Thema:	DSGVO, Facebook, Privacy Shield	Journalist:	[redacted]
		Termin:	03.05.18, 13 -14 Uhr
Medium:	Deutschladradio	Ort:	Haus der BPK, Berlin

Teil A: Hintergrundinformationen

1) Welche Auswirkungen hat die DSGVO in der Praxis der Aufsichtsbehörden?

Tatsächlicher Hintergrund /aktueller Zusammenhang:

- Neue Aufgaben (z.B.):
    - Akkreditierung und Zertifizierung
        - Aufsichtsbehörden können wenn sie wollen künftig Zertifikate vergeben; die BfDI wird dies nicht tun
        - In ihrem Zuständigsbereich werden die Aufsichtsbehörden Kriterien festlegen, nach denen küntige Zertifizierungsstellen akkreditiert werden
        - zusammen mit der Deutschen Akkreditierungsstelle (DAKKS) erstellen die Aufsichtsbehörden in der AG Zertifizierung entsprechende Verfahrensgrundsätze
    - Unternehmen oder Verbände können den Aufsichtsbehörden Codes of Conduct zur Prüfung vorlegen, diese können dann in der künftigen aufsichtsrechtlichen Beurteilung berücksichtigt werden
    - Unternehmen können von den Aufsichtsbehörden im Rahmen der vorherigen Konsultation innerhalb einer festgelegten Frist von 8 Wochen (Verlängerung um 6 Wochen möglich) eine verbindliche Aussage zu konkreten Datenverarbeitungsprozessen verlangen
    - Aufsichtsbehörden müssen weitreichender als bisher Meldungen von Datenschutzvorfällen entgegen nehmen
        - Meldepflichtig sind nicht mehr nur Unternehmen, sondern jede datenverarbeitende Stelle, also auch Behörden
        - keine Schwellen mehr, die die Meldung auf besonders sensiblen Daten oder Finanzdaten beschränkt
- Neue Kompetenzen:

- Anordnungs- und Bußgeldkompetenzen sind – jedenfalls für die BfDI viel weitreichender als bisher
- Schaffung neuer Strukturen ist erforderlich (z.B. Einrichtung einer Bußgeldstelle bei der BfDI)
- Positiver Effekt: höhere Bußgeldrahmen können abschreckend wirken und damit das Compliance-Interesse der Unternehmen erhöhen

- Neue Prozesse:
  - Kooperations- und Kohärenzverfahren erfordern weitergehende Abstimmung auf europäischer Ebene
    - Schaffung der Zentralen Anlaufstelle (ZASt)
    - Aufgrund föderaler Struktur sind hier im Vorfeld zudem auch Anpassung der nationalen Abstimmungsverfahren notwendig
    - Das Verfahren ist an Fristen gebunden (z.B. Einspruchsfrist gegen die Entscheidung der federführenden Behörde)
  - One-Stop-Shop ermöglicht es Bürgerinnen und Bürgern auch solche Beschwerden an nationale Aufsichtsbehörden zu richten, die bislang aufgrund Unzuständigkeit abgegeben werden mussten => höheres Beschwerdeaufkommen
  - Bei der BfDI wird weitergehender als bisher rechtsformelle Entscheidungen in Form von Verwaltungsakten erforderlich
    - aufwändigeres Verfahren (z.B. aufgrund von notwendigen formellen Anhörungen, etc.)
    - Entscheidungen werden justiziabel => es ist mit einem erhöhten Aufkommen an Gerichtsverfahren zu rechnen
    - BfDI hat ein Justitiariat eingerichtet um diesen Herausforderungen zu begegnen

- Neues Recht:
  - DSGVO enthält viele unbestimmte Rechtsbegriffe und Prozesse die der Auslegung bedürfen (z.B. bei der DSGVO, der Videoüberwachung, der Auftragsdatenverarbeitung)
  - Neues Recht birgt anfangs immer einen gewissen Grad an Rechtsunsicherheit

- Es ist eine wesentliche Aufgabe der Aufsichtsbehörden, durch Auslegung des neuen Rechts Sicherheit zu schaffen. Damit wurde bereits in Form der Kurzpapiere der DSK begonnen (z.B. zu dem oben benannten auslegungsbedürftigen Themen)

2) Neue Macht der Aufsichtsbehörden - sind Sie darauf vorbereitet?

