Positionspapier
Netzpolitik

(Stand: 23. Mai 2015)

Wer wesentliche Freiheit aufgeben kann, um eine geringfügige bloß jeweilige Sicherheit zu bewirken, verdient weder Freiheit, noch Sicherheit. (Benjamin Franklin)

1. VISION

Das Internet hat die Welt in so einer kurzen Zeit so stark verändert wie noch kaum eine andere Entwicklung davor. In einigen Bereichen ist eine solch disruptive Kraft, dass vieles, was bisher unvorstellbar war, nun möglich ist und das, was gegolten hat, keine Gültigkeit mehr besitzt. In vielen Bereichen bemerkt man Brüche zwischen der analogen und der digitalen Welt, obwohl eine Unterscheidung in zwei Welten schon lange überholt ist.

NEOS sieht die großen Chancen dieser Entwicklungen und steht ihnen äußerst aufgeschlossen gegenüber.

Dennoch erfordern diese Veränderungen noch viele Anpassungen: die technischen Grundlagen wurden gelegt in Zeiten, in denen noch nicht abzusehen war, dass diese Entwicklung eine solche Schlagkraft besitzen wird.

So wurde beispielsweise der Schutz von Nutzerdaten nicht als Automatismus in die Technik eingepflegt. Mit Privacy by Design gibt es dazu ein gutes Konzept, das bei jedem erdenklichen Produkt, jeder Anwendung oder sonstigen Dienstleistung direkt implementiert werden sollte – unabhängig davon, ob das Angebot von staatlicher oder privater Stelle stammt. Auch muss der Staat einen höchstmöglichen Datenschutz und Datensicherheit rechtlich verankern, um seiner Schutzfunktion angemessen nachzukommen. Bürger_innen können dazu unterstützend selbst tätig werden, indem sie kryptographische Methoden konsequent einsetzen.

Die Möglichkeit große Datenmengen in hoher Qualität auszutauschen hat auch die Verhältnisse im Urheberrecht verändert. Wir müssen darüber diskutieren, was uns Kunst und Kultur wert ist und wie wir es finanzieren wollen.

Einzelne Firmen besitzen große Teile der Plattformen, welche für die Auffindbarkeit von Inhalten im Internet verwendet werden. Man muss darüber nachdenken, wie man mehr Wettbewerb und damit mehr Pluralität in diesem Bereich ermöglicht.

Neue Chancen tun sich durch den digitalen Wandel in vielen Feldern auf. So wird auch eine neue Form der Partizipation und Mitentscheidung auf Augenhöhe möglich. Bürger_innen haben die Möglichkeit, sich viel umfassender und vor allen Dingen auch schneller zu informieren, als je zuvor. Unsere Demokratie muss sich daran noch anpassen, zum Beispiel hinsichtlich der Informationsfreiheit und Transparenz im Allgemeinen.

Hinsichtlich einer größtmöglichen Partizipation ist es wichtig, möglichst niederschwelligen Zugang für alle zu gewährleisten. Nur so werden eine echte Teilhabe und ein Ergreifen der Chancen tatsächlich möglich. Dies betrifft nicht nur die Ausgestaltung von Anwendungen, Prozessen, etc., sondern auch den Bereich der Bildung und Weiterbildung.

Weiters bestehen durch den digitalen Wandel auch enorme Chancen für Gründer_innen. Innovative Start-Ups tragen dazu bei, den Prozess voranzutreiben, schaffen Arbeitsplätze und neue Geschäftsmodelle.

Wir wünschen uns eine Gesellschaft, in der die mit dem digitalen Wandel einhergehende Entwicklung als Chance gesehen wird, die noch vorhandenen Brüche geschlossen werden,

Partizipation und Teilhabe ermöglicht werden und bei all dem der Schutz der Privatsphäre vollumfänglich geleistet wird.

Das Internet ist ein gesellschaftlicher Game Changer. Seit mehr als vier Jahrzehnten ist das Netz ein Experimentierfeld für neue Möglichkeiten der Kommunikation und Vernetzung. Es veränderte sich vom Spielplatz zum dominanten Faktor gesellschaftlicher Aushandlungsprozesse. Netzpolitik ist viel mehr als die Summe aus Medienpolitik und Briefgeheimnis. Was wir in den letzten Jahrzehnten erleben, ist nicht nur ein Kommunikationswandel, sondern ein Gesellschaftswandel. Heute verfügen, laut Eurostat, mehr als drei Viertel der EU-Bürger_innen über einen Zugang zum Netz. Das Internet ist eine Ebene, auf der wir Kernwerte unserer Gesellschaft verhandeln, wo Meinung entsteht und geformt wird. Unser Verhältnis zu öffentlicher und privater Sphäre, wie wir in Zukunft über geistiges Eigentum denken und wo das Recht an der eigenen Identität liegt, wird in Diskussionen um die Regulierung des Netzes definiert.

Für dieses Jahrhundert zeichnet sich ein Ende der Ideologien ab. Die Frage lautet: “Wie definieren wir in Zukunft Demokratie und welche Rolle hat Freiheit in dieser Definition?” Die Weichen für die Antworten der nächsten Jahrzehnte stellen wir jetzt.

Um als Gesellschaft diesen Wandel mitzugestalten, fehlen uns immer noch jegliche, politische Strukturen. Bereits bestehende Gremien haben weder das notwendige Know-How, noch den benötigten Einfluss um langfristige Rahmensetzungen zu entwickeln und durchzusetzen. Auch dieser Mangel ermöglicht, dass staatliche Stellen die Verantwortung für Überwachungsskandale von sich weisen können. Viele Entscheidungen aus dem netzpolitischen Bereich werden oft scheinbar uninformiert getroffen oder es wird abgewartet, was dazu auf EU-Ebene entschieden wird.

NEOS spricht sich für die Implementierung eines_r Netzminister_in ebenso wie für einen ständigen Ausschuss “Netzpolitik” im Nationalrat aus. So können die Kompetenzen gebündelt werden, Österreich kann endlich als starker Player in der EU und international Netzpolitik mitgestalten und der digitale Wandel wird nicht weiter verschlafen.

2. GRUNDLAGEN

2.1. Internet Governance

Die zentrale Verwaltung des Internet gehört reformiert. Die sich aus der Gründung des Internet ergebene Vormachtstellung der USA abgeschafft. Hierbei ist es wichtig, dass sich alle Beteiligten auf ein neues Modell verständigen.

