4. OTURUM

ÖZEL HAYATIN GİZLİLİĞİ VE KİŞİSEL VERİLERİN KORUNMASI

Oturum Başkanı: Bilal ÇALIŞKAN

Federal Anayasa Mahkemesi İçtihadının Işığında Polis ve Güvenlik Hukukunda Kişisel Verilerin Korunması

Dr. Şeyda EMEK- Die voranschreitende Technologisierung und zunehmende elektronische Datenverarbeitung und elektronische Kommunikation bergen Chancen und Risiken zugleich. Sie ermöglichen dem Individuum, sich über territoriale Grenzen hinweg schnell und einfach zu vernetzen, zu kommunizieren und sich zu informieren. Den staatlichen Instanzen ermöglichen sie, elektronische Daten zu erheben und zu verarbeiten. Zugleich bergen die neuen Technologien aber auch Gefahren, sowohl für die Freiheiten des Individuums selbst als auch für den Staat.

Das Bundesverfassungsgericht hat früh erkannt, dass die Auswirkungen der technologischen Entwicklungen verfassungsrechtlich nicht unbeachtet bleiben können. Auf diese Rechtsprechung des Bundesverfassungsgerichts möchte ich im Folgenden eingehen. Insbesondere im Bereich des Polizei- und Sicherheitsrechts hat das Verfassungsgericht in den vergangenen Jahren wegweisende Entscheidungen getroffen. Stets war das Gericht dabei bemüht, einen Ausgleich zwischen dem Interesse des Einzelnen am Schutz seiner Privatheit gegenüber dem öffentlichen Interesse aus berechtigten Gründen in diese Privatheit einzugreifen.

Die Herausforderungen, vor denen das Gericht in diesen Fällen steht, treten besonders deutlich in dem Urteil zur sogenannten “Online-Durchsuchung” hervor. Damit sind heimliche Aufklärungsmaßnahmen der Polizei- und Nachrichtendienste gemeint. Hierbei beobachten die Behörden heimlich Internetkommunikation, nehmen an Internetkommunikation teil oder infiltrieren Computersysteme von verdächtigen Personen, um an gespeicherte Daten zu gelangen. Diese, für den Datenschutz bei polizeilichen und nachrichtendienstlichen Behörden wichtige Entscheidung möchte ich gerne mit Ihnen besprechen. Denn die Vorgaben des Verfassungsgerichts in diesem Urteil sind für die Verwaltungsgerichtsbarkeit von besonderer Relevanz. Zuständig für die Überprüfung des Einsatzes von technischen Mitteln in informationstechnische Systemen sind – jedenfalls bei Maßnahmen der Polizei in den Bundesländern, die Verwaltungsgerichte. Laut den

Polizei- und Ordnungsgesetzen der Bundesländer Rheinland-Pfalz und Bayern bedarf die Anordnung einer entsprechenden präventiv-polizeilichen Maßnahme der Überprüfung durch das Oberverwaltungsgericht. Dies ist bei Maßnahmen des Bundeskriminalamtes und des bayrischen Verfassungsschutzamtes anders, dort sind es die ordentlichen Gerichte.

Zunächst will ich ihnen zum besseren Verständnis kurz die allgemeine Entwicklung des Datenschutzrechts in der Rechtsprechung des Bundesverfassungsgerichts darlegen.

Das Grundgesetz enthält keine ausdrückliche Regelung, in der allgemeine verfassungsrechtliche Vorgaben für das Datenschutzrecht normiert sind. Ein Grundrecht, dass den allgemeinen Datenschutz ausdrücklich regelt, wie es z.B. im europäischen Recht, in Artikel 8 der Charta der Grundrechte der Europäischen Union existiert, gibt es im Grundgesetz nicht.

Im ersten Abschnitt des Grundgesetzes finden sich einige Grundrechte, die sich mit speziellen Fragen der Privatheit bzw. des Datenschutzes beschäftigen, dieses sind

Artikel 10 GG, der das Post- und Fernmeldegeheimnis regelt sowie Artikel 13 GG über die Überwachung von Wohnungen. Diese Grundrechte regeln aber nur einen Ausschnitt möglicher und datenschutzrechtlich relevanter Sachverhalte. (Hierauf werde ich im Folgenden noch eingehen).

Die verfassungsrechtlichen Vorgaben für das Datenschutzrecht wurden vom Bundesverfassungsgericht geschaffen. Die bedeutenste Entscheidung für die Entstehung des Grundrechts auf Datenschutz stellt das sogenannte Volkszählungsurteil vom 15. Dezember 1983 dar.

In diesem Verfahren hatte das Gericht über das Volkszählungsgesetz zu urteilen. Es war geplant, dass 1983 eine umfassende Volkszählung durchgeführt werden sollte. Auf Grundlage des Volkszählungsgesetzes sollten daher personenbezogene Daten erhoben werden. Diese Daten sollten nicht nur für die Volkszählung sondern auch zu anderen Zwecken verwendet werden. Bei den Meldeämtern sollten die Melderegister sollten mit den erhobenen personenbezogenen Daten auf ihre Richtigkeit und Vollständigkeit überprüft werden.

Aus diesem und vor allem auch aufgrund der damals neuartigen Datenverarbeitung war die Volkszählung sehr umstritten. Von zahlreichen Personen wurde befürchtet, dass ihre persönlichen Daten unkontrolliert erfasst und weitergeben würden.

Das Bundesverfassungsgericht hielt die Erhebung für die Volkszählung als solche für verfassungsgemäß. Für verfassungswidrig erachtete es indes die Verwendung der für die Volkszählung erhobenen personenbezogenen Daten zu weiteren Zwecken, die mit der Volkszählung nicht unmittelbar in Verbindung standen.