Tatsächlicher Hintergrund /aktueller Zusammenhang:

- Anordnungs- und Bußgeldkompetenzen sind – jedenfalls für die BfDI viel weitreichender als bisher => Schaffung neuer Strukturen bei der BfDI erforderlich
  - Einrichtung einer Bußgeldstelle
  - Einrichtung eines Justitiariats (da mit Klagen gegen Beschlüsse zu rechnen ist)
- Positiver Effekt: höhere Bußgeldrahmen können abschreckend wirken und damit das Compliance-Interesse der Unternehmen erhöhen

3) Zusammenspiel DSBs national / international, was ändert die DSGVO?

Tatsächlicher Hintergrund /aktueller Zusammenhang:

- Kooperations- und Kohärenzverfahren erfordern weitergehende Abstimmung auf europäischer Ebene
  - Schaffung der Zentralen Anlaufstelle (ZASt)
  - Aufgrund föderaler Struktur sind hier im Vorfeld zudem auch Anpassung der nationalen Abstimmungsverfahren notwendig
  - Das Verfahren ist an Fristen gebunden (z.B. Einspruchsfrist gegen die Entscheidung der federführenden Behörde)
- Europäischer Datenschutzausschuss (EDSA) wird verbindliche Entscheidungen zur Rechtsauslegung treffen, an die die nationalen Aufsichtsbehörden der Mitgliedstaaten gebunden sind
  - Verfahren im EDSA wird aufwändiger als bei der Artikel 29-Gruppe (z.B. aufgrund der zu beachtenden Fristen)
  - EDSA tagt öfter als Art. 29-Gruppe => Nationale Behörden müssen mehr Arbeit in die europäische Koordinierung stecken als bisher

4) Es gibt Befürchtungen, dass die Regulierung zu weit gehe, Innovation verhindere - Sichtweise der BfDI?

Tatsächlicher Hintergrund /aktueller Zusammenhang:

- Vor allem aus dem Bereich der Wirtschaft kommt immer wieder der Vorwurf, das zu strenge Datenschutzrecht hindere den Wirtschaftswachstum.
    - Aktuell wird beispielsweise im Rahmen der Debatte um die ePrivacy Verordnung vor allem von der Internetwerbewirtschaft in Aussicht gestellt, dass diese das Internet in der Form wie wir es jetzt kennen zerstören würde. Die strengeren Vorschriften zum Tracking würden aktuell gut funktionierende Geschäftsmodelle zerstören und zu existenzgefährdenden Einbußen bei Verlagen, Websitebetreibern und anderen im Internet agierenden Unternehmen führen. Die fehlenden Gelder würden insbesondere im Bereich der Innovation spürbar, da an dieser Stelle zuerst gespart werden würde.
- Auch aus Teilen der Politik wurde der Datenschutz zuletzt häufiger als Innovationshemmnis und Nachteil für die deutsche und europäische Wirtschaft dargestellt:
    - Bundeskanzlerin warnte im Zusammenhang mit Big Data, dass Deutschland wegen einem überzogenen Datenschutz drohe ein digitales Entwicklungsland zu werden
    - Dorthee Bär hat als neue Staatsministerin für Digitalisierung mehrfach den Datenschutz als Innovationshemmnis bezeichnet
- Datenschutz kann auch innovationsfördernd und Wettbewerbsvorteil sein.
    - Gerade im europäischen Markt zeigt sich, dass bei der Bevölkerung ein hohes Interesse an datenschutzfreundlichen Angeboten besteht. Selbst amerikanische Unternehmen wie Facebook und Apple fangen an, Datenschutz als Maketingthema zu entdecken.
    - Die in der DS-GVO festgeschriebenen Grundsätze von Privacy by Design und Default, bieten neue Möglichekeiten auch im B2B-Markt.
    - Es gibt bereits Beispiele für wirtschaftlich lukrative Big Data Anwendungen, die mit anonymisierten Daten arbeiten (s.u.)

