SOZIALDEMOKRATISCHE PARTEI DEUTSCHLANDS
DER PARTEIVORSTAND

SPD-Parteivorstand, Wilhelmstraße 141, 10963 Berlin

Berlin, 3. Mai 2019

Aktion Freiheit statt Angst
WPSEU 068/2019

1. Cyberkriminalität

Wie stehen sie zur Forderung nach mehr Datensparsamkeit?

Antwort:
Die Datenminimisierung ist als zentrales Prinzip in der DSGVO verankert und wird von den Sozialdemokratinnen und -demokraten vollumfänglich unterstützt.

Wie kann die Datenminimierung im Sinne der DSGVO gerade in Zeiten von Big Data durchgesetzt und gefördert werden?

Antwort:
Big Data stellt eine Herausforderung für den Datenschutz dar. Denn aus der Verknüpfung und Analyse einer Vielzahl von einzelnen Datensets lassen sich sehr genaue Profile von Menschen erstellen. Dieses Wissen kann gezielt missbraucht werden, sowohl für kommerzielle als auch für politische Zwecke. Big Data-Anwendungen können nur in den Grenzen der DSGVO erfolgen. Das beinhaltet neben dem Prinzip der Datenminimierung insbesondere auch strenge Anforderungen an die Rechtsgrundlage für eine Datenverarbeitung, gerade wenn es um besonders sensible Daten geht, etwa aus dem Gesundheitsbereich. Zudem müssen Datenverarbeitungsprozesse transparent sein und die Betroffenen umfassend informiert werden. Bei der Einhaltung dieser Datenschutzregeln im besonders sensiblen Bereich von Big Data kommt den nationalen Datenschutzaufsichtsbehörden eine entscheidende Rolle zu. Wir befürworten die enge Zusammenarbeit aller im digitalen Umfeld zuständigen Regulierungsbehörden, damit es zu mehr Synergien im Verbraucher-, Wettbewerbs- und Datenschutzrecht kommt (Digitales Clearinghouse). Zudem pochen wir Sozialdemokratinnen und -demokraten auf eine angemessene personelle und finanzielle Ausstattung der Aufsichtsbehörden. Ergänzend kann die Anwendung von Pseudonymisierungs-, Anonymisierungs- und Verschlüsselungstechniken für personenbezogene Daten die Risiken für die betroffenen Personen verringern.

SPD-Parteivorstand
Willy-Brandt-Haus
Wilhelmstr. 141
10963 Berlin

Fon 030 25991-500
Fax 030 25991-410
parteivorstand@spd.de
www.spd.de

SEB AG
Berlin
BLZ 100 101 11
Konto 1000 435 800

facebook.com/SPD
youtube.com/SPDvision
twitter.com/SPDde

2. Identitätsdiebstahl und Umkehrung der Unschuldsvermutung

Welche juristischen Möglichkeiten haben geschädigte Bürger zur ihrer Rehabilitation und zur Wahrung ihrer Menschenwürde?
Welche Instanzen planen Sie zu stärken, um Geschädigte und Opfer zu schützen?

Gemeinsame Antwort:
Identitätsmissbrauch bedeutet in der Regel einen massiven unbefugten Eingriff in das Datenschutzrecht der Rechteinhaber. Das hierfür erforderliche Abgreifen der personenbezogenen Daten (§ 42 Datenschutzgesetz) und / oder das Ausspähen gesicherter Daten (§ 202 StGB) ist strafbewehrt und wird mit bis zu drei Jahren Freiheitsstrafe geahndet. Im Rahmen der Strafverfolgung kann das Opfer nicht nur im moralischen Sinne Wiederherstellung des verletzten Rechts verlangen, sondern auch alle materiellen Schäden vom Täter ersetzt verlangen. Hierfür wollen wir, dass die Strafermittlungsbehörden technisch und personell gut ausgestattet sind. Den in Europa begonnen Weg zum Aufbau einer Europäischen Staatsanwaltschaft unterstützt wir und wollen Europol stärken.
In Deutschland soll zudem das Bundesamt für Sicherheit in der Informationstechnik eine zentrale Anlaufstelle werden für Verbraucherinnen und Verbraucher, die von Identitätsdiebstahl betroffen sind.

Durch welche Maßnahmen wollen Sie das Prinzip der Unschuldsvermutung stärken?

Antwort:
Mit dem Lissabonner Vertrags wurde auch die polizeiliche und justizielle Zusammenarbeit in Strafsachen, die bis dahin alleine auf Ebene des Rates der EU verhandelt wurde, auf europäischer Ebene vergemeinschaftet. Seither ist das Europäische Parlament auch in diesem Bereich zusammen mit dem Rat gleichberechtigter Gesetzgeber. In dieser Rolle hat das Europäische Parlament in den letzten zwei Legislaturperioden intensiv dazu beigetragen, das Recht auf ein faires Verfahren, inklusive des Rechts auf Unschuldsvermutung, deutlich zu stärken und somit die Sicherung der Rechte zu sichern, die unter anderem in den Artikeln 47 und 48 der Charta der Grundrechte der Europäischen Union und in Artikel 6 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten verankert sind.
Nach einem ersten Richtlinien-Paket zur Stärkung von Verfahrensrechten in der Legislaturperiode 2009-2014 (inkl. Recht auf Dolmetschleistungen und Übersetzungen, dem Recht auf Belehrung und Unterrichtung und dem Recht auf Zugang zu einem Rechtsbeistand), hat das Europäische Parlament in der Legislaturperiode 2014-2019 drei weitere wichtige Richtlinien verabschiedet, darin die Richtlinie zur Unschuldsvermutung und das Recht auf Anwesenheit in der Verhandlung sowie die Richtlinie über Verfahrensgarantien für Kinder in Strafverfahren und über Prozesskostenhilfe.
Mit der Verabschiedung der Richtlinie (EU) 2016/343 über die Stärkung bestimmter Aspekte der Unschuldsvermutung und des Rechts auf Anwesenheit in der Verhandlung in Strafverfahren im März 2016 konnten wir wichtige grundlegende Aspekte des Unschuldsvermutungsprinzips festhalten. Als Sozialdemokrat_innen haben wir uns insbesondere dafür eingesetzt, dass das Recht sich nicht selbst zu belasten, das Recht nicht mitzuwirken sowie das Aussageverweigerungsrecht deutlich gestärkt wurden. Gleichzeitig konnten wir mit der Richtlinie das Recht auf Anwesenheit in der Verhandlung ausbauen. Ein

weiteres wichtiges Anliegen der Sozialdemokrat_innen war es, sicherzustellen, dass eine Beweislastumkehr nur in Ausnahmefällen möglich ist, und dass Betroffene, im Falle einer Missachtung der ihnen zustehenden Rechte, über effektive Rechtsbehelfe verfügen.