Das Gericht entwickelte zum ersten Mal allgemeine verfassungsrechtliche Maßstäbe für den staatlichen Umgang mit personenbezogenen Daten. Das Recht auf informationelle Selbstbestimmung wurde geboren.

Das Bundesverfassungsgericht leitet das Recht auf informationelle Selbstbestimmung zunächst aus Artikel 1 Abs. 1 GG ab. Artikel 1 Abs. 1 GG regelt, dass die Würde des Menschen unantastbar ist. Der Schutz der Würde des Menschen bedeutet u.a., dass der Einzelne in freier Selbstbestimmung Glied einer freien Gesellschaft ist. In Verbindung mit diesem Schutz der Würde des Menschen ist Artikel 2 Abs. 1 GG zu sehen. Artikel 2 Abs. 1 GG gewährleistet, dass jeder das Recht auf freie Entfaltung seiner Persönlichkeit hat. Diese beiden Gewährleistungen stellen die Grundlagen für das Recht auf informationelle Selbstbestimmung dar.

Bereits zuvor hatte das Bundesverfassungsgericht in seiner Entscheidung zum Mikrozensus im Jahr 1970 über die Grenzen staatlicher Informationserhebung und – Informationsverarbeitung zu entscheiden. (Beim Mikrozensus wird eine repräsentative Statistik der Bevölkerung und des Erwerbslebens erstellt).

Bereits damals bestimmte das Bundesverfassungsgericht, dass staatliche Informationserhebung und Informationsverarbeitung Eingriffe in das allgemeine Persönlichkeitsrecht darstellten. Es entschied, dass es mit der Menschenwürde nicht zu vereinbaren wäre, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren und ihn damit wie eine Sache zu behandeln.

Das Neue am Volkszählungsurteil war, dass das Bundesverfassungsgericht die Vorgaben des allgemeinen Persönlichkeitsrechts an die modernen Bedingungen der automatisierten Datenverarbeitung anpasste:

Die freie Entfaltung der Persönlichkeit setzt unter den Bedingungen der modernen Datenverarbeitung voraus, dass die persönlichen Daten des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe geschützt werden.

Das Grundrecht auf informationelle Selbstbestimmung gewährleistet dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Seit dem Volkszählungsurteil hängt es für die Beurteilung eines Datums als sensibel nicht mehr davon ab, ob einen intimen Vorgang betrifft. Denn unter den Bedingungen der modernen Informationstechnologie gibt es kein von vornherein belangloses Datum. Um festzustellen, ob ein Datum persönlichkeitsrechtliche Bedeutung hat, muss sein Verwendungszweck beurteilt werden.

Denn die modernen Mittel der Datenverarbeitung erlauben, dass erhobene Informationen beliebig zusammengeführt werden können, ohne dass der Einzelne die Richtigkeit und Verwendung kontrollieren könnte. Nach dem Bundesverfassungsgericht gilt aber:

"Wer nicht mehr überschauen kann, wer in einr Gesellschaft was, wann und bei welcher Gelegenheit über einen weiß, wird in der freien Entfaltung seiner Persönlichkeit und in der Ausübung von Freiheitsrechten, die auch für die Mitwirkung in einem demokratischen Gemeinwesen von Bedeutung sind, gefährdet."[1]

Das Recht auf informationelle Selbstbestimmung bedeuted jedoch nicht, dass der Einzelne ein eigentumsgleiches Recht an "seinen Daten" hat. Das Bundesverfassungsgericht hat festgehalten, dass der Mensch Teil einer miteinander kommunizierenden Gemeinschaft ist. Eine Information, auch wenn sie personenbezogen ist, ist eine soziale Realität. Diese soziale Realität kann nicht allein dem Betroffenen zugeordnet werden. Sie gehört ihm nicht allein. Aus diesem Grund muss der Einzelne auch Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Interesse der Allgemeinheit hinnehmen.[2]

Wichtig ist also, dass das Individuum für seine Entfaltungsfreiheit Transparenz über die Informationsbeziehungen bedarf. Jeder soll überschauen können, "welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind".[3] Die Rechtsordnung soll so eingerichtet sein, dass Transparenz herrscht; die Informationsströme und –sammlungen sollen jedermann bekannt sein.

Das Recht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet. Es gelten die Schranken des Artikels 2 Abs. 1 GG. Danach darf das Recht zum Schutze der Rechte anderer und der verfassungsmäßigen Ordnung beschränkt werden. Der Einzelne muss also Einschränkungen seines Rechts im überwiegenden Allgemeininteresse hinnehmen. Solche Beschränkungen bedür-

---

[1] Bundesverfassungsgericht (BVerfG), 65,1 ((45); Tute, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, 2.5 Rn. 10.

[2] Vgl. BVerfGE 65, 1 (44).

[3] BVerfGE 65,1 (42).

fen nach Artikel 2 Abs. 1 GG einer gesetzlichen Grundlage und müssen dem Prinzip der Verhältnismäßigkeit entsprechen.

