Institut für Europäisches Medienrecht
Institute of European Media Law
Institut du droit européen des médias

Workshop

In Kooperation mit

BDZV Bundesverband Deutscher Zeitungsverleger

APR Arbeitsgemeinschaft Privater Rundfunk

VPRT Verband Privater Rundfunk und Telemedien e.V.

Montag, 22. Mai 2017, 10:30 bis 16:00 Uhr

Datenschutz und Datensicherheit für Medienunternehmen

Begrüßung und Einführung - Prof. Dr. Stephan Ory

Herr Prof. Dr. Stephan Ory, Direktor des EMR, führte das Publikum in die interdisziplinäre Thematik ein und ordnete zugleich die Referenten den zu auf der Agenda stehenden Themenkomplexen zu: Im ersten Teil wird der namensgebende Sachverhalt der Datensicherheit aufbereitet: Was spielt sich technisch ab, welche Motive bewegen Angreifer und wie kann sich ein Unternehmen wirksam schützen? Im zweiten Teil zum ebenfalls namensgebenden Datenschutz wird zunächst die Frage erörtert werden, ob die Datenschutzgrundverordnung nunmehr eine tatsächliche Änderung für Unternehmen bringt oder nur „alten Wein in neuen Schläuchen" darstellt. Mit der Zulässigkeit von Werbung vor dem Hintergrund der Datenschutzgrundverordnung soll anschließend ein praktisch relevantes Thema besprochen werden. In einem dritten Abschnitt kommen die Vertreter aus Medienunternehmen und datenschutzrechtlichen Aufsichtsbehörden zusammen, um die Entwicklungen in einem Streitgespräch zur Datenschutzgrundverordnung, zur geplanter E-Privacy Verordnung und nationaler Datenschutzgesetze vertieft zu diskutieren.

Zusätzlich zu dieser Gliederung und grundsätzlichen Ordnung wurde von Herrn Prof. Dr. Ory der jeweilige Hintergrund der Referentin oder des Referenten kurz dargestellt. Ganz im Sinne der Veranstaltung rekrutierten sich die Referenten aus dem technischen wie auch juristischen Bereich. Dabei kamen Vertreter von Forschungseinrichtungen ebenso wie operativ Verantwortliche zu Wort.

Herr Prof. Dr. Ory dankte den Kooperationspartnern – namentlich dem Bundesverband Deutscher Zeitungsverleger, der Arbeitsgemeinschaft Privater Rundfunkt und dem Verband Privater Rundfunk und Telemedien e.V. – für ihre Unterstützung.

Serienreif: Pro7Sat1 im Cyberwar - Martin Neubauer

Herr Neubauer konnte direkt aus seiner beruflichen Praxis als Head of Information Security im Bereich Corporate Security der ProSiebenSat.1 Media SE berichten. Zu Beginn seines Vortrags stellte er den unterschiedlichen Diskussionsstand dar, ob Medienunternehmen als „kritische

Infrastrukturen" im Sinne des Gesetzes einzustufen seien. Diese Frage gilt es seines Erachtens nach zu bejahen. Hintergrund der Feststellung sei die Tatsache, dass Medienunternehmen einen wichtigen Beitrag zur Sicherung der Medien- und Meinungsvielfalt liefern. Zudem haben die Bürger ein besonders hohes Vertrauen in die von den klassischen Medienunternehmen verbreiteten Inhalte. Nicht zuletzt hob Herr Neubauer auch die große Bedeutung der Medien für demokratische Wahlen hervor und betonte zusammenfassend die Bedeutung der Medien als Meinungsplattform.