Beispiele:

- In der Fernsehserie „Mission Impossible – Cobra übernehmen sie“ aus den späten 60er Jahren, haben sich die Anweisungen an die Agenten nach dem Anhören immer selbst zerstört. Dieser datenschutzrechtlich sinnvolle Ansatz wurde von Messengerdiensten wie SIMSme oder Snapchat aufgegriffen. Hier kann der Versender einer Nachricht selbst bestimmen, nach wievielen Sekunden, Minuten, Stunden, etc. sich diese auf dem Gerät des Empfängers löscht. *(Anmerkung: Jedenfalls bei Snapchat soll es nach Medienberichten jedoch möglich sein, die Daten bei einer Recherche im Dateisystem des Gerätes wiederherzustellen. Das Beispiel soll aber vor allem die innovative Idee hervorheben.)*

- Sowohl die deutsche Telekom als auch Telefonica haben Anonymisierungsverfahren entwickelt, die es ermöglichen Mobilfunkstandortdaten z.B. für städteplanerische Maßnahmen zur Verfügung zu stellen. Laut Aussage eines Mitarbeiters eines der Unternehmen wurde bei einem Test sogar festgestellt, dass die Aussagekraft der anonymiesierten Daten im Vergleich zur Nutzung von Klardaten (bei einer Implementation in den USA) keine Defizite aufwies.

5) Einschätzung zu Facebook und dessen Regulierungsnotwendigkeit

Tatsächlicher Hintergrund /aktueller Zusammenhang:

- Über eine App, die von November 2013 bis Mai 2015 direkt auf der Plattform Facebook angeboten wurde, wurden – nach Angaben von Facebook – die Daten von insgesamt rund 87 Millionen Nutzern, davon 2.7 Millionen Europäern und etwa 310.000 Deutschen erhoben und an Cambridge Analytica weitergegeben. Diese Angaben sowie die Anzahl von 65 Downloads deutscher Nutzer wurden von Facebook per E-Mail übermittelt. Da die internen Untersuchungen bei Facebook noch nicht abgeschlossen sind, kann sich die Anzahl noch ändern.

- Die App bot dem aktiven Nutzer einen Persönlichkeitstest und forderte neben dem Zugriff auf die eigenen Daten auch Zugriff auf die Profile der Freunde. Hatten diese Facebook-Freunde von Nutzern der App einem Datenzugriff von Apps ihrer Freunde nicht explizit in ihren Einstellungen widersprochen (opt-out), wurden ihre Daten im selben Umfang erfasst (Schneeball-System).

- Eventuell gab es weitere Unternehmen (berichtet wurde bspw. über eines namens Cubeyou), die ebenfalls eine ähnliche App auf dem Netzwerk angeboten hat – das Unternehmen Cubeyou und die angebotene App wurden gesperrt. Facebook hat angekündigt, die bisher auf der Plattform verfügbaren Apps hinsichtlich ihrer Datenverarbeitung hin zu überprüfen und neue Apps vor

Veröffentlichung einer Prüfung zu unterziehen. Ob diese Untersuchung bereits begonnen hat und welche ähnlich agierenden Apps dadurch noch gefunden werden, bleibt abzuwarten.

- Bei einer der Anhörungen von Facebooks CEO Zuckerberg vor dem US Kongress kam auch die Thematik der sog. Schattenprofile zur Sprache. Dort gab Facebook zu, dass sie Daten von Nicht-Nutzern anlegen – angeblich aus Sicherheitsgründen. Fest steht, dass diese Daten genutzt werden, um neuen Nutzern direkt passende Freunde vorzuschlagen. Überaus fraglich erscheint dabei, ob personenbezogene Daten Teil dieses Profils werden und wenn ja, auf welcher Rechtsgrundlage die Daten erhoben werden.

- Facebook hat zwischenzeitlich zumindest für die europäischen Nutzer eine Umstellung der Datenschutzeinstellungen umgesetzt. Hiermit wird auf die Anforderungen der DSGVO reagiert. Auch die neuen Einstellungen begegnen Kritik, da es einfacher ist mit einem Klick einer weitgehenden Datennutzung zuzustimmen als datenschutzfreundliche Einstellungen zu wählen, wofür mehrere Klicks notwendig sind.