3. Anonyme Kommunikation

Wie stehen Sie zur anonymen Internetnutzung und zur gesetzlichen Erhaltung derselben?

Antwort:
Die Möglichkeit zur anonymen Internetnutzung ist wichtig. Niemand sollte zur Verwendung des Klarnamens im Internet gezwungen werden. Auch sollte verschlüsselte Kommunikation zum Standard werden. Das kann nicht allein in der Verantwortung der Nutzer liegen. Vielmehr muss es verbindliche Standards für Anbieter geben.

Wie stehen Sie zu technischen Erweiterungen und der Erleichterung der Anonymisierung?

Antwort:
Die Möglichkeit zur anonymen Internetnutzung ist wichtig. Wenn technische Erweiterungen dies erleichtern, sind diese begrüßenswert.

Wie stehen Sie zu anonymen Zahlungsmitteln und der Bereitstellung anonymer Zahlweisen im Internet?

Antwort:
Wir Sozialdemokratinnen und -demokraten befürworten die Möglichkeit, Alltagsgeschäfte online auch anonym zu bezahlen. Über die bargeldlose Bezahlung ist das Erstellen von persönlichen Profilen möglich. Deswegen müssen Verbraucherinnen und Verbraucher in der Lage sein, bei Alltagsgeschäften online anonym zu bezahlen – in dem Rahmen, in dem dies auch bei Bargeldzahlungen möglich ist.

4. Smart Home und Haftungsfragen

Was werden Sie zur Stärkung von Verbraucherrechten in solchen Fällen tun?

Antwort:
Die neuen Richtlinien über bestimmte vertragsrechtliche Aspekte bei digitalen Inhalten und beim Warenhandel schaffen im Verbraucherrecht einen neuen Rechtsrahmen für Haftungsfragen. Dies war überfällig, weil das bisherig bestehende einmalige Austauschgeschäft über den Erwerb von Waren zunehmend an Bedeutung verliert und abgelöst wird von Nutzungs- und Servicevertragsverhältnissen mit Dauerschuldcharakter. Dadurch wird der traditionelle Gefahrübergang durch die Übergabe eines Produkts in Frage gestellt.

Mit der Verabschiedung der Richtlinie über vertragsrechtliche Aspekte bei digitalen Inhalten haben Software-Anbieter und Verkäufer von „smarten“ Produkten ab Oktober 2021 die Pflicht Softwareupdates für einen Zeitraum zu liefern, den Verbraucher und Verbraucherin vernünftigerweise erwarten und dies in einer Weise, dass die ursprüngliche Software auf einem solchen Stand erhalten bleibt, dass vernetzte Produkte solange funktionsfähig bleiben, solange auch das Gerät von seiner physischen Funktion her einsatzbereit ist.
Diese Regelung wurde aufgrund der Forderung von Sozialdemokraten und Sozialdemokratinnen in das neue Regelwerk aufgenommen. Denn wir sind der Ansicht, dass Softwareprogramme nicht fehlerfrei programmiert werden können. Deshalb spielen nachträgliche Sicherheitsupdates eine zentrale Rolle für die Nutzbarkeit von vernetzten Gegenständen und die Sicherheit des Internets. Dabei kommt den Softwareherstellern eine gesteigerte Verantwortung zu, weil nur sie über die Ressourcen und über die rechtlichen Möglichkeiten verfügen, Sicherheitslücken zu schließen.
Für die kommende Wahlperiode fordern wir zudem eine umfangreiche Reform der Produkthaftungsrichtlinie, die der zunehmenden Vernetzung, dem Einsatz von autonomen Systemen, dem 3-D-Printing sowie digitalen Dienstleistungen Rechnung trägt.
Deshalb müssen etwa der Anwendungsbereich, die Definition des Hersteller- und des Fehlerbegriffs, die Beweislast, geschützte Rechtsgüter und insbesondere die Zurechnung von mehreren Haftungsbeteiligten ebenfalls modernisiert werden.

Wie können Sie im Falle von eCall und (verpflichtenden) PKW-Telematiksystemen die informationelle Selbstbestimmung des Menschen schützen und gewährleisten?

Antwort:
Seit April 2018 müssen alle Neuwagen mit einem eCall-System ausgestattet sein. Befürchtungen, wonach mittels eCall der Überwachung der Autofahrer_innen Tür und Tor geöffnet werde, konnten wir durch intensive Beratungen ausräumen. eCall ist ein ruhendes Notrufsystem und wird ausdrücklich nur bei einem Unfall ausgelöst - Positionsdaten werden somit nur im Falle eines Notfalls an die zuständigen Behörden übermittelt. Auch bei weiteren Sicherheitssystemen, wie zum Beispiel beim Notbrems- oder Spurhaltesystem, konnten wir erreichen, dass diese der Europäischen Datenschutzgrundverordnung unterliegen und ausschließlich anonymisiert verarbeitet werden müssen.
So darf zum Beispiel beim Unfalldatenspeicher oder beim Aufmerksamkeitsassistenten in Zukunft kein Rückschluss auf den Fahrenden gezogen werden - die Daten werden anonymisiert.

Wer haftet im Falle eines Missbrauchs oder eines Softwarefehlers?

Antwort:
Derzeit müsste der Geschädigte nach der Produkthaftungsrichtlinie den Softwarefehler und den Kausalzusammenhang zwischen Fehler und Schaden beweisen.
Im Verbraucherrecht gilt dagegen spätestens ab Oktober 2021 eine Beweislastumkehr von einem Jahr gegenüber dem Verkäufer, wenn eine Software mangelhaft ist.
Eine gesamtschuldnerische Haftung mehrerer Hersteller oder beim Erwerb mehrerer Produkte, wie es beim Erwerb von smarten Gütern inzwischen die Regel ist, besteht nach geltendem Recht allerdings nur dann, wenn jeder Hersteller dem Grunde nach haftet.