Wichtige Kriterien dabei sind die Beibehaltung des Multi-Stakeholder-Ansatzes, die Festlegung von kohärenten, globalen und den Grundrechten und demokratischen Werten entsprechenden Grundsätzen. Weiters ist dabei die Festlegung einer klaren Rollenverteilung im Interesse eines offenen, freien Internet von Bedeutung. Die Stabilität und Sicherheit des Domänennamenssystems soll durch eine Kooperation aller Akteure bei der Globalisierung der IANA (Internet Assigned Numbers Authority) erreicht werden.

2.2. Netzneutralität

Netzneutralität bedeutet, dass jedes Datenpaket, unabhängig von Absender, Empfänger, Tarif oder Dienst technisch und ökonomisch gleich behandelt werden muss. Sie ist eines der wichtigsten Prinzipien des freien Internets, und von fundamentaler Bedeutung für die Erhaltung der gesellschaftlichen und wirtschaftlichen Entwicklung.

Seit Jahren versuchen Internetprovider neben dem klassischen Netzzugang sogenannte „Specialised Services“ zu vermarkten. Die in der aktuellen politischen Diskussion ungenau geführte Definition dieser „Specialised Services“ droht in ein Zwei-Klassen-Internet zu münden, wobei manche Dienste priorisiert und andere gebremst werden.

NEOS bekennt sich zur Erhaltung der Netzneutralität. Specialised Services sind aus unserer Sicht nur dann zulässig, wenn diese komplett getrennt vom Internet angeboten werden und die Qualität des Internets nicht beeinträchtigen. Die Definition der Specialised Services ist derart zu treffen, dass jede Auslagerung von Diensten des offenen Internet auf diese Spezialdienste unmöglich ist.

Darüber hinaus muss jeder Internetanschluss eine uneingeschränkte Teilnahme am Netz hinsichtlich Dienste-Nutzung und Dienste-Bereitstellung ermöglichen.

NEOS begrüßt, dass die EU im Zuge der Verhandlungen zur Globalisierung der IANA mit einer Stimme sprechen will.

2.3. Open Source

Open Source ist Software, deren Quelltext offen liegt. Durch den offenen Quelltext kann jede_r genau nachvollziehen wie ein Programm arbeitet, anstatt sich auf die Behauptung der Herstellerfirma zu verlassen. Open Source führt damit zu mehr Kontrolle und Transparenz auf der Nutzerseite und Unabhängigkeit gegen über einzelnen Herstellern.

NEOS spricht sich für einen verstärkten Einsatz von Open Source Software in der Verwaltung und im Bildungswesen aus.

2.4. Open Data

Informationen und Daten, die in öffentlichen Institutionen gesammelt werden, sollten grundsätzlich allen Bürger_innen, die diese schließlich auch als Steuerzahler_innen finanzieren und ermöglichen, zugänglich sein.

Eine Veröffentlichung solcher Datensätze ist kein nachträglicher Schritt, sondern sollte für Behörden selbstverständlich sein und im Betriebsablauf verankert werden. Ein einfacher Zugriff sorgt nicht nur für Transparenz, er ermöglicht auch Anwendungen, die nicht im Aufgabenbereich der ursprünglichen Auftraggeber liegen und daher ohne Zurverfügungstellung für Dritte nicht stattfinden würden.

Bereits bestehende Open Data-Angebote zeigen die Möglichkeit und den Willen, diese Datensätze in kreativen, neuen Wegen zu verwenden und durch deren Aufarbeitung und Kombination einen Mehrwert für die Bevölkerung entstehen zu lassen.

NEOS fordert eine Verpflichtung zur Veröffentlichung von Datensätzen, mit Ausnahme von personenbezogenen Informationen, durch öffentliche Stellen. Nicht-zugängliche Daten sollten nicht mehr Standard, sondern die Ausnahme sein. Um eine entsprechende Nutzung

und automatisierte Verarbeitung zu ermöglichen ist es nötig, dass diese Daten in maschinenlesbarer Form unter einer freien Lizenz wie Creative Commons CC-BY oder gemeinfrei zur Verfügung gestellt werden. Hierzu müssen offene Standards bei den Schnittstellen und der Software verwendet werden, um den Verwaltungsaufwand zu minimieren und Transparenz und Partizipation zu ermöglichen. Die dafür nötigen offenen Standards wurden bereits von der *Verwaltungskooperation Cooperation OGD Österreich* (http://www.ref.gv.at/Veroeffentlichte-Informationen.2774.0.html) erarbeitet.

2.5. Informationsfreiheit

Im Bereich der Informationsfreiheit ist ein Paradigmenwechsel in Österreich längst überfällig: vom Amtsgeheimnis zum Grundrecht auf Zugang zu Information. Nur so wird staatliches Handeln für alle Bürgerinnen und Bürger transparenter und offener.

Die genaue gesetzliche Ausgestaltung eines solchen Informationsfreiheitsgesetzes darf insbesondere nicht am österreichischen föderalistischen System scheitern; es bedarf einer bundeseinheitlichen Regelung, um der Gefahr vorzubeugen, dass es insbesondere durch unterschiedliche Ausnahmeregelungen in den Bundesländern zu unterschiedlichen Ausgestaltungen des Rechts auf Information kommt. Diese Uneinheitlichkeit würde nämlich auf eine Schwächung der geforderten Transparenz hinauslaufen. Generell müssen Ausnahmetatbestände zwingend und eng formuliert sein, wobei auch eine Pflicht zur Abwägung zwischen diesen Ausnahmen und dem Recht auf Zugang zu Information vorzusehen ist.

Zur besseren Durchsetzung des Rechts auf Zugang zu Information ist zudem eine unabhängige Behörde (Informationsfreiheitsbeauftragte/r) notwendig, da diese Behörde abwägen kann, ob das Recht auf Information oder das Recht auf Privatsphäre und Datenschutz überwiegt und ob das, was passiert ist, von hohem Interesse ist und es rechtfertigt, dass Unternehmensdaten herausgegeben werden müssen.

Eine vergleichbare Regelung soll auch auf EU-Ebene geschaffen werden.

2.6. Netzsperren und Zensur

Netzsperren werden in der politischen Diskussion hauptsächlich im Zusammenhang mit der Bekämpfung von Kinderpornographie und Urheberrechtsverletzungen angeführt. Netzsperren sind aber kein geeignetes Steuerinstrument, denn sie bewirken lediglich, dass der gesperrte Inhalt der Wahrnehmung mehr oder weniger entzogen wird, aber nach wie vor verfügbar ist. Auch sind Netzsperren technisch oft zu umgehen und schaffen eine Zensurinfrastruktur, die auch auf andere, eigentlich legale Bereiche, ausgeweitet werden könnte.