- Der in Deutschland zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat aufgrund des Vorfalls um Facebook und Cambridge Analytica ein Verfahren eröffnet und widmet sich der Aufklärung. Ebenso ermitteln weitere europäische Aufsichtsbehörden (u.a. in GB, ES, BE, IT).

- Die Artikel 29-Gruppe unterstützt die nationalen Behörden in ihren Ermittlungen, die auf der Ebene der WP 29 bereits seit längerem in einer Facebook Kontaktgruppe zusammenarbeiten. Sie wird die Arbeiten auch ausdehnen durch eine neue Arbeitsgruppe, die „Social Media Working Group“, um eine Strategie zum künftigen Umgang mit sozialen Netzwerken zu entwickeln.

- Bei dem Vorfall um Facebook und die Datenweitergabe an das Datenanalyseunternehmen Cambridge Analytica handelt es sich womöglich nur um die Spitze eines Eisbergs. Das Vorkommnis zeigt die Risiken für Profilbildung im Internet und anschließendes Mikrotargeting in erschreckendem Ausmaß.

    - Mikrotargeting beschreibt eine Kommunikationsstrategie der gezielten Ansprache von Menschen aufgrund ihrer Vorlieben, Einstellungen und Meinungen. Die Zwecke des Mikrotargetings erfassen sowohl die passgenaue Ansprache mit Werbung als auch den Versuch der politischen Einflussnahme.

    - Während den Nutzern soziale Netzwerke zum Austausch über ihre Interessen, ihre Vorlieben sowie ihr Privat- und Arbeitsleben dienen, erwachsen mithilfe der preisgegebenen Daten intransparente Geschäftsmodelle. Werden diese Daten nicht nur gespeichert, sondern miteinander verknüpft oder noch mit Informationen aus weiteren Quellen

angereichert, entsteht potentiell ein komplexes und aussagekräftiges Persönlichkeitsprofil – ohne das Wissen der Betroffenen.

Rechtliche Einordnung / relevante Normen (soweit relevant):

- Facebook hat sich in seiner Argumentation darauf zurückgezogen, dass die Nutzer selbst in die Nutzung ihrer Daten eingewilligt haben. Allerdings hatten die Nutzer zu keiner Zeit das Recht, eine Einwilligung für die Nutzung der Daten ihrer Freunde zu erteilen. Hier zieht sich Facebook auf die Argumentation zurück, dass die Freunde der Nutzer dies durch ihre eigenen Voreinstellungen selbst hätten verhindern können.

- Kernfrage ist, ob die hier erteilten Einwilligungen datenschutzrechtlichen Anforderungen entsprechen. Dies dürfte aufgrund mangelnder Transparenz eher kritisch gesehen werden. Eine konkrete datenschutzrechtliche Bewertung obliegt allerdings dem LfD Hamburg bzw. der irischen Datenschutzaufsicht

- Die Datenschutz-Grundverordnung und das neue Bundesdatenschutzgesetz (BDSG) enthalten nach derzeitigem Kenntnisstand ein ausreichendes Instrumentarium für die adäquate Behandlung derartiger Vorkommnisse.

    - Marktortprinzip stellt sicher, dass die DSGVO auch für außereuropäische Unternehmen zur Anwendung kommt, sofern diese auf dem europäischen Markt Waren und Dienstleistungen anbieten.

    - Kooperationsmechanismus und das Kohärenzverfahren führen zu einem europaweit einheitlichen und verbindlichen Entscheidungsprozess

    - Stärkung der Betroffenenrechte aufgrund strikterer Transparenz- und Informationspflichten

    - höhere Anforderungen an eine Einwilligung und ein strengeres Kopplungsverbot

    - "Privacy by Design“ und „Privacy by Default“

    - Pflicht Datenschutzvorfälle den Aufsichtsbehörden zu melden und unter gewissen Voraussetzungen die Betroffenen zu benachrichtigen

    - Weitergehende Verwaltungs- und Sanktionsbefugnisse für die Aufsichtsbehörden inkl. eines stark erhöhten Bußgeldkatalog

- Gerade das Thema Mikrotargeting mittels Online-Tracking (durch Cookies, Device Fingerprinting, etc.) wird rechtlich durch die in Abstimmung befindlichen ePrivacy Verordnung geregelt werden