Insbesondere im Falle von vernetzten Systemen verschiedener Hersteller kann die Fehlerhaftigkeit jedoch immer weniger lokalisiert werden.
Dementsprechend wird es zunehmend schwieriger Haftungsfragen zufriedenstellend zu klären. Dies macht die Einforderung von Schadensersatzansprüchen teilweise unmöglich.

Wer sollte Ihrer Meinung nach haften?

Antwort:
In Zukunft sollte der Vernetzung von Systemen in Bezug auf die Haftung dergestalt Rechnung getragen werden, dass die Verantwortung für ein sicheres System im Zweifel alle Hersteller treffen. Die Hersteller vernetzungsfähiger Produkte sollten dann grundsätzlich gesamtschuldnerisch haften. Sie sollten dementsprechend auch die Beweislast gegenüber dem Kunden tragen und sich lediglich im Innenverhältnis von der Haftung befreien können.

Sind europäisch einheitliche Regelungen für Entschädigungen geplant?

Antwort:
Während im Verbrauchervertragsrecht Gewährleistungsrechte modernisiert wurden, besteht bei der Produkthaftung dringender Regelungsbedarf. Die Europäische Kommission, die das Initiativrecht für die Reform der Produkthaftungsrichtlinie innehat, hat dazu eine Sachverständigengruppe ins Leben gerufen, die eine Modernisierung bewerten soll. Ein entsprechender Bericht ist für dieses Jahr angekündigt.

Wie können für die Betroffenen lange gerichtliche Auseinandersetzungen vermieden werden?

Antwort:
Eine Modernisierung der Produkthaftung und eine damit einhergehende Erleichterung der Beweislast wäre für die Betroffenen von Vorteil, um ihre Ansprüche einfacher durchzusetzen. Verbraucher haben darüber hinaus schon jetzt die Möglichkeit die Plattform zur Online-Streitbeilegung aufzurufen.
Außerdem haben wir Sozialdemokraten und Sozialdemokratinnen uns in dieser Legislaturperiode sehr für die Verabschiedung einer Verbandsklage, also einer kollektiven Rechtsdurchsetzung auch für Schadensersatzansprüche eingesetzt.
Es ist bedauerlich, dass zuerst die Fraktion der Europäischen Volkspartei mit ihren Mitgliedern CDU/CSU das Gesetzgebungsverfahren im Europäischen Parlament verschleppt hat und im weiteren Verlauf die Mitgliedstaaten im Europäischen Rat keine Einigung erzielen konnten. Wir werden aber in der kommenden Legislaturperiode den Druck aufrechterhalten, dass die Verbandsklage als Teil des Gesetzespakets „New Deal for Consumers“ zügig umgesetzt wird.

5. Störungsfreie Funktion technischer Geräte und fehlerfreie digitale Datensätze

Sicherheitslücken werden von Hackern und Kriminellen erkannt und ausgenutzt. Die Fehlbarkeit der Technik ermöglicht diese Angriffe und der Betroffene hat kaum die Möglichkeit seine Unschuld zu beweisen.

Wie kann hier das Verursacherprinzip* aufrechterhalten werden?

Antwort:
Im Grundsatz sollte bei Haftungsfragen im Falle von Hacker- und Cyberangriffen auf Verbraucher und Unternehmen immer das Verschuldensprinzip gelten.
Für den Fall, dass ein Betroffener alle zumutbaren und gängigen Maßnahmen zur Abwehr von Hackerangriffen getroffen hat, er als Verbraucher oder Verbraucherin etwa ein Virenschutzprogramm oder als Unternehmen ein angemessenes System installiert hat und die eigentlichen haftbaren Personen oder Organisationen, Hacker oder Kriminelle, nicht haftbar gemacht werden können, sollte der Programmhersteller entsprechend für Schäden und Folgeschäden haften.

** Da der Begriff „Verursacherprinzip“ dem Umweltrecht zuzuordnen ist, wurde dieser bei der Beantwortung der Frage durch den haftungsrechtlichen Begriff des „Verschuldens“ ersetzt.*

Wie kann in jedem Fall die Unschuldsvermutung sichergestellt werden?

Antwort:
Die Unschuldsvermutung ist ein zentrales Grundprinzip des Rechtstaates bei einem Strafverfahren und darf niemals angetastet werden. Dies gilt selbstverständlich auch bei strafrechtlich relevanten Taten in Zusammenhang mit Cyberattacken und Hackerangriffen. Bezüglich des zivilrechtlichen Begriffs der Beweislast wird auf die Fragen unter Nr. 4 verwiesen.

6. Überwachungs- und Transportdrohnen

Wie stehen Sie zu Überwachungsdrohnen, Transportdrohnen im öffentlichen Raum?
Was planen Sie zum Schutz der Bevölkerung vor der privaten und öffentlichen Überwachung durch Drohnen?

Die Fragen 1, 2 und 4 zum Thema Überwachungs- und Transportdrohnen werden im Zusammenhang beantwortet:
Auf die technischen Möglichkeiten sowie den Anstieg der Drohnenbesitzer in der Bevölkerung haben wir in Deutschland mit einer Änderung der entsprechenden Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten reagiert. Die Luftverkehrs-Verordnung (LuftVO) enthält ein Verbot zum Betrieb unbemannter Luftfahrtsysteme und Flugmodelle an bestimmten Orten. Nach § 21b Abs. 1 Ziff. 2 der LuftVO ist der Betrieb von Drohnen u. a. über und in einem seitlichen Abstand von 100 Metern von Menschenansammlungen, Unglücksorten, Katastrophengebieten und anderen Einsatzorten von Behörden und Organisationen mit Sicherheitsaufgaben verboten. Zudem ist nach Ziff. 7 der gleichen Vorschrift u.a. auch der Betrieb von Drohnen, die elektronische Bildaufnahmen anfertigen können, über Wohngrundstücken verboten, wenn der betroffene Eigentümer oder sonstige Nutzungsberechtigte nicht ausdrücklich zugestimmt hat. Dadurch wird der zulässige örtliche Einsatzbereich von Kameradrohnen durch nichtöffentliche Stellen von vornherein eingeschränkt.