Als ersten Inhaltpunkt untersuchte der Referent die Frage, was die Motive der Angreifer sind. In erster Linie kämen hier wirtschaftliche Interessen in Betracht. Dies äußere sich besonders auch daran, dass die „Cyberkriminellen" zur Verfolgung wirtschaftlicher Interessen - beispielsweise bei der Verbreitung von Erpressertrojanern oder gefälschten Überweisungsaufträgen, welche angeblich von Vorstandsmitgliedern an Mitarbeiter versendet werden – ein sehr hohes Organisationsniveau aufweisen würden, welches sich von der virtuellen bis in die reale Welt reiche. Der Vortrag beleuchtete neben diesen professionellen und wirtschaftlich motivierten Angreifern auch den Ex-Mitarbeiter und ausländischen Nachrichtendienste als Gefahr für die eigene Cybersicherheit. Beim letzteren Angreifer gab Herr Neubauer zu bedanken, dass Medien nicht nur als Kommunikationstechnologie zu begreifen sind, sondern auch ein für andere Staaten interessantes Machtmittel darstellen können.

Auf die Frage, welches das schwerwiegendste Angriffsszenario für Medienunternehmen sei, gab Herr Neubauer bereits im Vortrag eine klare Antwort: Die allergrößte Sorge bereiten natürlich die Situation, dass durch einen Angreifer fremde Inhalte in das eigene Programm eingespielt wird. Dieses Szenario konnte mittels der Darstellung des TV5 Monde Hacks praktisch veranschaulicht werden. Eine vergleichbare Gefahr bestehe ebenso für Drittanbieter, welche in die eigenen Medien Inhalte einspielen und naturgemäß schwerer als eigenen Plattformen mit den Mitteln der Cybersicherheit zu erfassen sind.

Weiteres enormes Schadenspotenzial sah Herr Neubauer für den Fall der Veröffentlichung von sensiblen Daten, was gerade hinsichtlich Partnerbörsen und Shops relevant werden würde. Angebote dieser Art sind aktuell ebenfalls Teil der ProSiebenSat.1 Media SE. Die enthaltenen sensiblen Kundendaten gelte es ganz besonders zu schützen.

Medienunternehmen als kritische Infrastruktur – was droht aus dem Netz? - Prof. Dr. Christoph Sorge

Herr Prof. Dr. Christoph Sorge, der Inhaber der juris Stiftungsprofessur an der Universität des Saarlandes vertrat in Beitrag „Medienunternehmen als kritische Infrastruktur – was droht aus dem Netz?" Frau Nora Apel, die krankheitsbedingt ihren Vortrag leider nicht halten konnte. Frau Apel ist im Referat Grundsatzfragen, Kritische Infrastrukturen am Bundesamt für Sicherheit und Informationstechnik beschäftigt.

Der Vortrag nahm entsprechend des Titels die Bedrohungslage der Medienunternehmen in den Blick. Vorweg wurde deutlich herausgestellt, dass grundsätzlich auch Medienunternehmen ein „kritische Infrastruktur" im Sinne des Gesetzes darstellen können. Als Beispiele wurden nunmehr die politische Willensbildung und die Warnung im Katastrophenfall genannt. Diese Szenarien wurden sogleich mit praktischen Beispielen vom gefälschten Interview im Blog von Reuters bis hin zur börsenwirksamen aber rein erfundenen Meldung über eine Bombe im Weißen Haus untermauert.

Hinsichtlich der möglichen Angreifer werde im Folgenden die Motive und Angriffsmöglichkeiten von Einzelpersonen bis hin zu organisierten Gruppen erläutert. In dieser übersichtlichen

Darstellung geht der Vortrag auch auf das Interessengeflecht der Gruppen, die Ziele und die jeweils zur Verfügung stehenden Ressourcen ein. Gerade der letzte Punkt ist in der heutigen Zeit zwar mithin entscheidend, jedoch stellte der Vortrag klar, dass auch technisch wenig versierte Angreifer die benötigte Schadsoftware für ihren Angriff relativ günstig einkaufen können. Insgesamt habe sich eine „arbeitsteilige" Wirtschaft der Cyberkriminalität herausgebildet. Eine Gruppe oder Person verkauft die benötigte Schadsoftware oder Sicherheitslücke, während andere den eigentlichen Angriff durchführen. Doch auch die erlangten Daten, wie beispielsweise Kreditkartennummern, werden letztendlich wieder weiterverkauft und von Dritten zum Missbrauch genutzt.