Wir anerkennen das Problem von gewerbsmäßigen Urheberrechtsverletzungen. Für NEOS gilt das wirksame Prinzip „löschen statt Sperren“ von illegalen Inhalten (*Löschbericht Kinderpornografie des dt. BMJ/BMI vom 13.02.2014, nach maximal 4 Wochen, Löschquote 97%*). Darüber hinaus meinen wir, dass die technische Infrastruktur eines freien und offenen Internets nicht durch Gesetzesentwürfe eingeschränkt werden darf. Wir lehnen jede Form von Zensur ab.

2.7. Konsument_innenschutz & Jugendschutz

Der Schutz von Konsument_innen erschöpft sich nicht allein im Schutz und der Sicherheit ihrer Daten oder Maßnahmen wie dem “Recht auf Vergessen(werden)”. Um eine fundierte Entscheidung treffen zu können, müssen Konsument_innen entsprechend und so transparent wie möglich informiert werden.

So sind Nutzungsbedingungen oft zu juristisch geschrieben und sollten für durchschnittliche Nutzer_innen leichter verständlich gestaltet werden. Dies kann beispielsweise durch eine Gegenüberstellung von juristischer Version und leicht verständlicher Version, oder visuell durch Symbole geschehen.

Jugendschutz im Internet ist wichtig, darf aber nicht zur Einschränkungen von eigentlich legalen Inhalten für alle Menschen führen. Es gibt bereits vielfältige Angebote, z.T. auch mit staatlicher Unterstützung, die ein sicheres und altersgerechtes Surfen für Kinder und Jugendliche ermöglichen. Dazu gehören Whitelists (weiße Listen/Positivlisten), die entsprechende Internetseiten oder Apps auflisten, welche für Kinder und Jugendliche

besonders geeignet sind. Weiters müssen Eltern und auch Bildungsinstitutionen in die Pflicht genommen werden und bei allen Beteiligten sinnvolle und altersgerechte Aufklärungsarbeit leisten.

Zahlreiche Informationsangebote stehen dazu bereit, auch hinsichtlich der Förderung von Medienkompetenz aller Beteiligten (vgl. auch den folgenden Punkt "Bildung & Recht auf Teilhabe"). Eltern sollten sich hier, genau wie sie es auch offline tun, einen Überblick über den Umgang ihrer Kinder online schaffen und die dazu genutzten Geräte entsprechend einstellen und sichern.

Hinsichtlich möglicher Gefahren, wie beispielsweise Cyber-Grooming (gezieltes Ansprechen von Minderjährigen durch Erwachsene im Internet mit dem Ziel der Anbahnung sexueller Kontakte), ist eine Sensibilisierung der Kinder, Eltern und Bildungsinstitutionen wichtig, insbesondere was Prävention und rechtliche Möglichkeiten betrifft.

2.8. Bildung & Recht auf Teilhabe

Die Kenntnis der neuen Medien umfasst nicht bloß die reine Bedienung, sondern auch das tiefergehende Verständnis dieser. Wichtig ist es NEOS dabei vor allem auch auf die großen Chancen einer vernetzten Gesellschaft hinzuweisen, anstatt nur auf die Gefahren zu zeigen.

Ein breit gefächertes und generationenübergreifendes Bildungsangebot ist dazu notwendig, dies ist auch bei der Aus- und Weiterbildung von Lehrkräften zu beachten. Vermittlung von Medienkompetenz und grundlegenden technischen Zusammenhängen sollte heute genauso selbstverständlich sein wie Lesen und Schreiben. Um dies zu erreichen müssen schon in der Schule weitgehende Grundlagen gelegt werden. Darunter fallen zum Beispiel Internet Governance und der Umgang mit persönlichen Daten. Lehrkräfte sind darauf und auf den Einsatz von neuen Medien allgemein in der Aus- und Weiterbildung entsprechend vorzubereiten.

Es reicht aber nicht nur die Jungen miteinzubeziehen, auch die vorhergehenden Generationen müssen mitgenommen werden. Daher müssen über die unterschiedlichen Bildungsträger zielgruppenspezifische Kurse angeboten werden.

Auch für Menschen mit Beeinträchtigungen muss eine Partizipation möglich sein. Barrierefreiheit, einfache Sprache und digitale Angebote zur Unterstützung dieser Gruppe sind hier neben technischen Hilfsmitteln, wie z.B. speziellen Tastaturen, wichtige Punkte, bei denen vor allem auch die jeweiligen Seitenanbieter_innen in der Pflicht sind. Staatliche Stellen müssen hier mit gutem Vorbild vorangehen, Österreich hat sich auch schon zu den WAI-Leitlinien verpflichtet. Digitale Inklusion sollte sich aber nicht nur darauf beschränken, sondern insbesondere auch die Medienkompetenz von Menschen mit Beeinträchtigungen fördern, damit eine Teilhabe an der digitalen Gesellschaft für alle möglich wird.

Die Teilhabe an neuen Medien ist nur möglich, wenn der technische Zugang gegeben ist, auch durch mehr öffentliche Hotspots und Zugangsmöglichkeiten, und alle gesellschaftliche Schichten und Generationen vollständig damit umgehen können. Lebenslanges Lernen wird auch vor diesem Hintergrund noch einmal wichtiger.

3. DATENSCHUTZ & BÜRGER_INNENDATEN

Maßnahmen, die die Freiheit der Menschen beschränken, müssen immer dahingehend geprüft werden, ob sie zur Problemlösung überhaupt

1. notwendig und
2. geeignet sind und auch, ob sie als Eingriff in die Selbstbestimmung der Menschen
3. verhältnismäßig zu
4. real existierenden Problemen stehen, d.h. überhaupt einen legitimen Zweck befolgen.

Diese Abwägung hat in jedem Einzelfall und immer wieder auch nachträglich zu geschehen, um ihre Verhältnismäßigkeit zu überprüfen und so insbesondere systematische Beschränkungen zu verhindern.

Denn für NEOS gilt: Im Zweifel für die Freiheit.

3.1. Social Networks

Social Media und andere Plattformen im Internet sind für viele Menschen zum festen Bestandteil des Lebens geworden. Das "Einschließen" von Daten hindert Nutzer_innen aber daran, den Plattformanbieter schnell und unkompliziert zu wechseln und hemmt den Wettbewerb zwischen den Plattformen. Offene und freie Standards sind daher notwendig, da sie eine Portabilität der Daten ermöglicht. Auch muss sichergestellt sein, dass Nutzer_innen ihre Daten jederzeit unmittelbar und unwiederbringlich löschen können sowie diese selbstverständlich vollumfänglich bei den Betreibern der Plattformen anfordern können. Die Datenhoheit muss bei den Nutzer_innen liegen!