Zudem muss sich der Einsatz an den datenschutzrechtlichen Vorgaben der Datenschutz-Grundverordnung (DS-GVO) messen lassen, sobald eine Datenverarbeitung nicht ausschließlich im Rahmen persönlicher oder familiärer Tätigkeiten erfolgt, sondern z. B. zu gewerblichen Zwecken oder zum Zwecke der Veröffentlichung. So bedarf es für die Verarbeitung einer Rechtsgrundlage. Beispielsweise muss die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich sein und demgegenüber dürfen schutzbedürftige Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, insbesondere, wenn es sich bei der betroffenen Person um ein Kind handelt (Art. 6 Absatz 1 Satz 1 Buchstabe f DS-GVO). Das bedeutet, die Interessen des Verantwortlichen, der eine Drohne einsetzt, sind mit den Interessen der davon Betroffenen abzuwägen. Eine entscheidende Rolle spielt dabei jeweils der Einsatzzweck. Die genannten Voraussetzungen sind in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht erfüllt. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet erstellt werden.
Insbesondere die Sicherheit und der Schutz der Privatsphäre sowie von sensiblen Einrichtungen ist damit deutlich verbessert worden. Drohnen müssen zudem gekennzeichnet sein.

Im Rahmen der gesetzlichen Möglichkeiten sollte die Nutzung von Transportdrohnen jedoch weiter erlaubt bleiben und weiterentwickelt werden können. Mittelfristig ist zu überlegen, ob durch den Einsatz von Geofencing unter Beachtung datenschutzrechtlicher Vorschriften der Überflug von Drohnen technisch besser und klarer gelöst werden kann.
Setzen Sicherheitsbehörden Drohnen ein, die Bildmaterial aufzeichnen, haben sie sich an die entsprechenden datenschutzrechtlichen Vorgaben und Grenzen der Eingriffsbefugnisse zu halten. Dann können sie in geeigneten Einsatzszenarien ein wertvolles technisches Hilfsmittel zur Gewährleistung der öffentlichen Sicherheit sein. Wir setzen uns für vergleichbare Vorschläge auch auf europäischer Ebene ein.

Wie kann sich der Nutzer von der Haftung für Softwarefehler befreien?

Antwort:
Die SPD setzt sich für die gesetzliche Verankerung von Gewährleistungsrechten für digitale Güter und für eine Umkehr der Beweislast bei einem Mangel ein. Die Produkt- und Herstellerhaftung wollen wir so anpassen, dass auch Schäden aufgrund von Programmierfehlern oder unzureichenden Verschlüsselungen oder mangelnder IT-Sicherheit so geregelt sind, wie Schäden aufgrund von Produktionsfehlern. Es ist klarzustellen, dass auch Software und Softwaredienste bzw. Dienstleistungen im Hinblick auf die Speicherung, Nutzung und Verarbeitung von Daten, Produkte i.S.d. Gesetze sind, um so auch Software zum Download sowie Cloud-Dienste mit aufzunehmen.

Wie wollen Sie die Bevölkerung vor der zu erwartenden Lärmverschmutzung schützen?

Antwort:
In der Luftverkehrs-Ordnung ist in § 21a festgehalten, dass eine Erlaubnis nur erteilt wird, wenn der Schutz vor Fluglärm angemessen berücksichtigt wird. Darüber hinaus können weitere fachspezifische Bewertungen oder Gutachten, insbesondere zum Natur- und Lärmschutz, angefordert werden. Details werden derzeit auf europäischer Ebene ausgehandelt.

Lärm ist ein gesellschaftlich relevantes Problem. Viele Menschen fühlen sich durch Lärm belästigt. Deshalb setzen wir uns dafür ein, die Lärmbelastung der Bevölkerung zu reduzieren.

7. Biometrie 1. Gesetz zur Förderung des elektronischen Identitätsnachweis

Wie sollte die Entscheidungsfreiheit für Menschen gewährleistet werden, die eine Abbildung oder Vermessung durch technische Geräte außerhalb medizinischer Notwendigkeit ablehnen (z.B. aus Glaubensgründen)?

Antwort:
s. Antwort zu Block 8

Wie stehen Sie zu der Absicht, dass künftig die Abgabe des Fingerabdrucks für den elektronischen Personalausweis verpflichtend werden soll?

Antwort:
Wir lehnen die verpflichtende Abgabe der Fingerabdrücke zur Speicherung auf den Personalausweisen, die kürzlich im Rahmen der Verhandlungen zur Verordnung über die Sicherheit von Personalausweisen beschlossen wurde, ab. Sie ist ein Eingriff in die Grundrechte von bis zu 370 Millionen Europäerinnen und Europäer.
Die Europäische Agentur für Grundrechte und der Europäische Datenschutzbeauftragte haben kritische Stellungnahmen zu dieser Maßnahme abgegeben. Die Kommission hat selbst ihrer Folgenabschätzung zum Gesetzesvorhaben festgestellt, dass es effizientere Optionen als die verpflichtende Abnahme von Fingerabdrücken gibt, um das Ziel mehr Fälschungssicherheit bei Personalausweisen zu erreichen.
Wir Sozialdemokratinnen und Sozialdemokraten haben uns daher seit Beginn der Verhandlungen über die Gesetzgebung gegen diese Verpflichtung eingesetzt und im Europäischen Parlament auch gegen den finalen Gesetzestext gestimmt, der diese Maßnahme enthielt.

Wie wollen Sie den Bürger unterstützen, dass seine Daten von RFID-Chips nur bei echtem physischen Zugriff gelesen werden können (Sicherheitsetui gegen NFC Zugriff, Verhinderung des Extended Access Control Zugriffs?