Damit skizzierte der Vortrag letztendlich eine multiple Bedrohungslage. Die sich anschließende Frage wieso es die Angreifer eigentlich „so leicht haben", beantwortete der Vortrag damit, dass die Bedrohung vielfach unterschätzt werden würde, zu wenige Ressourcen in die Sicherheit investiert werden, Monokulturen an Software im Unternehmen unterhalten werden und vielfach Nutzer mit der Technik überfordert sich. Das an diese Feststellungen anschließende Resümee kann man derart zusammenfassen, dass eine ständige Beschäftigung mit der IT-Sicherheit erforderlich ist und es sich keineswegs nur um eine singuläre Aufgabe handelt.

Nichts ist unmöglich: Konzepte zur Cybersicherheit in Unternehmen - Prof. Dr. Christoph Sorge

Prof. Dr. Christoph Sorge kann mit seinem eigenen Vortrag direkt an den vorhergehenden Beitrag anschließen. Er stellt die Frage, was nun passieren müssen, um die Aufgabe der IT-Sicherheit beständig im Unternehmen wahrzunehmen. Einleitend nannte er nun verschiedenen Konzepte und technische Möglichkeiten, wie man dieses Ziel erreichen könnte. Die Auswahl reicht im Feld der IT-Sicherheit von Firewalls über Intrusion Detection Systems bis hin zu Antivirensoftware. Herr Prof. Dr. Sorge stellte an dieser Stelle klar, dass gleichwohl all dies nur einen kleinen Ausschnitt eines umfassenden IT-Sicherheitskonzeptes darstellt.

Der Vortrag betrachtete im Folgenden unterschiedliche Angriffsszenarien und welche Schutzmöglichkeiten sich jeweils bieten. Im Bereich des „low tech" können bereits Recherchen im Müll des Unternehmens oder der versteckte Einsatz von Keyloggern kritische Informationen in die Hände von Angreifern gelangen lassen. Während gegen derartige Angriffe noch relativ alltagstaugliche Gegenmaßnahmen ergriffen werden können, sei dies im Bereich von professionalen, mit großem Ressourceneinsatz und damit auch meist auf das Unternehmen maßgeschneiderten Angriffen, nur noch schwerlich möglich.

Zumindest die Zero-Day-Lücke, also ein Einfallstor für einen Angreifer in der Soft- oder Hardware des Unternehmens, welche noch nicht einmal dem jeweiligen Hersteller bekannt ist, stellt den Prototyp der unmöglichen Schutzaufgabe dar. Angesichts dieser Situation brachte Prof. Dr. Sorge die Frage auf, ob man nunmehr auf Stift und Papier zurückgreifen solle. Die Antwort darauf ist jedoch nicht eindeutig. Herr Prof. Dr. Sorge verdeutlichte, dass immer eine Abwägung erforderlich ist. Bei der Auswahl der Schutzmechanismen sei zu berücksichtigen, welche Strukturen und Werte es zu schützen gilt und welches Risiko jeweils besteht.

Im Schutzkonzept wären zudem die Mitarbeiter einer der wichtigsten Ansatzpunkte. Sogleicht führt dies zu einem ganz praktischen Problem, denn die Abwägung Vertrauen gegen Überwachung ist eine diffizile Werteentscheidung nicht nur rechtlicher Natur, sondern auch für die gewollte Unternehmenskultur.

Letztendlich kommt Herr Prof. Dr. Sorge zum Ergebnis, dass die Unternehmenssicherheit die Nutzbarkeit der Sicherungsmaßnahmen vor dem Hintergrund einer Alltagstauglichkeit nicht aus dem Blick verlieren darf. Nur wenn diese in einem vernünftigen Maße gewahrt wird, kann die IT-Sicherheit in einem Unternehmen auch wirklich zu einer dauerhaft wahrgenommenen Aufgabe werden.