3.2. Informationelle Selbstbestimmung

Das Grundrecht auf informationelle Selbstbestimmung gewährleistet das Recht des Einzelnen grundsätzlich über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Es muss also weiterhin einen Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten geben.

Die Auskunftsrechte der Nutzer_innen gegenüber den Anbietern sind zu stärken. Anbieter sollen in verständlicher Sprache, kostenfrei und möglichst schnell mitteilen, welche Nutzer_innendaten sie in welchen Kontexten verarbeiten und diese auf elektronischem Wege aushändigen.

3.3. Anonymität, Pseudonymität und Klarnamenpflicht

Ein Recht auf eine anonyme Nutzung des Internets ist die Grundlage für die freie Meinungsäußerung und Teilhabe. Dazu gehört auch die dynamische Vergabe von IP-Adressen. Nur durch eine anonyme Nutzung können auch unliebsame Vorgänge veröffentlicht und gelesen werden (Whistleblowing, Oppositionsbewegungen).

Eine anonyme/pseudoanonyme Nutzung des Netzes hat in unserer Gesellschaft auch ein hässliches Gesicht: in sog. Shitstorms entlädt sich der geballte Unmut einzelner. Auch wenn das Diskussionsniveau aller Beteiligten nicht das Maß erreicht, dass man sich in öffentlichen Debatten erwartet, so ist deshalb eine Aufhebung der Anonymität, also eine Klarnamenpflicht, der vollkommen falsche Weg.

Technische Lösungen sind für NEOS keine Lösung gesellschaftlicher Spannungen.

3.4. Cookies

Cookies können zur Bildung von anbieter-übergreifenden Nutzungsprofilen genutzt werden, daher ist eine klare und umfassende Information über den Speicherungszweck von Seiten der Diensteanbieter gegenüber den Nutzer_innen wichtig, wie es auch in der EU-Richtlinie (2009/136/EH) festgeschrieben ist. Es liegt ein hohes Gefährdungspotential für die Persönlichkeitsrechte der Nutzer_innen vor. Ein Explizites Nutzer-Opt-in, also eine ausdrückliche Zustimmung zur Cookie-Nutzung auf der besuchten Seite selbst, ist daher wichtig und sollte auch nutzerfreundlich gestaltet sein (bspw. durch eine Leiste am Seitenbeginn).

Eine Zustimmung der Nutzer_innen über Browsereinstellung bzw. nur ein Verweis in den Nutzungsbedingungen der besuchten Seiten ist hingegen zu versteckt und intransparent.

Die Information über das, was genau die Cookies jeweils beinhalten, muss ebenso transparent, vollumfänglich und verständlich dargelegt sein, damit Nutzer_innen auch tatsächlich eine informierte Entscheidung treffen können. Das betrifft auch den Hinweis darüber, ob Informationen verknüpft werden, wie dies beispielsweise bei Social Media Einbindungen auf der Seite eines anderen Anbieters der Fall sein kann.

3.5. Verschlüsselung/Kryptographie

Die Möglichkeiten zur Verschlüsselung von Online-Kommunikation oder Dateien sind vielfältig und werden insbesondere nach den Snowden-Enthüllungen verstärkt von Privatpersonen genutzt, ebenso Netzwerke zur Anonymisierung von Verbindungsdaten wie Tor. Auch Unternehmen nutzen Kryptographie, um ihre sensiblen Daten und Betriebsgeheimnisse zu schützen.

Da diese Methoden aber ebenso von Kriminellen und Terrorist_innen genutzt werden können befürchten manche, dass dies eine effektive Verfolgung durch Nachrichtendienste und Strafverfolgungsbehörden verhindert. Daher fordern Regulierungsbefürworter neben einem generellen Verbot bspw. eingebaute “Hintertüren” in Verschlüsselungs-Programmen, “schwache” Verschlüsselung durch Begrenzung der Schlüssellänge oder die Hinterlegung von Schlüsseln in einer weltweiten Infrastruktur.

NEOS lehnt ein Verschlüsselungsverbot oder eine Einschränkung in diesem Bereich klar ab. Jeder Mensch hat das Recht auf die Achtung seiner Privatsphäre, Brief- und Fernmeldegeheimnis haben als Grundrechte Verfassungsrang. Diesen Grundrechten kann durch Verschlüsselung Geltung verschafft werden. Auch würde durch eine Aufweichung der Verschlüsselungssicherheit der angestrebte Schutzzweck ad absurdum geführt - ein Abhören oder Eindringen von krimineller Seite wäre nun erheblich einfacher möglich.

3.6. Recht auf Vergessen(werden)

Im Mai 2014 hat der EuGH mit einem Urteil das „Recht auf Vergessenwerden im Netz“ geschaffen. Das Urteil weist Google und andere Suchmaschinenbetreiber an, Suchergebnisse im Zweifel zu löschen, wenn Persönlichkeitsrechte von Privatpersonen betroffen sind. Die betroffene Person muss dazu einen Antrag auf Löschung an die Suchmaschine stellen. Diese muss prüfen, ob die Löschung berechtigt ist. Es geht also im Kern um die Abwägung zwischen zwei Grundrechten: Persönlichkeitsrecht vs. Informations- und Meinungsfreiheit.

NEOS sieht ein „Recht auf Vergessenwerden“ grundsätzlich positiv. Durch das Urteil hat der EuGH das Recht der privaten Nutzer_innen auf Schutz ihrer Privatsphäre und ihrer personenbezogenen Daten gestärkt und eine Art „Recht auf zweite Chance“ geschaffen.

Privatpersonen sollen nicht ihr Leben lang mit einem negativen Ereignis in Verbindung gebracht werden. Die Informations- und Meinungsfreiheit wird durch das Urteil nicht im Kern verletzt, da sie zum einen bei der Abwägung des Löschantrags beachtet wird und zum anderen die Löschung nur die Suchergebnisse, nicht den Seiteninhalt selbst betrifft. Auch wird nicht über den Inhalt selbst entschieden, sondern darüber, ob die Fakten noch relevant, nicht mehr aktuell oder sehr privat sind. Die Abwägungsgründe sind hier relativ detailliert und es sind jeweils Einzelfallentscheidungen.