Hinsichtlich der ersten Voraussetzung für einen zulässigen Eingriff in das Recht auf informationelle auf informationelle Selbstbestimmung, hat das Bundesverfassungsgericht im Volkszählungsurteil klargestellt, dass es einer hinreichend bestimmten gesetzlichen Grundlage bedarf.[4]

Dabei muss der Gesetzgeber den Verwendungszweck der zu erhebenden Daten bereichsspezifisch, das heißt für den jeweiligen Verwendungsbereich wie etwa das Polizeirecht, präzise festlegen.[5] Eine Weitergabe von Daten kommt grundsätzlich nur zu dem gleichen Zweck in Betracht, zu dem die Daten erhoben wurden. Zwar schließt die Zweckbindung einmal erhobener Daten eine nachträgliche Zweckänderung nicht aus. Diese Zweckänderung und die Übertragung der Daten an eine neue Stelle bedarf jedoch ihrerseits einer verfassungskonformen gesetzlichen Grundlage.[6]

Erforderlich ist außerdem, dass die Einschränkung des Rechts auf informationelle Selbstbestimmung verhältnismäßig ist. Das bedeutet, dass eine Grundrechtsbeschränkung von hinreichenden Gründen des Gemeinwohls gerechtfertigt wird. Dazu muss das gewählte Mittel zur Erreichung des Zwecks geeignet und erforderlich sein und bei einer Gesamtabwägung der Schwere des Eingriffs muss die Grenze des Zumutbaren noch gewahrt sein (Angemessenheit). In der Konsequenz sind zum Beispiel u.a. auch verfahrensrechtliche Schutzvorkehrungen, wie Aufklärungs-, Auskunfts- und Löschungspflichten etc. Vorzusehen.[7]

Diese Rechtsprechung hat das Bundesverfassungsgericht in seinem Urteil zur "Online Durchsuchung" fortentwickelt. Das Urteil zur Online-Durchsuchung ist neben dem eben vorgestellten Urteil zur Volkszählung aus dem Jahre 1983 in einer Gesamtschau mit sicherheitsrechtlich relevanten Urteilen des Gerichts zur präventiven Rasterfahndung[8] von 2006, zur Wohnraumüberwachung[9] und zur Telefonüberwachung[10] zu sehen. Auf die Telefonüberwachung und zur Wohnraumüberwachung komme ich sogleich zum Sprechen, da es hier eine gewisse Problematik zur Abgrenzung zur Online-Durchsuchung gibt.

---

[4] BVerfGE 65, 1 (44).
[5] BVerfG, a.a.O.
[6] BVerfGE 100, 313 (360).
[7] Vgl. BVerfGE 65, 1 (46).
[8] BVerfGE 115, 320.
[9] BVerfGE 109, 1.
[10] BVerfGE

Zum Fall der präventiven Rasterfahndung nur so viel: In diesem Urteil ging es darum, dass die Landeskriminalämter bei Universitäten, Meldebehörden und dem Ausländerzentralregister Daten erhoben. Die erhobenen Daten dienten dazu, nach den terroristischen Anschlägen vom 11. September 2001 ohne konkreten Verdachtsmoment nach möglichen islamistischen Terroristen zu suchen. Die Daten wurden dem Bundeskriminalamt übermittelt, dass sie mit weiteren Daten abglich und in einer Datei über potentielle Terroristen speicherte. Das Ergebnis des Abgleichs wurde sodann den Landeskriminalämtern übermittelt. Das Bundesverfassungsgericht entschied, dass eine bloß allgemeine Bedrohungslage, wie sie im Hinblick auf terroristische Anschläge seit dem 11. September 2001 durchgehend bestanden hatte, oder außenpolitische Spannungslagen für die Anordnung der Rasterfahndung nicht ausreichten. Vorausgesetzt sei vielmehr das Vorliegen weiterer Tatsachen, aus denen sich eine konkrete Gefahr, etwa für die Vorbereitung oder Durchführung terroristischer Anschläge, ergebe. Aus Datenschutzsicht besonders beachtenswert ist, dass das Gericht diese Art der Rasterfahndung als einen schweren Eingriff in die informationelle Selbstbestimmung wertete. Für den die verfassungsrechtliche Zulässigkeit der Maßnahme überprüfenden Richter ist es daher wichtig zu überprüfen, ob eine durch Tatsachen belegte „konkreten Gefahr" vorliegt. Falls keine Tatsachen dafür sprechen, liegt eine Verletzung des Rechts auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 GG vor.

Zurück zum Urteil um die sogenannte "Online-Durchsuchung". Hierbei ging es um die heimliche Ausspähung privater Datenträger und die Infiltration von technischen informationssystemen anhand von sogenannter "Trojanern"-Computersoftware. Das Land Nordrhein-Westfalen hatte eine ausdrückliche gesetzliche Ermächtigung zur Online-Durchsuchung für nachrichtendienstliche Behörden erlassen. Danach hatten die Verfassungsschutzbehörden die Befugnis zum "heimlichen Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel" sowie "das heimliche Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche in den Kommunikationseinrichtungen des Internets. Diese gesetzlichen Ermächtigungen wurden mit mehreren Verfassungsbeschwerden angegriffen.

Anlässlich dieses Urteils entwickelte das Bundesverfassungsgericht ein neues Grundrecht, das "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme". Die Gewährleistung dieses Grundrechts sei notwendig, weil weder die speziellen Freiheitsrechte noch die übrigen Ausprägungen des allgemeinen Persönlichkeitsrechts gegen die Gefahren hinreichend Schutz gewähren würden, die sich aus der zunehmenden Nutzung der

Informationstechnik ergäben.[11] Das Grundrecht ist, ebenso wie das Recht auf informationelle Selbstbestimmung ein Unterfall des Allgemeinen Persönlichkeitsrechts. Es ist also kein vollständig neues Grundrecht im eigentlichen Sinne. Es ist eine Konsequenz des Schutzes des Grundrechts auf Menschenwürde und auf freie Entfaltung der Persönlichkeit, die sich aus der modernen Datenverarbeitung und Kommunikationstechnologie ergeben.