- Insb. Fragen zum Tracking sind stark umstritten; die Wirtschaft sieht hier Geschäftsmodelle massiv gefährdet

- Europäisches Parlament und Datenschützer (WP 29) fordern strenge beschränkung des Trackings insb. ein Verbot ausdrücklicher "Tracking Walls" und standardmäßige Browsereinstellungen, die es erleichtern, die Zustimmung zum Tracking auszudrücken oder zu verweigern

6) PrivacyShield - Erfahrungswerte, Bewertung

Tatsächlicher Hintergrund /aktueller Zusammenhang:

- Die Art. 29 Gruppe hat in ihrer Stellungnahme zur Ersten Jährlichen Gemeinsamen Überprüfung des Privacy Shield (Joint Review) vom 9. Oktober 2017 weiterhin gewichtige Kritikpunkte am EU-US Privacy Shield aufgeführt, die aus ihrer Sicht abgestellt werden müssen. Insbesondere fehlt es zurzeit noch an der Benennung einer unabhängigen Ombudsperson, der Erläuterung der Verfahrensregelungen für den Ombusmechanismus und der vollständigen Besetzung des Privacy and Civil Rights Oversight Board (PCLOB). Hier hat die Art. 29 Gruppe der US-Seite eine Frist bis zum 25. Mai 2018 gesetzt, die offenen Fragen zu klären.

- Weitere Kritikpunkte, die bis zur Zweiten Jährlichen Gemeinsamen Überprüfung des Privacy Shields im September 2018 ausgeräumt werden sollten, sind Fragen in Bezug auf die Überwachung durch Sicherheitsbehörden, zur effektiven Möglichkeit, sich hiergegen juristisch zu wehren und zu den effektiven Abhilfebefugnissen der Ombudsperson.

- Im kommerziellen Bereich hat die US-Seite deutliche Anstrengungen unternommen, den Zertifizierungsmechanismus für US-Unternehmen unter dem Privacy Shield und die Aufsicht der US-Behörden über die Zertifizierung zu stärken. Diese Maßnahmen werden in der Zweiten Jährlichen Gemeinsamen Überprüfung des Privacy Shields im September 2018 überprüft werden. Offen sind u.a. noch Leitlinien zu den Themen Beschäftigtendaten, Anwendung des Privacy Shields auf Auftragsverarbeiter und automatisierte Entscheidungen/Profiling. Hierzu hat die US-Seite einen Austausch angeboten. Dieses Angebot soll zunächst in Form einer Telefonkonferenz mit dem Joint Review Team beantwortet werden, wobei klargestellt wird, dass die Art. 29-Gruppe auch schriftliche Unterlagen erwartet, um die Angemessenheit der geplanten Leitlinien überprüfen zu können.

- Beschwerden unter dem Privacy Shield hat es in Deutschland bisher nicht gegeben.

Rechtliche Einordnung / relevante Normen (soweit relevant):

- Kapitel V DS-GVO, hier insbesondere Art. 45 DS-GVO (vormals Art. 25 Abs. 6 DS-RL, der Grundlage für den Angemessenheitsbeschluss der Kommission zum Privacy Shield ist).

Teil B: Sprechzettel

1) Welche Auswirkungen hat die DSGVO in der Praxis der Aufsichtsbehörden?

- Die DSGVO erlegt den Aufsichtsbehörden beispielsweise **neue Aufgaben** auf, wie z.B. die Mitwirkung bei der Erstellung von Codes of Conduct oder der Bearbeitung von Beschwerden im Rahmen des One-Stop-Shops. Bereits hieraus folgt ein **erhöhter Aufwand in der täglichen Arbeit.**

- Die DSGVO führt **neue Prozesse** ein, wie z.B. die europaweite Koordinierung datenschutzrechtlicher Fragen im Rahmen des **Kooperations- und Kohärenzverfahrens**. Hierfür musste die **ZASt** geschaffen werden und auch auf nationaler Ebene ein Abstimmungsverfahren erstellt werden.

- Die DSGVO führt **neue Kompetenzen der Aufsichtsbehörden** ein und erhöht den Bußgeldrahmen. Hierfür muss – jedenfalls die BfDI – strukturelle Anpassungen vornehmen, wie die **Schaffung einer Bußgeldstelle und eines Justitiariats**. Letzteres auch weil das Verwaltungshandeln insgesamt weitergehend justiziabel werden wird.