Allerdings gibt es auch berechtigte Kritik an der aktuellen praktischen Auslegung des Urteils und NEOS sieht gesetzgeberischen Handlungsbedarf in einigen Punkten: Die Löschung gilt absurderweise nur für alle EU-Domains der Suchmaschine, nicht aber weltweit. Es ist auch nicht klar, wann und in welchem Umfang Webmaster, deren Link gelöscht wurde, informiert werden darf.

Ebenso muss geregelt werden, dass Inhaltsverantwortliche früher beteiligt werden können und Gelegenheit zur Stellungnahme bekommen müssen, um den Sachverhalt in manchen Fällen besser und umfassender aufklären zu können. Eine freiwillige, unabhängige Schlichtung nach einer ablehnenden Entscheidung der Suchmaschine wäre sinnvoll, um die Beschwerde für Betroffene möglichst niedrigschwellig möglich zu machen und neben dem bereits bestehenden Gerichtsweg und der Möglichkeit, sich an die Datenschutzaufsicht zu wenden, einen weiteren Weg zu eröffnen.

Insgesamt sollte im Zweifel zugunsten der Privatperson entschieden werden. Auch sollte die Transparenz so hoch wie möglich sein!

3.7. EU-Datenschutzverordnung

Datenschutz ist ein Grundrecht. Aktuell ist der Datenschutz in den Mitgliedsstaaten sehr unterschiedlich geregelt. Die nationalen Datenschutzgesetze basieren auf einer Richtlinie aus dem Jahr 1995. Mit einer neuen EU Datenschutzgrundverordnung soll das bestehende unterschiedliche Datenschutzniveau durch ein einheitliches, modernes europäisches Datenschutzrecht ersetzt werden.

NEOS unterstützt die Bestrebungen zur Schaffung eines einheitlichen europäischen Datenschutzrechts, basierend auf hohen Standards. Diese neuen Standards sollen immer dann gelten, wenn Daten den Ursprungsort Europa haben, unabhängig davon, ob diese Verarbeitung innerhalb oder außerhalb der EU geschieht.

Darüber hinaus soll sich Österreich und die EU dafür stark machen, ein möglichst hohes Datenschutzniveau auch im Zuge von Verhandlungen mit Staaten außerhalb der EU zu erreichen.

3.8. SWIFT-Abkommen

Das sogenannte SWIFT-Abkommen erlaubt den USA Zugriff auf Kontoinformationen über in der EU ansässige Finanzdienstleister zum Zweck der Terrorismusbekämpfung. Zwar sind die Gründe, unter denen eine Einsicht möglich ist, streng eingegrenzt, eine Kontrolle der Einhaltung jedoch schwer und kaum Informationen über die Anwendung des Abkommens öffentlich. Jede Anfrage muss von Europol auf Rechtmäßigkeit überprüft und stattgegeben werden, Berichte werden jedoch nicht veröffentlicht, betroffene Kontoinhaber_innen nicht in Kenntnis gesetzt. Die spärlichen in der Vergangenheit gewährten Einblicke lassen sowohl Zweifel an Nutzen als auch am verantwortungsvollem Umgang mit diesem Instrument aufkommen.

NEOS spricht sich grundsätzlich und auch im speziellen Fall des SWIFT-Abkommens gegen Generalüberwachungsmaßnahmen aus. Anstatt Behörden, speziell solchen von Drittstaaten, Zugriff auf bestehende Datenbanken zu gewähren ist eine Zusammenarbeit

mit lokalen Strafverfolgungsbehörden zu bevorzugen. Diese Zusammenarbeit hat unter Einhaltung geltenden Rechts und demokratisch legitimierter Ermittlungsmaßnahmen stattzufinden. Auf diese Weise können Missbrauch und durch Sicherheitslücken bedingte unrechtmäßige Zugriffe besser verhindert und Rechenschaftspflichten besser nachgekommen werden.

3.9. Safe Harbor

Die europäische Datenschutzrichtlinie sieht vor, dass ein Datentransfer in Drittstaaten, die über kein dem EU Recht vergleichbares Datenschutzniveau verfügen, verboten ist (*Art.25 und Art.26 der Europäischen Datenschutzrichtlinie*). Dies trifft eigentlich auch auf die USA zu, da es dort keine umfassenden gesetzlichen Regelungen gibt, die dem Datenschutzstandard in Europa entsprechen. Allerdings ermächtigt die europäische Datenschutzrichtlinie die Kommission, die Angemessenheit des Datenschutzes in einem Drittland festzustellen, wenn dieses bestimmte Anforderungen erfüllt (*Art.25 Abs.6 der Europäischen Datenschutzrichtlinie*).

Safe Harbor ist ein Abkommen der EU mit den USA, die es europäischen Unternehmen trotzdem ermöglicht, personenbezogene Daten legal an US-Unternehmen zu übermitteln, sofern diese sich zu den „Grundsätzen des sicheren Hafens“ verpflichten. Es bestehen allerdings berechtigte Zweifel ob die Datenhaltung der meisten US Unternehmen Europäischen Datenschutzstandards überhaupt genügt.

Den sicheren Datenhafen gibt es nämlich de facto nicht, denn nach den Bestimmungen des USA PATRIOT Act können US amerikanische Geheimdienste ohne richterliche Anordnung auf die Daten aller US-Unternehmen zugreifen. Dies betrifft auch die Daten aller ausländischen Tochterunternehmen.

NEOS fordert die sofortige Beendigung des Safe Harbor-Abkommens mit den USA. Den sicheren Hafen gibt es dort nicht, da in Europa übliche Datenschutzstandards nicht im Ansatz gewährleistet werden, wenn NSA und andere Geheimdienste umfassend und anlasslos auf personenbezogene Daten zugreifen, die im Rahmen dieses Abkommens an die USA übermittelt werden.

3.10. PNR (Passenger Name Record)

PNR umfasst die Daten, die von Passagieren bei Flügen angegeben werden. Es sind dies Name, Alter, Adresse, Bezahldaten sowie Flugroute und eventuelle Speisewünsche. Fluggesellschaften verwenden die Daten für kommerzielle Zwecke. Mit den USA und weiteren Ländern gibt es bereits solch eine Vereinbarung, dass diese Daten von EU-Bürger_innen gespeichert werden dürfen. Ebenso wird in der EU ein solches Abkommen für die EU selbst diskutiert. Das EU-Parlament hat mit Mehrheit beschlossen, eine EU-Richtlinie bis Jahresende 2015 auszuarbeiten. Durch diese EU-Richtlinie sollen diese Daten dann auch innerhalb der EU erfasst und für Strafverfolgungszwecke verwendet werden dürfen.