Ausgangspunkt des Urteils ist die vollständige Veränderung der Kommunikation unter den Bedingungen und Möglichkeiten der modernen Technik und die vielfältigen, heute allgemein üblichen Verwendungen eines Personalcomputers. Diese Veränderungen der Wirklichkeit müsse beachtet werden, wenn die freie Entfaltung der Persönlichkeit und eine Kommunikation frei von Befangenheit, Anpassung und Angst bleiben solle. Denn bei der digitalen Kommunikation würden immer mehr bleibende Spuren entstehen. Dies würde neue rechtliche Antworten erfordern. Der Einzelne sei auf die Benutzung von informationstechnischen Systemen angewiesen, wenn er nicht in soziale Isolation geraten wolle.

Das neue Grundrecht sichere den persönlichen Bereich dann, wenn auf das informationstechnische System insgesamt zugegriffen werde.

Das Recht auf informationelle Selbstbestimmung biete hier keinen Schutz, da der Zugriff auf Daten bei der Online-Durchsuchung "in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen hinaus gehe". Das Recht auf informationelle Selbstbestimmung schütze lediglich gegen die Erhebung, Speicherung, Verwendung und Weitergabe einzelner personenbezogener Daten wegen der Gefahr der Persönlichkeitsprofilbildung. Bei der Online-Durchsuchung hingegen könnten besonders viele und besonders sensible Daten in einem Vorgang erhoben werden. Dies mache den Eingriff besonders gravierend.

Das neue Grundrecht gewährleiste die Vertraulichkeit des informationstechnischen Systems als solches. Der Persönlichkeitsbezug ist hier nur mittelbar und instrumentell. Das Gericht begrenzt den Schutz auf solche Systeme, die in hohem Maße Zugang zu personenbezogenen Daten ermöglichen.

Das Post- und Telekommunikationsgeheimnis aus Artikel 10 GG biete ebenfalls keinen ausreichenden Schutz. Das Telekommunikationsgeheimnis schütze vor den spezifischen Gefahren räumlich-distanzierter Kommunikation. Es schütze alle Telekommunikationsverbindungen, dies gelte unabhängig davon, ob es sich um eine inhaltliche Kontrolle der Kommunikation während eines andauernden Gesprächs oder ob es sich sich um bloße Verbindungsdaten wie die Daten die Verbindungsdaten des Anrufers oder seines Gesprächspartners, die

[11] Vgl. BVerfGE 120, 274 (303 ff.).

Dauer des Gespräches etc. handele. Sobald allerdings die Kommunikation beendet werde und der Inhalt des Gespräches möglicherweise abgespeichert und damit der Verfügungsgewalt des Kommunikationspartners unterliege, sei kein Fall des Telekommunikationsgeheimnisses mehr gegeben.

Nach dieser Rechtsprechung fällt auch ein über das Internet geführtes Telefongespräch (Voice over IP) grundsätzlich unter das Telekommunikationsgeheimnis. Dieses schützt gegen die Überwachung von laufenden und gesicherten Kommunikationsinhalten. Das heißt, der Staat nutzt bei dieser Art der Überwachung Zugangsschlüssel, die er ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hat. Als Beispiele für eine Betroffenheit des Telekommunikations- und Postgeheimnisses im Zusammenhang mit Online-Maßnahmen der Aufklärung nennt das Bundesverfassungsgericht die Erhebung eines Passwortes durch Aufzeichnen von Eingaben auf die Tastatur (Keylogging), um Zugang zu einem E-Mail-Postfach oder einen geschlossenen Internet-Chat zu erhalten.

Nicht geschützt durch das Telekommunikations- und Postgeheimnis ist nach der Rechtsprechung das Vertrauen, wenn einer der Kommunikationsbeteiligten dem Staat heimlich die Teilnahme an der Kommunikation ermöglicht, indem er den Zugang zur Verfügung stellt. Denn Artikel 10 GG schützt lediglich das Vertrauen darauf, dass eine Fernkommunikation als solche nicht von Dritten zur Kenntnis genommen wird, nicht aber das Vertrauen in den Kommunikationspartner.

Vor dem Urteil war in der Literatur auch diskutiert worden, ob die Online-Durchsuchung und fortlaufende Überwachung der Datenverarbeitung von Computern einer Wohnungsdurchsuchung vergleichbar ist. Dann wäre sie vom Schutz des Artikels 13 GG erfasst, der die Unverletzlichkeit der Wohnung schützt. Denn in diesem Rahmen wird auch vor dem nicht-körperlichen Eindringen in die Wohnung, also vor der Informationserhebung mittels technischer Hilfsmittel von außerhalb der Wohnung (sogenannter "Lauschangriff") geschützt. Da sich die meisten Computer in Wohnungen oder Betriebs- und Geschäftsräumen befinden, wurde der Online-Zugriff überwiegend als Eingriff in dieses Grundrecht gewertet. Das Bundesverfassungsgericht lehnte diese Bewertung ab.

Denn der Eingriff könne unabhängig vom Standort des Gerätes erfolgen. Ein raumbezogener Schutz könne daher die spezifische Gefährdung es informationstechnisches Systems nicht gewährleisten. Die Unverletzlichkeit der Wohnung ist daher nur betroffen, wenn die Online-Durchsuchung dadurch ermöglicht wird, dass Mitarbeiter der Ermittlungsbehörde nach dem körperlichen Eindringen in den räumlichen Bereich der Wohnung einen Computer manipulieren oder die

Manipulation des Computers zur optischen oder akustischen Überwachung der Wohnung als solche durch Kamera oder Mikrophon dienen soll.