- Die DSGVO bringt als neues Recht eine gewisse Rechtsunsicherheit mit sich. Es ist eine wesentliche **Aufgabe der Aufsichtsbehörden**, **an der Auslegung mitzuwirken** und Unternehmen, Behörden und Bürgerinnen und Bürgerinnen **bei der Anwendung des neuen Rechts zu unterstützen**.

2) Neue Macht der Aufsichtsbehörden - sind Sie darauf vorbereitet?

- Bei Spiderman heißt es: **Aus großer Macht folgt große Verantwortung**. Das gilt auch hier. Deshalb bereiten sich die Aufsichtsbehörden schon seit längerer Zeit auf die neuen Kompetenzen vor.

- Ob wirklich alle Eventualitäten bedacht worden sind, wird sich ab dem 25. Mai zeigen. Sicherlich ist es denkbar, dass sich in der Praxis (neue) Probleme auftuen, die man nicht auf dem Schirm hatte. Aber auch hier werden Lösungen gefunden werden. **Ich habe jedenfalls deshalb keine schlaflosen Nächte**.

- Wenn sich alle datenverarbeitenden Stellen ebenfalls gut auf die DSGVO vorbereitet haben, müsste die neue Machtfülle im Idealfall gar nicht ausgeschöpft werden. **Ich stelle doch lieber bei einer Kontrolle keinen Datenschutzverstoß fest, als dass ich ein Bußgeld im siebenstelligen Bereich verhänge**.

- Es bleibt zu hoffen, dass die neuen Kompetenzen der Aufsichtsbehörden und vor allem der höhere Bußgeldrahmen dazu führen, dass Unternehmen den Datenschutz ernster nehmen, denn: **Die Aufsichtsbehörden sind künftig nicht mehr Hunde die nur bellen, sondern auch kräftig zubeißen können**.

3) Zusammenspiel DSBs national / international, was ändert die DSGVO?

- Vor allem wird die **Zusammenarbeit enger und intensiver**. Damit ist natürlich auch ein erhöhter bürokratischer und zeitlicher Aufwand verbunden.

- Aufgrund der föderalen Struktur der deutschen Datenschutzaufsicht müssen **gewisse Fragen erst national abgestimmt** werden, bevor Sie nach Brüssel transportiert werden. Das macht es für Deutschland nicht leichter, zumal die DSGVO in vielen Fällen Fristen vorgiebt.

- Im Ergebnis wird **Europa datenschutzrechtlich zusammenrücken**. Und die DSGVO beweist schon heute eine gewisse internationale Strahlkraft. Wenn sich der Koordinierungsprozess innerhalb Europas bewährt kann das auch ein **Vorbild für eine weitergehendes internationales Modell** sein.

4) Es gibt Befürchtungen, dass die Regulierung zu weit gehe, Innovation verhindere - Sichtweise der BfDI?

- **Dem, der Datenschutz als Investitionshemmer kritisiert, fehlt schlichtweg die Perspektive, ihn für sich nutzbar zu machen!**

- Die Betrachtungsweise von Datenschutz als Wirtschaftshemmnis ist wie die Betrachtungsweise eines Lagerfeuers ausschließlich als potentielle Ursache für einen Flächenbrand. Denn so wie ein Lagerfeuer dazu genutzt werden kann, um sich aufzuwärmen und Marshmallows oder Würstchen zu rösten, können Unternehmen den Datenschutz auch zu ihrem Vorteil nutzen.

- Wird der **Datenschutz** so eingesetzt, dass hieraus ein **imagefördernde Qualitätsmerkmal** entsteht, wird aus dem hierfür aufgewandten „Mehraufwand“ schnell ein echter „Mehrwert“. Gerade in Zeiten von Skandalen wie aktuell bei Facebook gibt es eine erhebliche **Nachfrage nach datenschutzfreundlichen Produkten und Dienstleistungen**.

- Gerade Deutschland hat in Sachen Datenschutz eine **Kernkompetenz**. Wir können diesbezüglich auf eine **Erfahrung von fast einem halben Jahrhundert** zurückgreifen. Warum nutzen wir diesen Vorteil nicht aus?