Es gibt bereits ein transatlantisches Abkommen, welches den USA (und weiteren Ländern wie Australien) ermöglicht, die Daten 15 Jahre zu speichern. NEOS steht PNR grundsätzlich ablehnend gegenüber. Es stellt sich hier die Frage nach der Verhältnismäßigkeit dieser riesigen Datenbank, ebenso wie nach der Notwendigkeit. Rasterfahndung und Erstellung von personenbezogenen Profilen ist so problemlos möglich. Ein automatischer Datenabgleich mit Gefahrenprofilen ebenfalls. Die Unschuldsvermutung wird ausgehebelt und anlasslos und massenhaft Daten unbescholtener Bürger_innen erfasst.

NEOS will daher die bestehenden Formen abschaffen und kein neues „EU-PNR“ einführen.

3.11. Vorratsdatenspeicherung

Die Vorratsdatenspeicherung ist ein massiver Eingriff in die Privatsphäre der Bürger_innen. Die umfassende und anlasslose Aufzeichnung und Speicherung von Telekommunikationsdaten stellt de facto einen Pauschalverdacht gegenüber der Allgemeinheit dar und lässt Zweifel am Prinzip der Unschuldsvermutung aufkommen. Darüber hinaus sind das Recht auf Privatleben und der Schutz personenbezogener Daten Grundrechte der EU (Vgl. Art.7 und Art.8 Charta der Grundrechte der Europäischen Union).

NEOS ist klar gegen die anlasslose Massenüberwachung durch die Vorratsdatenspeicherung und begrüßt daher deren Aufhebung durch den EuGH und österreichischen VfGH. Die Urteilsbegründungen sind als Leitlinien im gesamten

Gesetzgebungsprozess zur Verfassungskonformität anderer Überwachungsgesetze zu berücksichtigen.

Eine Neuauflage einer derartigen Vorratsdatenspeicherung stellt für uns kein probates Mittel dar. Eine mögliche Alternative, um einen Ausgleich zwischen den Grundrechten auf Freiheit und Sicherheit zu ermöglichen, kann das Quick Freeze-Verfahren sein. Allerdings nur, solange deren Grenzen bzgl. Personen, Dauer und sonstiger Parameter so eng wie möglich definiert ist und ein Zugriff der Ermittlungsbehörden letztendlich nur mit Richtervorbehalt möglich ist. Ebenso müssen Benachrichtigungspflichten der Betroffenen im Nachhinein geprüft werden, genauso wie zuallererst die Notwendigkeit einer zusätzlichen Maßnahme nachgewiesen werden muss.

4. INFRASTRUKTUR

4.1. Breitbandversorgung

Für den Ausbau der Informationsgesellschaft sowie das wirtschaftliche Wachstum in Europa ist eine flächendeckende Breitbandversorgung eine wichtige Voraussetzung. Obwohl die Anzahl der Breitbandanschlüsse in Europa stark zunimmt, besteht weiterhin eine digitale Kluft zwischen städtischen Ballungszentren und ländlichen Gebieten. Oftmals fehlen in den ländlichen Gebieten aufgrund des mangelnden Mitbewerbs Anreize, weiter in den Ausbau der Telekommunikationsnetze zu investieren.

Für NEOS ist eine europaweite Breitbandversorgung ein elementarer Infrastrukturbestandteil. Hierbei gilt es eine intelligente Kombination von Mobilen- und Festnetzen auszubauen, wobei die Frage nach der Definition von Breitband in Beziehung zur jeweiligen Region zu beantworten ist. Ein lebendiger Wettbewerb ist die stärkste Triebfeder für den Netzausbau. In diesem Sinne ist eine Trennung von Netzbetreiber und Internet-Diensteanbieter ein befürwortenswertes Konzept.

4.2. Internet der Dinge

Mit der Einführung des Internetprotokolls Version 6 können potentiell ungefähr 340 Sextillionen Adressen vergeben werden. Dies stellt eine wichtige Grundlage für das Internet der Dinge (IoT, Internet of Things), also beispielsweise vernetzte Häuser, Autos, Gebrauchsgegenstände, etc. dar. Aber auch die Infrastruktur muss darauf ausgelegt sein, Stichwort Breitbandausbau.

Die Kommunikation zwischen den Dingen, ohne zwingende Einbeziehung von Menschen, wie beispielsweise zwischen Auto und Ampel, beinhaltet auch eine gewisse Art des menschlichen Kontrollverlusts. Das Internet der Dinge wirft viele ethische Fragen auf und fordert eine gesamtgesellschaftliche Diskussion und Betrachtung, neben den zahlreichen rechtlichen Fragen, die noch geklärt werden müssen. IoT bietet große Chancen für die

Gesellschaft und Unternehmen, aber es ist auch wichtig, für potentielle Gefahren so früh wie möglich rationale Vorkehrungen zu treffen.

Gerade weil durch die neuen Systeme und Gegenstände viele, zum Teil sehr persönliche Daten der Menschen gesammelt werden, ist die Robustheit der Systeme ein wichtiger Punkt. Sicherheitsstandards für die Aufbewahrung müssen entwickelt werden, Übertragung der Daten sollten nur Ende-zu-Ende verschlüsselt stattfinden und ggf. anonymisiert werden.

Die rechtlichen Voraussetzungen sind allerdings in vielen Bereichen noch unklar, insbesondere im Bereich Datenschutz. Zur Strafverfolgung sollten für diese Daten die gleichen Bestimmungen wie für andere persönliche Daten gelten. Bei der Aufbewahrung und Verarbeitung der Daten ist Transparenz für die Nutzer_innen elementar. Bei ihnen muss auch die Kontrolle der Daten liegen. Sie sollten diese jederzeit unkompliziert und umfassend auslesen sowie unwiederbringlich löschen, ebenso wie die Datenerhebung gänzlich ein- und ausstellen können. Eine Verknüpfung mit anderen persönlichen Daten darf ausschließlich als explizites Opt-in erfolgen. Begehrlichkeiten hinsichtlich der Daten durch Unternehmen und staatliche Stellen gehört ein Riegel vorgeschoben, um Profiling zu verhindern. Dazu gehören beispielsweise Krankenkassen, die ein Interesse an den Daten des Fitnessarmbands haben, oder Versicherungen, die auf die Auto-Daten zugreifen wollen.