Mit allen diesen genannten Gründen hat das Bundesverfassungsgericht die Notwendigkeit des neuen Grundrechts begründet.

Hinsichtlich der Grenzen des neuen Rechts wendet das Gericht, wie auch beim Recht auf informationelle Selbstbestimmung und dem Allgemeinen Persönlichkeitsrechts das Verhältnismäßigkeitsprinzip an. Der die Zulässigkeit einer Online-Durchsuchung überprüfende Richter muss beachten, dass Eingriffe durch die Online-Durchsuchung besonders schwer wiegen, weil sie heimlich erfolgen.

Deshalb bedürfen sie einer speziellen gesetzlichen Grundlage, die insbesondere dem Bestimmtheitsgebot entsprechen muss.

Weil die heimliche Maßnahmen gravierende Eingriffe in die individuelle Lebensgestaltung des Individuums und Gefahren für den Kernbereich persönlicher Lebensführung bedeuten, muss bei der Anordnung der Maßnahme geprüft werden, ob der Eingriff zum Schutz überragend wichtiger Rechtsgüter unerlässlich ist. Dies trifft zu bei der Abwehr von konkreten Gefahren für Leib, Leben und Freiheit einer Person oder für "Güter der Allgemeinheit", deren Bedrohung die Grundlagen oder den Bestand des Staates, die Grundlagen der menschlichen Existenz und die Funktionsfähigkeit unverzichtbarer öffentlicher Versorgungseinrichtungen.

Besonders wichtig ist auch hier, dass konkrete Tatsachen vorliegend müssen, die für den gegebenen Einzelfall sowohl auf mögliche Täter, als auch darauf hinweisen müssen, dass sich die Gefahr ohne das Eingreifen in naher, absehbarer Zeit verwirklichen wird. Dies hat ein die Anordnung der Maßnahme überprüfender Richter sehr genau zu prüfen.

Denn ohne eine solche existenzielle Bedrohung ist eine staatliche Maßnahme, durch die die Persönlichkeit eines Betroffenen einer weitgehenden Ausspähung preisgegeben wird, grundsätzlich nicht angemessen und damit verhältnismäßig ist.

Neben diesen inhaltlichen Vorgaben verlangt das Gericht, genauso wie beim Recht auf informationelle Selbstbestimmung, dass bei Eingriffen in das Grundrecht auch besondere verfahrensmechanismen zum Schutz des Einzelnen gewährleistet sind.

Danach bedarf der Eingriff einer vorherigen richterlichen Anordnung oder der Entscheidung einer unabhängigen Instanz. Dies dient dem Schutz der Rechte des von dem Eingriff nichtinformierten Betroffenen. Eine solche unabhängige

Instanz kann z.B. ein nichtöffentlich tagendes Kontrollgremium des Parlaments sein.

Die nachträgliche Benachrichtung des Betroffenen und der besondere Schutz des Kernbereichs persönlicher Lebensführung müssen gesichert sein.

Daten des Kernbereichs persönlicher Lebensführung dürfen nicht erhoben werden, soweit das voraussehbar ist.

Da "Trojaner-Software" nicht nach Kernbereichs- und anderen Daten unterscheiden können, muss durch besondere Verfahrensvorschriften gesichert sein, dass diese Daten unverzüglich vor jeder Verwendung gelöscht werden, soweit sie erhoben worden sind.

Im Bereich der Beweiswürdigung in einem späteren Strafprozess ist auch zu beachten, dass der gesamte Datenbestand des infiltrierten Computers durch den Einsatz eines "Trojaners" irreversibel verändert werden kann, sodass die gerichtliche Verwertbarkeit der erlangten Daten erschwert werden kann.

Ich komme nun zum Fazit meines Vortrages.

Die vorgestellten Entscheidungen bestätigen die Entschlossenheit des Bundesverfassungsgerichts, an seiner Rechtsprechung zum Schutz des Rechts auf informationelle Selbstbestimmung und des Kernbereichs der privaten Lebensführung auch angesichts neuer technologischer Gefahrenlagen festzuhalten.

In dem Urteil zur Online-Durchsuchung hat das Gericht sein Konzept des unantastbaren Schutzes des Kernbereichs privater Lebensgestaltung fortgeführt und der neuen Qualität des Internets Rechnung getragen. Die Entscheidung ist nicht ohne Kritik geblieben. Insbesondere die Schaffung eines neuen ungeschriebenen Grundrechts wurde kritisiert. In der Literatur wird stattdessen diskutiert, ob nicht die Erweiterung des Schutzumfangs des Rechts auf informationelle Selbstbestimmung oder der Unverletzlichkeit der Wohnung und damit des Kernbereichs persönlicher Lebensführung ausgereicht hätten. Das Urteil wird die Rechtsprechung, Rechtswissenschaft und Gesetzgebung noch länger beschäftigen.