Journalistische Recherche zwischen Betriebsgeheimnis und Medienprivileg - Rechtsanwalt Lutz Tillmanns

Dass sich das Informationsbegehen der Presse, gestützt auf Presse und Meinungsfreiheit – auch in der datenschutzrechtlichen Ausprägung des Medienprivilegs – in einem ständigen Konfliktfeld mit den Betroffeneninteressen befindet, ist keine Neuheit. Dieser Konflikt wurde nun von Herrn RA Tillmanns verfassungsrechtlich aufgearbeitet und die Reihe der bedeutsamsten Urteile wie das Spiegel oder das Cicero Urteil des BVerfG kurz dargestellt. In der Interessenkollision zwischen Datenschutz und Pressefreiheit zeigte Herr RA Tillmanns auf, dass ein beständiges Abwägen erforderlich ist und somit auch eines der durchgängigen Arbeitsfelder des Presserats darstellt.

Die praktische Grundlage sei das sogenannte Zweisäulenmodell des Medienprivilegs. Während die erste Säule aus Normierungen wie § 41 BDSG und den Landesdatenschutzgesetzen besteht, baue die zweite Säule auf einer freiwilligen Selbstkontrolle auf. Gerade die zweite Säule ist es nun, welche durch die Struktur des Presserates abgedeckt werden müsse. Eine Aufgabe des Presserates sei es demzufolge auch, den Pressekodex herauszugeben. Herr RA Tillmanns beleuchtet im Folgenden die datenschutzrechtlichen Details des Pressekodexes, die teilweise bereits vor 15 Jahren geschaffen wurden. Neben diesen dogmatischen Einsichten in die Arbeit des Presserates und die Bedeutung des Medienprivilegs widmete sich der Vortrag auch ganz praktisch Beispielen rund um Berichtserstattung und Leserbriefen, die eine hohe datenschutzrechtliche Relevanz aufweisen. Insbesondere ging der Vortrag auch kurz auf den Anpassungsbedarf angesichts der kommenden Datenschutzgrundverordnung und der darauf aufbauenden Neuformulierung des Bundesdatenschutzgesetzes ein.

Die Datenschutzgrundverordnung ist (k)eine Zäsur - Prof. Dr. Mark D. Cole

Im zweiten Teil wurden die Auswirkungen der kommenden Datenschutzgrundverordnung erläutert. Herr Prof. Dr. Mark D. Cole, Wissenschaftlicher Direktor des EMR, stellte insbesondere die sich aus den gesteigerten und veränderten Betroffenenrechten ergebenden neuen Unternehmenspflichten dar. Dem Vortrag lag die Frage zugrunde, ob die Datenschutzgrundverordnung nun wirklich eine Neuerung sei. Um sich der Antwort zu dieser Frage zu näher, stellte Herr Prof. Dr. Cole zunächst die Genese der Datenschutzgrundverordnung dar. Bereits hier konnte man zum Ergebnis kommen, dass sie zwar vorhergehende Regelwerke wie die RL 95/46/EG beerbt, gleichwohl einen darüber hinausgehenden Regelungsgehalt aufweist. Dieser befindet sich in erster Linie in der Verbesserung der Betroffenenrecht, einer Anpassung der gesetzlichen Regelungen an das „Internet-Zeitalter", einer verstärkten Kontrolle der Betroffenen über ihre Daten und einer veränderten Rolle der Datenverarbeiter.