Optimal sind IoT-Lösungen, die sich an dem Prinzip Privacy by Design orientieren. Dieses Prinzip sollte sich als Standard etablieren. Es bedeutet, dass idealerweise die Gewährleistung von umfassendem Datenschutz direkt von Anfang an im Produktionsprozess mitgedacht wird. Die persönliche Kontrolle der Daten durch die Nutzer_innen kann bestmöglich erfolgen, wenn die 7 Grundprinzipien von Privacy by Design direkt von den Herstellern implementiert werden: Proaktive Präventionsmaßnahmen, Datenschutz als Standardeinstellung, Einbettung von Datenschutz in das Design, volle Funktionalität, Durchgängige Sicherheit während des gesamten Lebenszyklus der Daten, Sichtbarkeit und Transparenz sowie eine Nutzer_innenzentrierte Gestaltung. Solche datenschutzfreundlichen Vorkehrungen stellen für Unternehmen einen wichtigen Vorteil gegenüber anders agierender Konkurrenz dar.

Ein weiterer wichtiger Punkt, insbesondere hinsichtlich des Konsument_innenschutzes, sind einheitliche und möglichst offene Standards. Frei zugängliche Ansätze sind hierbei zu bevorzugen. Durch solche Standards wird Interoperabilität erst möglich, was auch den Wettbewerb fördert. So wird auch dem Problem vorgebeugt, das sich bei komplett geschlossenen Systemen für Konsument_innen stellt, falls der Anbieter irgendwann nicht mehr existieren sollte, oder sie sich in Teilen für einen anderen Anbieter entscheiden. Dies dient ebenfalls dem Umweltschutz, da so unnötiger Müll durch mangelnde Interoperabilität vermieden wird.

4.3. Cloud Computing

Durch immer größer werdende Datenmengen nutzen u.a. Unternehmen, NGOs, aber auch Privatpersonen verstärkt Cloud Dienste, um ihre Daten dort zu speichern. Dies kann dabei helfen, IT-Kosten zu senken sowie die Produktivität, das Wachstum und die Beschäftigung zu steigern. Gerade für mittelständische und junge Unternehmen aller Branchen bietet Cloud Computing große Vorteile, Regelungen sollten also auch für diese Gruppen praktikabel sein. Hier ist es wichtig, allen Nutzer_innen zuverlässige Cloud-Lösungen mit einem hohen Datenschutz- und Datensicherheitsniveau anzubieten, was ein wichtiger Schritt für den European Digital Single Market darstellen würde.

Handlungsbedarf besteht aber noch in vielen Bereichen, damit sich solche Lösungen nachhaltig entwickeln können. Probleme gibt es z.B. hinsichtlich unterschiedlicher nationaler rechtlicher Rahmenbedingungen, bestehender Rechtsunsicherheiten und vertraglicher Problemen (bspw. Bedenken in Bezug auf Datenzugang und –übertragbarkeit, Änderungskontrolle und Eigentum an den Daten). Cloud Computing wirft datenschutzrechtliche Bedenken auf, ebenso wie die Frage nach der Haftung und mögliche Urheberrechtsproblematiken.

Hinsichtlich eines Zugriffes durch öffentliche oder private Stellen sollen nicht-öffentliche Daten in der Cloud so behandelt werden, als würden sie sich auf der persönlichen Festplatte eines Gerätes des Nutzenden befinden. Privates muss auch in der Cloud privat bleiben!

Es ist wichtig, dass EU-einheitliche Regelungen im Bereich Cloud-Computing getroffen werden, die alle bestehenden Problematiken klären, Rechtssicherheit schaffen und den EU-Markt nicht fragmentieren.

Datenschutz kann hier als Wirtschaftsfaktor wirken: Dadurch wird der Standort Österreich bzw. EU bei hohen Datenschutzstandards attraktiv für Cloud-User und -Unternehmen. Zudem brauchen wir eine EU-weite Norm für technische Rahmenbedingungen der Clouddienstleistungen. Diese werden durch staatlich zertifizierte Stellen, die auch privat sein können, überprüft und für Nutzer_innen transparent gekennzeichnet.

4.4. E-Government und Bürger_innenbeteiligung

Österreich ist im Bereich E-Government auf einem guten Weg, muss diesen aber auch konsequent weiter verfolgen. Ziel sollte sein, dass alle Amtswege digital ermöglicht werden, aber zeitgleich auch die offline-Möglichkeiten erhalten bleiben. So ist sichergestellt, dass jede_r Bürger_in den Amtsgeschäften nachgehen kann. Wichtig sind höchstmögliche Sicherheitsvorkehrungen bei Übertragung und Speicherung der Daten, ebenso hinsichtlich des Zugriffs darauf. Ein sorgfältiges Lifecycle-Management der entsprechenden Zertifikate ist ebenfalls elementar. Bürger_innen sollten auch rechtzeitig über den Ablauf ihrer Zertifikate informiert werden.

Auch für eine stärkere Bürger_innenbeteiligung und größtmöglicher Transparenz staatlichen Handelns bietet das Internet viele neue Wege. Es sollten für Bürger_innen verstärkt Möglichkeiten eröffnet werden, Politik/Demokratie in neuen Formen und Formaten zu erleben und aktiv mitzugestalten. Innovative, dialogorientierte Formen sind hierbei wichtig, um einen differenzierten gesellschaftlichen Willensbildungsprozess gezielt zu unterstützen. Präsenzveranstaltungen und Onlinekommunikation sollten zu einer Informations- und Mitwirkungsplattform für Bürger_innen kombiniert werden. Demokratie-Innovation ist eines der Kernanliegen von NEOS, wozu sich auch in unseren „Plänen für ein neues Österreich“ viele weitere Punkte befinden.

5. SICHERHEIT

5.1. Cybersecurity

Innerhalb der europäischen Union bestehen derzeit große Unterschiede, was die Schaffung von Maßnahmen zur Erhöhung der Cyber Security betrifft. Spätestens seit den Enthüllungen des Whistleblowers Edward Snowden ist klar, dass es eines europäischen Gesamtansatzes zum Schutz der Netz- und Informationssicherheit in Europa bedarf. Dabei ist das Schwergewicht auf Prävention und Abwehrbereitschaft zu legen.

Der "Faktor Mensch" spielt dabei auch eine wichtige Rolle. Kompetenzen in Gesellschaft, Wirtschaft und Staat müssen hierzu ausgebaut werden. Möglich ist das bspw. durch interdisziplinäre Lehrstühle für IT-Sicherheit und regelmäßige Weiterbildung.