Kişisel Verilerin Korunması

Prof. Dr. Cemil KAYA:

Değerli katılımcılar bugün tebliğimin konusu "Türk Hukukunda Kişisel Verilerin Korunması" olacak. Ama takdir edersiniz ki, çok geniş bir başlık. Keşke daha dar kapsamlı olarak bunu tespit etseydim. Ben idare hukuku boyutuyla olayı ele alıp, o şekilde sizlere aktaracağım. Tabi kişisel verilerin korunması konusu,

Başkanımız da belirtti, Türkiye'nin aslında, çok eski zamandan beri değil, yakın zamandan beri gündemini oluşturan bir şeydir. Bunu da nereden biliyoruz, Başbakanlığın hazırlayıp, Meclise sevk etmiş olduğu 24 Nisan 2008 tarihli bir bu konuda Kişisel Verilerin Korunması Kanunu Tasarısı nedeniyle aslında Türkiye bu konuyu gündeme getirmiş oldu. Bu Kanun Tasarısının hazırlanmasında da Türkiye'nin Avrupa Birliği'ne vermiş olduğu söz yatmaktadır. Avrupa Birliği Müktesebatının kabulü açısından bu şekilde verilen bir sözün sonucunda bu Kanun Tasarısı hazırlanmıştır. Başkan Bey az önce söyledi, Avrupa Konseyi'nin 108 sayılı bir tane sözleşmesi var. İmzaya açıldığı gün, 28 Ocak 1981, ilk belki de defa, bütün üyeler arasında ilk imzayı atanlardandır Türkiye 1981'de. Ama aradan geçen, hani neye imza attığını inşallah biliyordur o dönemde. Ama aradan geçen zaman, yıl otuz üç yıl, imza atan, onaylayan ve yürürlüğe koyan diğer bütün ülkeler de, yaklaşık kırk dört tane ülke, hepsi bunu sonuçta yasalaştırmıştır. Ama Türkiye maalesef bu konuda adımlarını atamamıştır. Ben müsaadenizle genel olarak kişisel veriler konusunda birkaç bir şey söyledikten sonra hem kişisel veri kavramını, hem bunun tarihi gelişimini, çok kısa uluslararası alandaki gelişimini, ardından da Türk Hukukunda birkaç bir şey söylemek istiyorum. Bu Sözleşmenin de adı böyle, "Kişisel Verilerin Otomatik İşlenmesi" diyor, "otomatik işleme tabi tutulması" diyor. Bu anlamda, bir takım kişiler hakkında kayıtlar tutuluyor, gerek elle olsun, gerek bilgisayar yoluyla olsun, ve sair yollarla olsun. Hatta buna "otomatik işlenme" adını veriyorlar doktrinde. Bu işte, ister otomatik işlem yoluyla, ister elle tutulmuş olsun bu kayıtlardaki verilere biz "kişisel veri" yahut da "isme bağlı veri" adını veriyoruz.

Uluslararası kabulde, uluslararası düzenlemelerde, hem kanunlarda, hem uluslararası sözleşmelerde kişisel verilerin aslında standart bir tanımı vardır: Belirli bir kişiyle veya belirlenebilir bir kişiyle ilgili her türlü veridir. Belirli bir kişi, spesifik, somut, müşahhas bir kişi veya verilerden yola çıkmak kaydıyla bu verinin biz kime ait olduğunu eğer tespit edebiliyorsak, yani belirleyebiliyorsak, bu verilere biz kişisel veri adını veriyoruz. İşte örnek vermek gerekirse, bir kişinin ismi olsun, fotoğrafı olsun, e-mail adresi olsun, banka hesap numarası olsun, web siteniz olsun, tıbbi bilgilerimiz olsun, bilgisayarımızın IP numarası söz konusu olsun, hep bu kategoride değerlendirilir. Kişisel veriler üzerinde, az önce Şeyda Hanım da söyledi, Alman Anayasa Mahkemesi'nin meşhur bir kararı vardır, nüfus sayımı kararı söz konusudur 1984 tarihli bir karardır bu. Çok fazla Türkiye'de de aslında incelenmiş bir karar da değildir bu ama çok güzel Şeyda Hanım açıkladı. Orada bir şey dikkatimizi çekiyor, ben çok fazla ayrıntıya girmeyeceğim, sadece şunu söylemek istiyorum; kişisel verilerin akıbetini belirleme hakkı olduğunu bireylerin, kişilerin, böyle çarpıcı bir tespit. Kişisel verilerin akıbetini belirleme hakkından bahsediliyor bu kararda. Kişisel verilerin

korunması hukukta "veri koruma" olarak ifade ediliyor. Zaten kanunların adı da budur, kişisel verilerin korunması kanunlarıdır. Tabi bu kanunlarla bilgi edinme kanunlarının da çok yakın bir ilişkisi söz konusudur. Adeta bilgi edinme kanunları ile kişisel verilerin korunması kanunları bir paranın ön ve arka yüzü gibidir. Böyle herhalde söylesek, yanlış olmaz diye düşünüyorum. Veri koruma, İngilizce "data protection", tabi bu kavramın etimolojik olarak belirsiz olduğu ileri sürülmüş, ancak bu kavramı yine Almanlar bulmuş diye okudum kitaplarda, bir takım bilgilere rastladım. Artık Almancam yok, bağışlayın, "datenschutz" mu okunuyor bilmiyorum, bu şekilde buraya yazmışım. Yani orijinal olarak kavram Alman Hukukuna, Almanya'ya dayanmaktadır, bunu söyleyebiliriz. Ulusal ve uluslararası tabi birçok metinde veri koruma ele alınmıştır.