- Die taz feiert den Datenschutz in einem aktuellen Artikel (vom 28.04.2018) als **Exportschlager** und berichtet, dass viele Staaten ihr Recht bereits an die DSGVO angepasst haben. Ein südafrikanischer Anwalt wird dort wie folgt zitiert: ***„Die Datenschutzgrundverordnung hat lange Tentakeln.“*** Auch große US-Unternehmen wie Apple oder Google, versuchen aktuell Datenschutz als Geschäftskonzept zu integrieren.

5) Einschätzung zu Facebook und dessen Regulierungsnotwendigkeit

- Der Vorfall ist ein alarmierendes **Beispiel für die großen Risiken der Profilbildung im Internet**, vor denen die BfDI und andere Datenschutzaufsichtsbehörden bereits seit Jahren warnen.

- Fall ist sicherlich nur die **Spitze des Eisbergs,** denn letztendlich basiert das **Geschäftsmodell von Unternehmen wie Facebook** gerade darauf, die **Daten ihrer Kunden gewinnbringend zu vermarkten**. Auch Facebook hat gegenüber der Börsenaufsicht mitgeteilt, dass man damit rechnet bei internen Untersuchungen weitere Datenmißbräuche aufzudecken.

- Es ist wichtig, das **Thema konsequent weiter zu verfolgen** und lückenlos aufzuklären. Es wäre fatal, wenn ungeachtet des Umfangs des Problems ohne eine Grundlegende Aufarbeitung graduell zur Tagesordnung übergegangen würde.

- Die Politik sollte in Anbetracht von Vorfällen wie diesem erkennen, dass zum Schutz des Menschen in der digitalen Welt **ein starker Datenschutz erforderlich** ist und **nicht das Gegenteil**.

- Auch wenn **Mißbrauch nie vollständig verhindert** werden kann, **minimiert** das Bestehend eines guten **Datenschutzrechts zumindest die Risiken** für Bürgerinnen und Bürger, die ohne entsprechende Regeln mehr oder weniger schutzlos im Regen stehen würden.

- In diesem Zusammenhang kommt der **Datenschutzaufsicht eine elementare Rolle** zu. Gerade weil entsprechende Datenverarbeitungsprozesse für die Betroffenen oftmals intransparent sind, bedarf es der fachlichen Expertise und Kontrolle der **Aufsichtsbehörden**. Diese **müssen** hierfür aber auch **entsprechend aufgestellt und ausgestattet sein**.

- Sowohl nationale als auch europäische Aufsichtsbehörden werden dieses Thema eng abgestimmt in den Fokus nehmen.

- Die **DSGVO ist bereits eine gute Grundlage**, um die dem Skandal zu Grunde liegende Thematik regulatorisch in den Griff zu bekommen. Allerdings muss die

Politik nun auch den weiteren Schritt gehen und **dem Werkzeugkasten der DSGVO noch das Feinwerkzeug der ePrivacy Verordnung beifügen**, in der es ja – jedenfalls im Entwurf der Kommission und des Parlaments – gute Lösungen gibt, um beispielsweise das Thema Online-Tracking im Sinne der Internetnutzerinnen und -nutzer neu zu regeln.

6) PrivacyShield - Erfahrungswerte, Bewertung

- Der erste **Joint Review** im vergangen Herbst hat gezeigt, dass es weiterhin **erhebliche Kritikpunkte** am Privacy Shield gibt.
- Dies betrifft vor allem den Bereich der **sicherheitsbehördlichen Überwachung**.
- Im kommerziellen Bereich hat die US-Seite hingegen erfreulicherweise ihre Hausaufgaben gemacht, auch wenn in diesem Bereich nicht alles rosig ist.
- Die **Artikel 29-Gruppe** hat der US-Seite eine **Frist bis zum 25. Mai** gesetzt, um beispielsweise die noch offenen Fragen zur Besetzung der Ombudsperson und der Regelung des entsprechenden Verfahrensmechanismus zu klären. Sollte diese Verstreichen, **behalten wir uns explizit auch gerichtliche Maßnahmen vor**. Es kann nicht sein, dass in einer so wichtigen Frage auf Zeit gespielt wird.