Im Vortrag konnte Herr Prof. Dr. Cole die bedeutsamsten Neuerungen an den Betroffenenrechten darstellen. Neben reinen Anpassungen bereits in den vorhergehenden Regelungen bestehender Rechte – wie beispielsweise das Recht

auf Löschung und Recht auf Sperrung – wurden mit der Datenschutzgrundverordnung auch neue Rechte eingeführt. Hierbei ist in erster Linie das Recht auf Datenübertragbarkeit zu nennen. Gleichwohl merkte Herr Prof. Dr. Cole bezüglich des neuen Rechts an, dass dieses in der Praxis sicherlich noch Probleme aufwerfen wird, was die technische Implementierung angeht. Die Frage der Implementierung im Betrieb sei jedoch keine singuläre Fragestellung, sondern eine Aufgabe, der sich die Unternehmen umfänglich widmen müssten. Betrachte man nämlich die sich aus den Betroffenenrechte für die Unternehmen ergebenden Verpflichtungen, müssen die Unternehmen nunmehr vielfach Vorbereitungen treffen, um den neuen Rechten der Betroffenen auch nachkommen zu können. Beispielsweise gilt es nunmehr, das Recht auf Löschung mit Tools und eines entsprechenden Workflows dem Betroffenen überhaupt zu ermöglichen.

In einem Ausblick auf die Rechtsmittel der kommenden Datenschutzgrundverordnung konnte Herr Prof. Dr. Cole die Möglichkeiten des Rechtsschutzes gegen die Datenschutzbehörden darstellen. Beachtenswert erschien ebenso die Konstruktion des Betroffenenvertreters, wonach eine betroffene Person das Recht hat, eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht zu mandatieren.

Aus der dargestellten Situation folgerte der Referent in erster Linie, dass mit der Datenschutzgrundverordnung die Rechte der Betroffenen verfeinert wurden und besser im modernen Kontext anwendbar werden. Neue Rechte erhöhen gleichzeitig den Wechsel von einem Datenverarbeiter zu einem andern und steigern wesentlich die Freiheiten der Betroffenen.

Zusammenfassend kann Herr Prof. Cole folgendes Fazit ziehen: „Die Verordnung ist mehr als alter Wein in neuen Schläuchen. Der europäische Datenschutz-Wein ist, um im Bild zu bleiben, gereift. Betroffene werden besser über die Datenverarbeitung informiert und bekommen mehr Mittel an die Hand, um die Verarbeitung ihrer personenbezogenen Daten kontrollieren zu können".

Werbeakquisition, Abo- und Vertriebsdaten, Datengewinnung im Web und bei Aktionen – Dr. Dominic Broy

Direkt anschließend an den vorhergehenden generellen Vortrag zur Datenschutzgrundverordnung, arbeitet Dr. Dominic Broy, Juristischer Referent am EMR, die datenschutzrechtlichen Herausforderungen heraus, welche die Medienunternehmen mit der Datenschutzgrundverordnung im Bereich der Werbung treffen werden. Der Vortrag ging die Aufgabenstellung mit einer Übersicht über die Voraussetzungen und Reichweite der zukünftig wichtigsten Erlaubnistatbestände an. Sofern das Unternehmen sich hinsichtlich der Werbedatenverarbeitung auf die Erlaubnisnorm zur Interessenwahrung berufen möchte, stellte der Referent die in diesem Bereich entscheidenden Punkte der notwendigen Interessenabwägung dar. Als zweiter möglicher Erlaubnistatbestand wurde die Einwilligung besprochen. Herr Dr. Broy konstatierte, dass die Voraussetzungen einer Einwilligung in der Praxis sehr unübersichtlich und unhandlich werden. Hinzu kommen Änderungen durch die Datenschutzgrundverordnung, welche insbesondere das Merkmal der Freiwilligkeit betreffen. Will man das damit verbundene Kopplungsverbot in strenger Auslegung verstehen, müssten Gewinnspiele, Gutschein- und Rabattaktionen immer mit der Möglichkeit versehen werden, auch ohne die Weitergabe der Daten zu Werbezwecken teilzunehmen. Ob sich diese Ansicht in Bereichen bei denen die Betroffenendaten faktisch die Bezahlung einer Dienstleistung sind letztendlich durchsetzen wird, müsse sich gleichwohl noch zeigen. Erste Anzeichen deuteten allerdings auf ein Einlenken der Aufsichtsbehörden hin. Der Referent beleuchtete auch das schwierige Verhältnis der Einwilligung zu anderen Erlaubnisnormen und zu Einwilligungen, welche noch in der

„Vor-Datenschutzgrundverordnungs-Zeit" eingeholt wurden. In beiden Fällen konnten praxistaugliche Lösungen skizziert werden.