Aufgrund der gegenseitigen Abhängigkeit der Kommunikationsnetze und IT-Systeme wird die Netz- und Informationssicherheit der EU durch Mitgliedsstaaten mit niedrigem Schutzniveau in Summe geschwächt. Aus diesem Grund ist das in Art 5 des Vertrags über die Europäische Union festgeschriebene Subsidiaritätsprinzip angemessen. Die Mitgliedstaaten haben Notfallpläne auszuarbeiten, Computer Emergency Response Teams (CERT) aufzustellen und die innerstaatliche Zusammenarbeit und den Informationsaustausch sicherzustellen. Die Entwicklung und Einführung eines Europäischen Informations- und Warnsystems (EISAS) ist zu unterstützen.

NEOS sieht das Thema Cyber Security als Europäisches Thema. Nur ein einheitliches Handeln auf Basis einheitlicher Bestimmungen kann den Anforderungen an eine europäische Netz- und Informationssicherheit genügen. Dazu soll die Europäische Agentur für Netz- und Informationssicherheit (ENISA) als Einrichtung zur Zusammenarbeit genutzt werden.

Nahezu alle Infrastrukturbereiche sind von der IT abhängig. Diese Abhängigkeiten und die zunehmende Vernetzung der Infrastrukturen untereinander bergen neben den Chancen auch zahlreiche Risiken, wie die Tätigkeiten von außer- oder innereuropäischen Geheimdienstaktivitäten sowie kriminelle Aktivitäten im Netz.. Neben verpflichtenden technischen Mindeststandards (beispielsweise für die Verschlüsselung von

personenbezogenen Daten) sollen auch Vorgaben für eine sichere Implementierung von kritischen IT Systemen gelten.

In diesem Zusammenhang fordern wir, dass Verletzungen der europäischen Datenschutzrichtlinie sanktioniert werden müssen. NEOS unterstützt die Entstehung der neue Datenschutzverordnung, wobei das Recht auf den Schutz der persönlichen Daten als vorrangig anzusehen ist.

5.2. Nachrichtendienste

Österreich ist nach wie vor Ziel nachrichtendienstlicher Tätigkeiten anderer Staaten. Die österreichische Gesetzgebung sieht vor, dass nur nachrichtendienstliche Aktivitäten unter Strafe gestellt werden, die sich gegen Österreich richten (ausgenommen für militärische Zwecke). Wir fordern eine strafrechtliche Verfolgung sämtlicher nachrichtendienstlicher Aktivitäten auf österreichischem Staatsgebiet und weisen darauf hin, dass europäische und andere Nachrichtendienste sich an die in der EU geltenden gesetzlichen Grundlagen zu halten haben. Die Spionagetätigkeiten gegenüber einem souveränen Staat und seinen Bürgern und Bürgerinnen stellt einen schweren Eingriff in die Grund- und Freiheitsrechte dar. Dagegen ist mit allen zur Verfügung stehenden diplomatischen und strafrechtlichen Mitteln vorzugehen.

Spähprogramme wie „Tempora“ des britischen Nachrichtendienstes GCHQ oder PRISM der NSA sowie andere Programme verletzen das in Art. 7 und Art. 8 der Charta der Grundrechte der EU festgeschriebene Grundrecht auf Privatsphäre. Der Schutz der Grundrechte ist gegenüber allen anderen Maßnahmen der Vorrang zu geben.

Wir fordern die Offenlegung sämtlicher Zusammenarbeit europäischer und österreichischer Behörden mit ausländischen Nachrichtendiensten in den entsprechenden Gremien. Nur wenn dem Parlament oder anderen Kontrollinstanzen bekannt ist, in welchem Ausmaß solche Kooperationen stattfinden, kann eine demokratische Kontrolle geheimdienstlicher Maßnahmen erfolgen. Diese Kontrolle muss so ausgestaltet sein, dass sie tatsächlich dazu geeignet ist ihrer Aufgabe in vollem Umfang nachzukommen.

Die Kontrolle der nachrichtendienstlichen Aktivitäten hat nach dem Grundsatz “Gläserner Staat statt gläserner Bürger” zu erfolgen.

5.3. Videoüberwachung

Videoüberwachung gibt es in vielen Bereichen. Grundsätzlich sieht NEOS diese skeptisch. Eine „menschliche Lösung“, bspw. durch erhöhten Einsatz von Exekutivkräften oder Sicherheitspersonal, die ein direktes Eingreifen bei Problemen ermöglichen, sind stets zu bevorzugen. Bei Videoüberwachung im öffentlichen Bereich muss daher der Nutzen gründlich abgewogen werden, auch in regelmäßiger Form im Nachhinein. Dabei müssen auch mögliche Verdrängungseffekte beachtet werden.

Die Kennzeichnung einer Videoüberwachung im öffentlichen Raum ist unbedingt erforderlich und muss deutlich sichtbar sein. Auf der Kennzeichnung müssen alle wichtigen Informationen enthalten sein, beispielsweise die aufzeichnende Stelle inkl. Kontaktmöglichkeit, damit sich Betroffene dorthin wenden können. Diese Stellen müssen selbstverständlich ihrer Auskunftspflicht nachkommen.

Transparenz, klare Regelungen hinsichtlich der Aufzeichnung, Löschverpflichtungen sowie eine strenge Regelung, wer ein Zugriffsrecht auf die Aufzeichnungen hat sind ebenso elementare Punkte.

Auch bei Videoüberwachung von Privaten müssen strenge Regeln zum Schutz der Privatsphäre und Daten der betroffenen Personen selbstverständlich eingehalten werden.

NEOS unterstützt das in Österreich bestehende Verbot von sog. „Dashcams“ (Videokamera, die im Auto installiert ist und Bilder von der Straße vor dem Auto aufnimmt und aufzeichnet).

6. VERWEISE

6.1. Krypto-Währungen

Mit Bitcoin entstand 2009 ein völlig neuartiges Tauschmittel und Werttransfersystem, das weltweit immer mehr Verbreitung findet. Rund um Bitcoin und weitere Krypto-Währungen bilden sich auch immer mehr äußerst innovative Start-ups mit großem Wachstumspotenzial.

Unsere detaillierte Position zu Bitcoin und weiteren Krypto-Währungen wird in einem eigenen Positionspapier dargestellt.

6.2. Urheberrecht

Das Urheberrecht muss an das digitale Zeitalter angepasst werden. Fragen wie Privatkopievergütung und Urhebervertragsrecht müssen an das digitale Zeitalter angepasst und schrittweise auf europäischer Ebene harmonisiert werden.

Wichtig ist dabei, dass ein angemessener Ausgleich aller Interessen stattfindet, aber impraktikable Ideen wie ein Leistungsschutzrecht für Presseverleger nicht implementiert werden.

Unsere detaillierten Positionen dazu finden sich in einem separaten Positionspapier.