Uluslararası alanda çok sayıda düzenleme var ama iki tanesini örnek vermek istiyorum, bir tanesi OECD'nin 1980 tarihli "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Transferi Hakkında Rehber İlkeler" diye bir ilkeler yayınlamıştır. Bağlayıcı değildir, ama yine baktığımızda 1980, kişisel verilerin sınır ötesi transferi de daha sonradan gelişen bir kavramdır ama buna rağmen gerçekten önemli, kayda değer bir uluslararası belgedir. İkincisi de meşhur, hepimizin bildiği 28 Ocak 1981 tarihli ve 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme"dir bu sözleşme. 1981 tarihli olduğunu söylemiştim. Türkiye 1981 yılında Sözleşme'yi imzalamıştır ama onaylamamıştır. Bu sözleşmeye, o da önemlidir, 2001 yılında bir ek protokol yapılmıştır; 181 sayılı Ek Protokol, Ek Sözleşme. Bu Ek Sözleşmede de, ilk Sözleşmede yer almayan, 1981 tarihli Sözleşmede yer almayan iki şey ilave edilmiştir: Bir; bağımsız idari otoriteler dediğimiz bir otoritenin bu Kanun'un işlenmesini gözetmek amacıyla yapılandırılması gerekir demiştir. İkincisi de; kişisel verilerin sınır ötesi transferi konusu, bu 181 sayılı Sözleşme ile ek yapılmıştır. Bu Sözleşme ile, 181 sayılı Sözleşme ile Türkiye yine aynı gün, 8 Kasım 2001, imzaya açıldığı ilk gün imzalamıştır. Ama aradan geçen on üç yıla rağmen bu sözleşmeyi imzalamamıştır. Ama diğer ülkeler de vardır imzalamayan, onaylamayan ve yürürlüğe koymayan. Bunu da söyleyelim. Avrupa Birliği'nde ise 1973 yılında başlayıp bugüne kadar gelen çok sayıda karar, tavsiye kararı vardır konuyla ilgili. Avrupa Birliği Temel Haklar Şartı'nda buna ilişkin spesifik bir madde vardır, 8. madde. Avrupa İnsan Hakları Sözleşmesi'nde ise doğrudan kişisel verilerin korunması diye bir şey yoktur, sadece Sözleşme'nin 8. maddesi kapsamında "Özel ve Aile Yaşamının Korunması" başlığı altında konunun değerlendirildiğini görüyoruz. 1 Aralık 2009'da yürürlüğe giren Lizbon Antlaşması ile de, bu Antlaşmanın 16. maddesinde konu düzenlenmiştir. Yine Avrupa Birliği'nde bir direktif vardır, 1995 tarihli, 95/46 sayılı, "Kişisel Verilerin İşlenmesiyle İlgili Olarak Bireylerin Korunması ve Bu Verilerin Serbest Dolaşı-

mı Direktifi" adını veriyoruz. Direktif, yabancı kitaplarda "Avrupa Birliği Özel Yaşamın Korunması Direktifi" olarak geçiyor. 1998 yılında hemen yürürlüğe girmemiş, üç yıl sonra yaklaşık yürürlüğe girmiştir. Önemli bir direktiftir. Bunun bu günlerde veya bu yıllarda, direktif, tabi biraz eski addedilerek değiştirilmesi, yeni bir direktif yürürlüğe girmesi Avrupa Birliği'nin gündemindedir. Yine keza Avrupa Birliği'nde Avrupa Toplulukları Adalet Divanı'nda konuya ilişkin olarak vermiş olduğu kararlar mevcuttur. Ulusal alanda ise bu konuda karşınıza şu çıkmaktadır; bazı ülkeler kişisel verilerin korunması konusunu anayasa ile güvence altına almış, bazıları hem anayasa hem kanun ile, bazıları ise sadece kanunlar ile düzenleme altına almıştır. Bu açıdan baktığımızda, ülkelerde üç tür yaklaşım göze çarpmaktadır. Birinci yaklaşım genel bir veri koruma kanununu çıkartmak yaklaşımıdır. "Omnibus Approach" adı veriliyor. Bu daha çok Avrupa Konseyi'ne üye ülkeler tarafından benimsenmiş bir yoldur. Genel bir bu alanda kanun çıkartmak bu. İkincisi daha ziyade Anglosakson ülkelerde ortaya çıkan Amerika olsun, İngiltere olsun, Yeni Zelanda, Avustralya farklı sektörler işte, ulaşım sektörüne, eğitim sektörüne, telekomünikasyon sektörüne, farklı sektörlere ilişkin bir anlamda "Özel Yaşamın Gizliliği Kanunları" çıkartılması şeklinde karşımıza çıkıyor. Üçüncü yaklaşım da "Habeas Data" diye adlandırılan, anayasalarda kişilere bir hak getiren "Habeas Data Bireysel Şikâyeti" olarak adlandırılan bir yaklaşımdır. "Habeas Data"yı yine İngilizce kitaplarda "veriye sahip olmalısın" yahut da "verine sahip olmalısın" şeklinde tercüme edildiğini görüyoruz. Bu yaklaşımda bireyler, mahkemeye verecekleri dilekçelerle kişisel verilerinin korunmasını istiyorlar. Daha ziyade bu Latin Amerika ülkelerinde karşımıza çıkan bir yaklaşımdır.