Antwort:
Gegen den Einsatz von RFID-Systemen, soweit er auf gesetzlicher Grundlage und unter Beachtung der datenschutzrechtlichen Bestimmungen erfolgt, ist grundsätzlich nichts einzuwenden. Dazu zählt auch, dass sichergestellt wird, dass Daten nicht unberechtigt ausgelesen werden und dass diese sicher und vertrauenswürdig verschlüsselt werden. Um die Potenziale von RFID zu nutzen und gleichzeitig die Persönlichkeitsrechte zu schützen, wird es entscheidend sein, wie die Vorgaben und Grundsätze der Datenschutz-Grundverordnung wie die Datenschutz-by-Design, Datensparsamkeit sowie schnellstmögliche Anonymisierung oder Pseudonymisierung personenbezogener Daten in RFID-Systemen bereits frühzeitig im Design-Prozess und bei der Markteinführung umgesetzt werden. Dies wird auch entscheidend für die

Akzeptanz dieser Systeme sein. Sofern notwendig werden wir dies auch gesetzlich konkretisieren.

8. Biometrie 2.

Befürworten Sie ethische Richtlinien zum Einsatz der Vermessungsgeräte?

Antwort:
Verweis auf Antwort auf Frage durch SPD im Vorfeld der Bundestagswahlen 2017:
Der Einsatz von Vermessungsgeräten und die damit verbundene Erhebung und Verarbeitung personenbezogener Daten ist ein Eingriff in das Recht auf informationelle Selbstbestimmung. Jeder Eingriff bedarf einer Rechtsgrundlage, in der normenklar definiert wird, wer welche Daten zu welchem Zeitpunkt erhebt und verarbeitet. Der Eingriff muss zudem verhältnismäßig sein. Die Aufgabe von Datenpolitik ist auch, Antworten auf zukünftige Entwicklungen zu liefern und den rechtlichen Rahmen vorzugeben. Aus der Verknüpfung von Daten, dem zunehmenden Umgang mit neuen Entwicklungen ergeben sich viele neuartige rechtliche und ethische Fragen. Diese wollen wir in einem umfassenden Dialog mit der Zivilgesellschaft, der Wissenschaft und der Wirtschaft im Rahmen einer Daten-Ethikkommission klären (SPD-Regierungsprogramm, Seite 38f.).
Die Datenethikkommission hat im Jahr 2018 ihre Arbeit aufgenommen.
Grundsätzlich setzen wir uns auch für die Schaffung einer Europäischen Agentur im Bereich der neuen Technologien und der Künstlichen Intelligenz ein, damit das erforderliche technische und ethische Fachwissen zur Verfügung steht, um öffentliche Akteure auf allen Ebenen zu unterstützen, fundierte Antworten auf die neuen Chancen und Herausforderungen zu geben, die durch die technologische Entwicklung entstehen. Hieraus können ggf. neue rechtliche Regelungen oder ethische Richtlinien entstehen.

Wie werden meine Persönlichkeitsrechte beim Einsatz solcher Vermessungsgeräte gewährleistet?

Antwort:
s.o.

Welche Grenzen setzen Sie in der Körpervermessung?

Antwort:
s.o.

Ist es möglich, medizinisch nicht-notwendige Körpervermessung abzulehnen?

Antwort:
Verweis auf Antwort auf Frage durch SPD im Vorfeld der Bundestagswahlen 2017:
Ja, es sei denn, es gibt eine verfassungskonforme gesetzliche Grundlage für den Eingriff.

Bedeutet das Bestehen auf Datensouveränität eine Einschränkung meiner Reisefreiheit? (kein Zugang zu einem Pass)

Antwort:
Verweis auf Antwort auf Frage durch SPD im Vorfeld der Bundestagswahlen 2017:
Was die Ausweispapiere anbelangt, gibt es im Personalausweisgesetz und im Passgesetz klare gesetzliche Grundlagen. Der Gesetzgeber hat vor einigen Jahren festgelegt, dass Fingerabdrücke im Chip des Reisepasses enthalten sein sollen. Ohne Fingerabdrücke wird kein Reisepass ausgestellt. Sie sind nur dann nicht zu speichern, wenn die Abnahme der Fingerabdrücke aus medizinischen Gründen, die nicht nur vorübergehender Art sind, unmöglich ist. Für die Einreise in Länder außerhalb der EU ist der deutsche Personalausweis grundsätzlich nicht ausreichend und es muss ein Reisepass mitgeführt werden.

9. Unangemessener/Falscher Umgang mit Daten seitens Behörden

Stichworte: Lagerung von Polizeiddatenbanken bei Amazon, Gesetz zur Förderung des elektronischen Identitätsnachweises und Videoüberwachungsverbesserungsgesetz

Wie wird sichergestellt, dass diese Regelungen/Handlungen nicht missbraucht werden, zum Beispiel zu privaten und kommerziellen Zwecken?

Antwort:
Bei den Gesetzen zur Förderung des elektronischen Identitätsnachweises und dem Videoüberwachungsverbesserungsgesetz handelt es sich um nationale Maßnahmen. Auf EU-Ebene haben die Sozialdemokratinnen und -demokraten in der vergangenen Legislaturperiode erfolgreich für eine EU-Datenschutzgrundverordnung zum Schutz personenbezogener Daten bei Unternehmen und Behörden sowie für eine EU-Richtlinie zum Schutz von personenbezogenen Daten bei der Verarbeitung durch Strafverfolgungsbehörden gekämpft. Diese EU-Richtlinie stärkt die Datenschutzrechte der Betroffenen und muss von jedem Mitgliedstaat in nationales Recht umgesetzt und respektiert werden. Respektieren die Mitgliedstaaten diese EU-Vorgaben nicht, muss die EU-Kommission notfalls auch Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof einleiten und die betreffenden Mitgliedstaaten mit Strafzahlungen belegen.

Wie stehen Sie zur automatisierten Identitätserkennung und Verhaltensinterpretation durch Videoüberwachungstechniken?

Antwort:
Videoüberwachung ist kein Allheilmittel im Kampf gegen Terrorismus und Kriminalität. Stattdessen ist sie mit erheblichen Grundrechtseingriffen für die betroffenen Personen verbunden. Deswegen lehnen die SPD-Europaabgeordnten auch die inzwischen ritualisierte Instrumentalisierung von Terroranschlägen oder Kriminalfällen für immer wiederkehrende Rufe nach mehr und möglichst flächendeckender Videoüberwachung ab. Wir unterstützen ein

schnelleres und konsequenteres Ahnden von Straftaten. Dafür bedarf es vor allem einer besseren personellen und finanziellen Ausstattung von Polizei- und Justizbehörden. Eine flächendeckende und anlasslose Videoüberwachung ist nicht zielführend und steht im Widerspruch zu europäischen Grundrechten. Eine Einführung automatisierter Gesichtserkennungs- und Verhaltensinterpretations-Software lehnen wir deswegen entschieden ab.