Die Auseinandersetzung mit den Verarbeitungsgrundsätzen der Datenschutzgrundverordnung führte zum Ergebnis, dass an dieser Stelle ein Handlungsbedarf der Medienunternehmen besteht. Als Beispiel sei nur die Speicherbegrenzung genannt, deren Einhaltung die Unternehmen nun – etwa über Löschrichtlinien – nachweisen müssen.

Abseits der juristischen Fakten plädierte der Referent dafür, grundsätzlich einen Datenschutzbeauftragen grundsätzlich auch dann einzusetzen, wenn die gesetzliche Notwendigkeit nicht besteht. Diese kann als zentraler Ansprechpartner für die Werbekunden und intern als Steuerorgan der durch die Datenschutzgrundverordnung notwendigen Änderungen fungieren.

Zur Lösung der anstehenden Herausforderungen solle der Datenschutz als Prozess begriffen werden, der alle Geschäftsbereiche eines Unternehmens erfasse. „Es gilt, vorhandene Prozesse jetzt anzupassen, um Risiken zu minimieren, Chancen zu nutzen und aktiv an der Entwicklung eines modernen unternehmensbezogenen Datenschutzes teilzunehmen", hob Dr. Broy hervor.

Streitgespräch: Geschäftsmodelle vs. Datenschutz und ePrivacy

Am die Veranstaltung abschließenden Streitgespräch nahmen Vertreter der Medienunternehmen, wie auch der Datenschutzaufsichtsbehörden teil. Vertreten waren Dr. Stefan Hanloser, VP Data Protection Law, Syndikusrechtsanwalt der ProSieben-Sat.1 Media SE, Prof. Dr. Ulrich Wuermeling, Rechtsanwalt bei Latham & Watkins LLP für den DDV Deutscher Dialogmarketing Verband e.V. sowie Thomas Kranig, Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht in Bayern. Die Moderation erfolgte durch Herrn Prof. Dr. Stephan Ory, Direktor des EMR. In der Diskussion waren sich Medienvertreter, wie auch Vertreter der Aufsichtsbehörden einig, dass die sich abzeichnende und gleichwohl noch inhaltlich nicht finale E-Privacy-Verordnung weitere erhebliche Auswirkungen haben wird. Sollte die aktuell angedachte Fassung tatsächlich umgesetzt werden, würde diese die großen ausländischen Internetunternehmen bevorzugen und gerade lokale kleine und mittlere Unternehmen vor erhebliche Herausforderungen stellen. Seitens Herrn Kranig wurde betont, dass den Aufsichtsbehörden vor allem an einem konsistenten System gelegen seien und die finale Fassung der E-Privacy Verordnung noch nicht absehbar wäre.

Überhaupt spielte der mit der Datenschutzgrundverordnung kommende bürokratische Aufwand für die Unternehmen eine große Rolle für die Beteiligten. Dieser manifestiere sich in Nachweis- und Dokumentationspflichten. Gleichwohl sei dies für die größeren Unternehmen im Rahmen normaler Compliance Prozesse wie gehabt abzubilden, während kleinere Unternehmen diesen Aufwand zunächst mühsam in das Geschäftsmodell integrieren müssten.

Hinsichtlich der drohenden hohen Sanktionen bei Datenschutzverstößen kündigte Herr Kranig an, dass man zur Halbzeit der Zeit bis zur Umsetzung der Datenschutzgrundverordnung einen Fragebogen veröffentlichen werde, mit dem jedes Unternehmen seinen eigenen Umsetzungsstand prüfen könne. Die Datenschutzbehörden würden die Zeit bis zum Mai 2018 zudem als Umsetzungsfrist verstehen, eine Schonung hinsichtlich der Sanktionshöhe werde es nach diesem Datum nicht mehr geben.