Informationsrecht Juristinnen und Juristen aller Fachbereiche, aber auch Vertreterinnen und Vertretern benachbarter Wissenschaften eine Gelegenheit zum offenen, intensiven und fächerübergreifenden Diskurs bieten.

Bei der Fachhochschule Frankfurt am Main wird bezüglich Forschungsprojekten zur Medienkompetenz auf die Antwort zu Frage 223. verwiesen.

Frage 227. Plant die Landesregierung ein medienpädagogisches Bildungskonzept?  
Falls ja: Bitte das geplante Bildungskonzept darstellen.

Die Landesregierung ergreift Maßnahmen, um die medienpädagogische Arbeit an den Schulen konsequent auszubauen und insbesondere die Erarbeitung von schulischen Medienkonzepten zu befördern.

Dazu zählen der Auf- und Ausbau von entsprechenden Beratungs- und Unterstützungsstrukturen durch das Landesschulamt, insbesondere durch die Fachberater/-innen Medienbildung an den Staatlichen Schulämtern, aber auch durch die Leiterinnen und Leiter der Medienzentren vor Ort.

Eine verstärkte Unterstützung sollen die Schulen bei der Erarbeitung von schulischen Medienbildungskonzepten erhalten. Dazu soll ein Mediencurriculum als Orientierungshilfe zur Verfügung gestellt werden, das die Schulen bei der Umsetzung der in den Kerncurricula formulierten überfachlichen Kompetenzen der Medienbildung in den Fächern unterstützt.

Wiesbaden, 23. Januar 2015

Priska Hinz

Große Anfrage 19/1569

Beitrag zu **Frage 148** / Projekte die gezielt Erwachsene mit dem Internet oder anderen digitalen Medien vertraut machen, aufgeschlüsselt nach Art des Projekts, unterstützten Maßnahmen, Ort/Region, Träger

Art des Projekts	Unterstützende Maßnahmen	Ort/Region	Träger
HESSENCAMUS (HC) Leitprojekt 2010	Regionales Repository für Lernszenarien der Partner des HC Limburg-Weilburg - Einrichtung einer autonomen E-Learning-Plattform (Moodle) - Einrichtung eines regionalen Kursrepository für HESSENCAMPUS-Partner	Limburg-Weilburg	HC Limburg-Weilburg
HC Leitprojekt 2010	Neue Medien im HESSENCAMPUS – Aufbau einer zentralen Community-Plattform zur Unterstützung der Kooperation und der Kommunikation zwischen den Hessencampusinitiativen - Entwicklung und Erprobung didaktischer Szenarien / Blended Learning-Szenarien / Beratungen über Potentiale Neuer Medien in Bildungsprozessen - Umsetzung technischer Infrastruktur / Moodle-Lernplattform / Integration des Community-Tools Alfresco - Entwicklung eines Entwurfs für ein Medienkompetenzkonzept für Lehrende - Bereitstellung der vorhandenen Erfahrungen von Hessencampus-Akteuren / Content-Entwicklung	landesweit ausgerichtet	Hessischer Volkshochschulverband (hvv)
HC Sonderförderung Freier Träger 2010	Entwicklung einer Lernplattform / E-Learning / Blended-Learning-Kurse	Fulda	Katholische Erwachsenenbildung
HC Leitprojekt 2011	Bildungsallianz Funkkolleg - Erstellung der Website funkkolleg-musik.de - Erstellung von Klausuraufgaben - Online-Klausur / Präsenzklausur	landesweit ausgerichtet	Hessischer Rundfunk
HC Leitprojekt 2011	Neue Medien im HESSENCAMPUS 2011 - Auf- und Ausbau der Community / Vernetzung der Akteure - Aufbau und Umsetzung der technischen Infrastruktur / Austausch von Inhalten zwischen den Akteuren und Bildungseinrichtungen / hessenweite lernplattform (Moodle) - Entwicklung eines hessenweiten Qualifizierungsrahmens für Dozierende / Qualifizierungsprogramm Online Education Skills - Entwicklung eines Geschäftsmodells (medienpädagogische Beratung, Implementierungsberatung) / Vision: Portal Hessencampus digitale	landesweit ausgerichtet	hvv
HC Sonderförderung Freier	Begleitendes Selbstlernen	Vogelsberg	Evangelische

Art des Projekts	Unterstützende Maßnahmen	Ort/Region	Träger
Träger 2011			Erwachsenenbildung
HC Leitprojekt 2012	<p>Neue Medien im HESSENCAMPUS</p> <ul style="list-style-type: none"> <li>- Qualifizierung, Beratung und Begleitung von Entscheidungsträgern bei Entwicklungen von Medienkonzepten / Bereitstellung und Betreuung von technischer Infrastruktur / Weiterentwicklung der Gesamtkonzeption in den Einrichtungen</li> <li>- Vernetzung von Akteuren und Bereitstellung einer hessenweiter Infrastruktur und Supportfunktion</li> </ul>	Main-Taunus-Kreis	HC Main-Taunus-Kreis
HC Leitprojekt 2012	<p>Neue Medien im HESSENCAMPUS</p> <ul style="list-style-type: none"> <li>- Umsetzung einer hessenweiten Implementierung und Ausweitung des Einsatzes neuer Medien in Bildungsprozessen</li> <li>- Verankerung zielgruppenorientierter Kompetenzen / Konzipierung selbständiger Bildungsangebote / Implementierung online-pädagogischer Formate</li> <li>- Unterstützung der Bildungseinrichtungen bei der technischen und pädagogischen Infrastruktur mithilfe hessenweiter Ansätze / Austausch von Erfahrungen / Best Practice Ansätze didaktischer Szenarien</li> <li>- Einheitliche Gestaltung von Qualifizierungsansätzen von Dozierenden im Bereich der Medienkompetenz</li> </ul>	landesweit ausgerichtet	hvv
HC Leitprojekt 2013	<p>Neue Medien im Hessencampus – Bestandsaufnahme und Weiterführungsempfehlung</p> <ul style="list-style-type: none"> <li>- Vorbereitung und Qualifizierung von Lehrkräften an Schulen und Volkshochschulen auf den Einsatz neuer Medien in Schule und Unterricht</li> <li>- Qualifizierung, Weiterentwicklung und Beratung von Beratern bei der Entwicklung von Medienkonzepten in ihren Einrichtungen</li> <li>- Hessenweiter Austausch und Vernetzung von Akteuren</li> </ul>	landesweit ausgerichtet	hvv
HC Sonderförderung Freier Träger 2013	<p>Implementierung von Facebook als strategische Maßnahme in kleinen Bildungseinrichtungen. Begleitende Evaluation verschiedener Praxisszenarien und Extrahierung der Erfolgs- und Machbarkeitsfaktoren</p>	Fulda	Evangelische Erwachsenenbildung