Wie wollen Sie die Sicherheit der Daten vor kriminellem Zugriff garantieren?

Antwort:
Es ist essentiell, dass Datenbanken umfassend vor Zugriff durch Unbefugte geschützt werden. Das umfasst technische Standards, wie etwa Verschlüsselung, sowie auch besondere physische und administrative Vorkehrungen, damit nur autorisierte Personen Zugriff auf Daten bekommen. Aber selbst wenn die technischen Anforderungen an die Datensicherheit erfüllt sind, muss jede Datenbank auch notwendig und verhältnismäßig sein. Daten-Sicherungssysteme können Risiken vorn unerlaubtem Zugriff minimieren, komplett ausschließen können sie sie nicht. Deswegen muss jede Datenbank strikt auf dem Prinzip der Datenminimierung basieren: Es dürfen nur jene Daten erfasst werden, die tatsächlich notwendig sind und der Speicherzweck und -dauer müssen klar benannt sein.

10. Pilotprojekte und Tests zur Erfassung und Zuordnung biometrischer Daten im öffentlichen Raum

Welche ethischen und rechtlichen Standards zu dieser Form der Datenerfassung sollten festgelegt werden?

Antwort:
Anonymität im öffentlichen Raum muss möglich bleiben. Die SPD-Europaabgeordneten lehnen eine Einführung automatisierter Gesichtserkennungs- und Verhaltensinterpretations-Software aufgrund massiver Grundrechtsbedenken ab. Biometrische Überwachung ist ein weitaus stärkerer Eingriff in die Grundrechte der Betroffenen als herkömmliche Videoüberwachung. Die Voraussetzungen und Grenzen so genannter „intelligenter" Videoüberwachung müssen streng geprüft werden. Wir unterstützen deshalb hohe Schutzstandards, die die Rechte der Betroffenen in den Mittelpunkt stellen. Bei der Entwicklung und beim Einsatz von Algorithmen werden wir uns für internationale Ethikstandards einsetzen.

Wie kann die Freiwilligkeit der Erfassung für die Reisenden garantiert werden? (ohne die Reisefreiheit einzuschränken)

Antwort:
Bei einer flächendeckenden biometrischen Überwachung kann die Freiwilligkeit der Erfassung der Daten der Reisenden in der Praxis kaum garantiert werden. Die SPD-Europaabgeordneten lehnen eine Einführung automatisierter Gesichtserkennungs- und Verhaltensinterpretations-Software deshalb ab.

Wie können sich Bürger, die nicht erfasst werden wollen, vor solchen Projekten schützen?

Antwort:
Es gibt für die/den Einzelne*n kaum Möglichkeiten, sich vor einer flächendeckenden biometrischen Überwachung zu schützen. Die SPD-Europaabgeordneten lehnen eine Einführung automatisierter Gesichtserkennungs- und Verhaltensinterpretations-Software deshalb ab. Es ist Aufgabe des Staates, verhältnismäßigere Mittel zur Verhütung und Verfolgung von Straftaten zu finden.

Wie bewerten Sie solche Projekte?

Antwort:
Siehe auch oben: Anonymität im öffentlichen Raum muss möglich bleiben. Die SPD-Europaabgeordneten lehnen eine Einführung automatisierter Gesichtserkennungs- und Verhaltensinterpretations-Software aufgrund massiver Grundrechtsbedenken ab.

11. Zusammenführung von staatlichen Datenbanken

Wie soll die Sicherheit der Daten gewährleistet werden, wenn das schon bei einzelnen nationalen Datenbanken nicht funktioniert? (Zugriff aus privatem Interesse, Missbrauch, Hacking)

Antwort:
Die angesprochene Verordnung sieht vor, Interoperabilität zwischen dem Visa-Informationssystem (VIS), der Eurodac-Datenbank, dem Schengener Informationssystem (SIS), dem Europäischen Strafregisterinformationssystem (ECRIS), dem Europäischen Reiseinformations- und -genehmigungssystem (ETIAS) und dem Einreise- und Ausreisesystem (EES) herzustellen. Zugangsrechte für Behörden, die auf diese Informationssysteme zugreifen möchten, sind in der Verordnung und nach nationalen Recht geregelt. Für sämtliche Datenverarbeitungsvorgänge werden Protokolle geführt, die von der zuständigen Aufsichtsbehörde oder dem Europäischen Datenschutzbeauftragten mindestens alle sechs Monate überprüft werden. Der Europäische Datenschutzbeauftragte ist bei Sicherheitsvorfällen ebenfalls unverzüglich zu informieren. Unsere Fraktion hatte sich während den Verhandlungen u.a. für strikte Zugangsrechte, sowie die Löschung des Gemeinsamen Identitätsspeichers eingesetzt. Beides wurde jedoch durch eine Mehrheit von rechts-konservativen und liberalen Fraktionen abgelehnt.

Wird diese Zusammenführung langfristig auch die Flugreisedatenbanken in der EU betreffen?

Antwort:
Die Gesetzesvorschläge zur Interoperabilität beziehen die sechs oben genannten Informationssysteme ein: VIS, Eurodac, SIS, ECRIS, ETIAS und EES. Die Einbeziehung von Flugreisedatenbanken ist nicht geplant oder von uns unterstützt. Wir lehnen anlasslose Massenüberwachung ohne Differenzierung nach geografischen Gebiet oder Zeitraum ab.

12. Gesundheitskarte und zentrale Datenspeicherung / Krankendaten

Wer soll nach Ihrer Ansicht mit welchen Kriterien einen Zugriff in dem „erweiterten

Antwort:
Das Ziel muss es sein, den Bürgerinnen und Bürgern EU-weit Zugang zu einer vollständigen elektronischen Datei ihrer Gesundheitsdaten zu geben. Auf diese Weise sollten sie in der Lage sein, die Kontrolle über ihre Gesundheitsdaten zu behalten und sie autorisierten Partnern (für medizinische Behandlung, Vorsorge, Forschung oder für andere Zwecke, die sie für angemessen halten) zur Verfügung stellen. Der unbefugte Zugriff auf die Daten muss ausgeschlossen und strafrechtlich sanktioniert werden.

Wie stellen Sie sich eine übernationale Erweiterung dieses Netzes vor?

Antwort:
Wir müssen uns auf EU-Ebene auf zwei verschiedene Bereiche konzentrieren: Datenschutz und -sicherheit im Gesundheitswesen und Interoperabilität der verschiedenen Systeme. Wie das genau aussehen soll muss die Kommission in Zusammenarbeit mit den Mitgliedstaaten entwickeln. Wichtig ist, dass nicht 28 verschiedene Systeme entwickelt und in Betrieb genommen werden, sondern dass Synergien innerhalb der Mitgliedstaaten genutzt werden.

Wie kann eine Behandlung eines Versicherten ohne eine Karte/ Nachweis einer Versicherung und außerhalb eines Notfalls garantiert werden?

Antwort:
Derzeitig gibt es noch keine einheitliche digitale Krankenversichertenkarte. Aus diesem Grund muss jedes Mitgliedsland sicherstellen, dass eine medizinische Versorgung auch ohne Karte immer garantiert ist. Ein solches Konzept muss jedoch zunächst in den einzelnen Mitgliedsländern entwickelt werden. Für Deutschland muss die Initiative vom Bundeministerium für Gesundheit kommen.

Ist auch künftig eine Behandlung eines Versicherten ohne eine Karte noch möglich?

Antwort:
Auf langer Sicht wird die grenzüberschreitende medizinische Behandlung ohne Versichertenkarte anhand eines bspw. Personalausweises möglich werden. Mit der Europäischen Gesundheitskarte ist die grenzüberschreitende medizinische Versorgung bereits jetzt garantiert. Da noch viel im Bereich des Datenschutzes getan werden muss, wird der Prozess der Behandlung ohne Versichertenkarte noch dauern.

Welche Instanz sollte nach Ihrer Ansicht Gesundheits-Apps auf ihre Funktion und die Sicherheit der Daten prüfen?

Antwort:
Der immer größere Einfluss von e-Health wird europaweit von grundlegender Bedeutung für die Art und Weise sein, wie wir in Zukunft eine hochwertige Gesundheitsversorgung erreichen. Dies betrifft insbesondere den Umgang mit personenbezogenen Daten. Der Datenschutz darf nicht nur als Innovationshemmnis gesehen werden, sondern muss integraler Bestandteil der Entwicklung sein. Es muss zum Beispiel die sichere Übertragung von Gesundheitsdaten im Digitalen Binnenmarktmöglich sein, um auch im EU-Ausland eine angemessene Behandlung zu erhalten. Diese Themen können nur durch eine koordinierte, sorgfältige und wirksame EU-Regulierung gelöst werden. Aus diesem Grund wäre eine europäische Datenschutzbehörde begrüßenswert, die aus Experten aus allen Mitgliedsländern zusammengestellt ist und so die Sicherheit der Daten garantiert.

13. Datenhandel

Gesellschaftlich hat sich die Schufa als Kontrollinstitut etabliert (Mietverträgen, Autokäufen, Kredite) Die Schufa ist ein privates, eigenständiges, nichtstaatliches Unternehmen. Persönliche Daten werden bei Zahlungsunfähigkeit, irrtümlichen Banküberweisungen, Verwechslungen, Zahlungsausständen u.a. seitens der Unternehmen fristlos, ohne Benachrichtigung (Mahnung) und ohne Zustimmung des Betroffenen an Inkassounternehmen und dann an die Schufa weitergeleitet. Die Folge davon sind Einschränkung in diversen Lebensbereichen.

Warum müssen sich die Bürger einem privaten Kontrollunternehmen unterwerfen?

Wie stehen Sie zum Datenhandel durch Schufa und Inkassounternehmen?

Was werden Sie zum Schutz der Betroffenen tun und wie soll eine europäische Lösung dafür aussehen?

Antwort zu allen:
Mit der Einführung der Datenschutzgrundverordnung im Mai 2018 hat der Europäische Gesetzgeber auch Auskunfteien verbindliche Grenzen für das Sammeln und die Weitergabe von Daten gesetzt. Danach dürfen Einträge nur nach den in Artikel 6 der Datenschutzgrundverordnung aufgeführten Erlaubnistatbeständen verarbeitet werden.
Wir wollen, dass auch die für die Bewertungskriterien von Personen durch Algorithmen, insbesondere das Scoring, die individuelle Risikovorhersage für einzelne Verbraucherinnen und Verbraucher samt Gewichtung europaweit offengelegt werden.

14. Netzneutralität

Unterstützen Sie das gesetzliche Festschreiben der Netzneutralität?

Antwort:
Ja. Anderenfalls besteht die Gefahr, dass sowohl auf Seiten der Anbieter als auch auf Seiten der Nachfragenden der Zugang zum Netz und die Art und Weise seiner Nutzung allein eine Frage des Geldes darstellen.

Wie wollen Sie Netzneutralität langfristig gewährleisten?

Antwort:
Von der Formel "alle Daten werden unabhängig vom Inhalt, Verwendungszweck, Empfänger oder von ihrer Herkunft nach dem „Best-Effort-Prinzip“ weiter geleitet" sollte es möglichst wenig Ausnahmen geben. Vor allem Spezialdienste und Netzwerkmanagement sollten nur dort zugelassen werden, wo dies technisch unbedingt notwendig ist. Eine technisch notwendige Differenzierung von Angeboten darf nur zulässig sein, wenn sie von objektiven Kriterien geleitet ist und nicht Meinungen oder Informationen diskriminiert.
Wir fordern flächendeckend leistungsfähige Glasfasernetze bis an den Hausanschluss auch im Sinne der Netzneutralität. Wir Sozialdemokraten lehnen eine "deep packet inspection" zum Zwecke des Netzwerkmanagements ab.
Zero-Rating, also das Nicht-Anrechnen eines Datenverkehrs auf das im jeweiligen Tarif zur Verfügung stehende Datenvolumen, halten wir für wettbewerbsverzerrend.

15. Online-Überwachung

Welches ist die Rechtsgrundlage für Deep-packet-inspection?

Was wollen Sie gegen diese Tiefenkontrolle des Datenstroms unternehmen?

Antwort zu beiden:
Deep-Packet-Inspection ist kein Bestandteil einer EU-Gesetzgebung und fällt daher aus dem Zuständigkeitsbereich der EU-Abgeordneten heraus.
Geheimdienste werden ebenfalls national koordiniert und beauftragt. Sie fallen aus dem Zuständigkeitsbereich der EU-Gesetzgebung heraus.

16. Whistleblower-Schutz

Werden Sie sich weiter für den rechtlichen Schutz von Whistleblowern einsetzen?

Antwort:
Zustimmung

Unterstützen Sie den am 15.3.19 in der EU gefundenen Kompromiss?

Antwort:
Zustimmung

Hinweisgeberinnen und Hinweisgeber, die im öffentliche Interesse Missstände aufdecken, gehören geschützt, nicht verfolgt. Wir unterstützen daher den in den Verhandlungen erzielten Kompromiss, der maßgeblich von der sozialdemokratischen Verhandlungsführerin des Europäischen Parlaments geprägt wurde. Das neue Gesetz wird künftig einen europaweiten Schutz für Personen bieten, die Verletzungen von bestimmten, klar definierten EU-Gesetzen melden, inklusive Fälle von Steuerbetrug, Geldwäsche oder Verstöße gegen Datenschutz- oder Umweltschutzbestimmungen. EU-Mitgliedstaaten haben die Möglichkeit, den Schutz auf weitere Bereiche auszuweiten.

Der Schutz erstreckt sich auf Arbeitnehmerinnen und Arbeitnehmer im privaten und öffentlichen Sektor aber auch viele weitere Personengruppen wie Selbständige, Praktikantinnen und Praktikanten, Bewerberinnen und Bewerber oder ehemalige Angestellte. Vergeltungsmaßnahmen gegen Whistleblower, wie Degradierung oder Kündigung, werden explizit unter Strafe gestellt. Personen, die Hinweisgeberinnen und Hinweisgeber unterstützen, wie zum Beispiel Kolleginnen und Kollegen, genießen ebenfalls Schutz vor jeder Form von Vergeltung.

17. Open Software

Ich werde mich für Maßnahmen stark machen, die die Nutzung und Verbreitung von freier Software (Open Source Software) erlauben und fördern.

Antwort:
Zustimmung

Öffentliche Einrichtungen und Projekte, die öffentliche Fördergelder aus dem EU-Haushalt erhalten, sollten freie Software (Open Source Software)

Antwort:
Zustimmung

In welcher Form sollte Open Source Software bei den Maßnahmen zur Digitalisierung in den Schulen eingesetzt werden?

Antwort:
Da freie Software grundsätzlich auch den Anreiz in sich birgt, den durch ihr gesteuerten Prozess mitbestimmen zu können, wenn er verstanden wird, open source damit Offenheit voraussetzt und Beteiligung auch im Digitalen ermöglicht, sollte sie bevorzugt zum Einsatz

kommen. Gerade wurde mit der Urheberechtsrichtlinie eine Ausnahme für open-source-software beschlossen, so dass künftig urheberrechtliche Fragen dem Einsatz von open source software an Schulen weniger behindern. Der Einsatz von Open Source Software an Schulen fördert Medienkompetenz indem nicht eine bestimmte Anwendung gelernt wird, sondern grundsätzlichere Kompetenzen, das Verstehen und Nachvollziehen eines digitalen Prozesses mit fördert, worin sehr viel eher Medienkompetenz besteht. Jedoch wäre es mit "jetzt macht mal alle schön open source" nicht getan, Netz und Technik müssen vor allem bei Problemen von open source-Kennern gemanagt werden können – einer clusterartigen Einführung, immer begleitet von Experten, die Lehrkräften bei Fragen und Problemen helfen können, scheint sinnvoll.

Wie wollen Sie sicherstellen, dass bei der Mittelvergabe auch andere als die Global Player dabei zum Zuge kommen?

Antwort:
Mit der Joinup collaboration platform will die Europäischen Kommission für den Bereich der öffentlichen Verwaltung mittels Vernetzung und Katalogisierung wiederverwendbarer, interoperabler Software gerade verhindern, dass sich der Bereich der öffentlichen Verwaltung von Lizenzsoftware eines bestimmten Herstellers abhängig macht. Auf der Plattform sollen öffentliche Verwaltungen auch zusammen an Projekten und Problemlösungen arbeiten. Neben der Mittelvergabe erscheint uns Sozialdemokraten dieses Instrument unterstützenswert und ausbaufähig für weitere Bereiche. Mit dem neuen Förderprogramm DigitalEurope will die EU zudem innereuropäische open source-Lösungen gezielt fördern und damit Widerverwendung, Vertrauenssteigerung, Transparenz und Sicherheit bezogen auf die Software zu erhöhen. Außerdem legt das Programm einen Förderschwerpunkt auf KMU.

Welche präventiven Maßnahmen zur Einschränkung von Mediensucht sollten bei der Digitalisierung in Schulen eingesetzt werden?

Antwort:
Die Vermittlung von Medienkompetenz beinhaltet auch kritische Selbstreflektion des Medienkonsums. Wir Sozialdemokraten setzen uns für eine bereits frühkindlich ansetzende Medienkompetenz-Vermittlung ein, die dazu ermuntert selbst zu hinterfragen, was wie lange zu welchem Zweck genutzt wird. Zudem setzen wir uns dafür ein, dass informellen und non-formalen Bildungsinhalten zur Unterstützung der Entwicklung von Selbstwertgefühl, Einfühlungsvermögen sowie kritischem und kreativem Denken, die Festigung der Kommunikationsfähigkeit sowie Förderung der Entscheidungs-, Problemlöse- und Stresskompetenz insbesondere in der Medienkompetenz-Vermittlung ein hoher Stellenwert eingeräumt wird und damit zur Vermeidung von Suchtverhalten beiträgt.