Gelelim Türk Hukukuna. Türk Hukukunda, az önce de ifade ettiğimiz gibi, genel bir kanun söz konusu değildir. Tasarıda birinci yaklaşım, yani genel bir veri koruma kanunu çıkartmak şeklinde olacaktır. Yalnız, iyi bir gelişme belki de, ama geliştirilebilir bir gelişme. 2010 yılında Anayasamızda 20. maddede, özel yaşamın korunmasına, gizliliğine ilişkin maddede, bir son fıkra eklenerek, kişisel verilere bir anayasal zemin kazandırılmıştır. Bu maddeye baktığımızda *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* diyor. Şimdi Anayasa'nın hükmü bu şekilde. Kanaatimce sadece birinci ve son cümle yasada yer alsaydı yeterli olurdu diye düşünüyorum. Yani *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Kişisel verilerin korunmasına ilişkin*

esas ve usuller kanunla düzenlenir." denseydi yeterli olurdu diye düşünüyorum. Çünkü diğerleri teferruattır aslında, onların kanunla düzenlenmesi ve her birinin ayrı bir madde olarak, bazılarının belki bir ilke olarak düzenlenmesi gerekirdi. Bu şekildeki bir düzenleme hükmün eksik kalmasına da yol açmaktadır. Örneğin, sondan bir önceki cümle *"Kişisel veriler, ancak kanunda öngörülen hallerde işlenebilir*" diğer taraftan araya *"veya kişinin açık rızasıyla işlenebilir."* diyelim, yani kişinin açık rızasını da getirmiş. Zaten kişisel verilerin korunmasıyla ilgili kanuna baktığımızda, kişisel verilerin işlenmesinin ilk şeyidir, ilk halidir kişinin açık rızasının bulunması. Diğerlerini de altta sıralar. Dolayısıyla bunun bu şekilde düzenlenmesi kanaatimce çok da isabetli olmamıştır. Türk Hukukunda bu konuda genel bir kanun olmadığını söyledik. Zaten Avrupa Konseyi'ne ilişkin 181 sayılı Sözleşmeyi Türkiye'nin imzalayamamasının da sebebi bu konuda çıkarttığı bir kanunun da bulunmamasıdır, tabi bunun da önemli etkisi söz konusu. Bu konuda hepimizin bildiği 27 Nisan 2008 tarihinde Meclise sevk edilen Kişisel Verilerin Korunması Kanun Tasarısı mevcuttur. Resmi olarak da herkes tarafından bilinmektedir. Diğer taraftan duyduğumuza göre bunun dışında bir tasarının da hazırlandığı ve Başbakanlığa sevk edildiği yönünde bir bilgi de mevcuttur, bunu da parantez içinde aktarmak istiyorum. Bu Tasarıya baktığımızda, aslında hem Bilgi Edinme Hakkı Kanunumuzun biz de 2003 yılında kabul edildiği, 2004 yılında yürürlüğe girdi. Hem de Kişisel Verilerin Korunması Kanun Tasarısı olsun, Kanunu olsun hemen hemen aslında bütün dünyadaki kanunlarda ne varsa, ana çatı aynıdır, bir defa onu söyleyeyim. Bizde de bu Kanun Tasarısı, diğer Avrupa Birliği ülkelerinde ne söz konusuysa, onun bir anlamda, tabii ki bizim Türk Hukukuna uyarlanma kaydıyla tasarının hazırlanması şeklinde karşımıza çıkmaktadır. Bu tasarıya baktığımızda, tasarının kırk bir maddeden oluştuğunu görüyoruz. Bir defa genel hükümler vardır, bütün kanunlarda olan. Kanunun amacı nedir, kapsamı nedir, tanımlar nelerdir. İkincisi, kişisel verilerin işlenmesine ilişkin temel ilkeler nelerdir, bunlar mevcuttur. Üçüncüsü, veri sahibinin hakları ne olacaktır, bunlar yer almaktadır. Kişisel verilerin üçüncü ülkelere aktarılması, kişisel verilerin transferi adını veriyoruz, bu mevcuttur. Ve bir düzenleyici ve denetleyici kamu kurumu oluşturulduğunu görüyoruz. Kişisel verilerle ilgili bir Kurul oluşturulduğunu görüyoruz. Ve son hüküm, Kanunun ceza hükümleri, bunu da Kanunda görüyoruz. Çok kısa olarak Kanunun amacının, aslında güzel bir şekilde formüle edildiğini söylemek mümkündür. *"Kişisel verilerin işlenmesinde, kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemektir."* diyor Kanun amacında. Kişisel verileri, *"kişisel veriyle belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler, bütün veriler"* olarak tanımladığını görüyoruz. Tabi veri koruma hukukunda bir tartışma; veri koruma acaba sadece gerçek kişilere mi özgüdür, yoksa tüzel kişilere mi özgüdür? Bunu da buradan görmek mümkün.

Bu anlamda bazı ülkeler kişisel verilerin sadece gerçek kişiler için söz konusu olabileceğini ve dolayısıyla veri koruma kanunlarının kapsamına kişisel veri adı altında bunların girebileceğinden hareketle, sadece bu kanunları gerçek kişilere özgülemektedir. Ama trend diyelim, kişisel verilerin hem gerçek kişilere ilişkin, hem de tüzel kişilere ilişkin olabileceği yönündedir. Bu anlamda kanunların kapsamına hem gerçek kişiler, hem tüzel kişileri sokmaktadır kanun koyucular. Kişisel verilerin işlenmesi tanımlanmış Kanunda. Şöyle düşünelim; kişisel veri, o verinin hazırlanması, kaydedilmesi, depolanması, bulundurulması orada, zaman içerisinde değiştirilmesi, yok edilmesi, bir kişiden bir kişiye aktarılması yahut da bir ülkeden diğer bir ülkeye aktarılması, bunun aleni hale getirilmesi, tasniflenmesi yani, veri üzerinde yapılabilecek hemen hemen bütün işlemler veri işleme kavramı ile, processing kavramı ile ifade edilmektedir. Oldukça geniş bir anlama sahip olan bir kavramdır veri işleme kavramı. Temel ilkeler acaba nelerdir, kişisel verilerin işlenmesine ilişkin temel ilkeler? Bunları da Tasarıda görmek mümkündür. İşte kişisel veriler hukuka ve dürüstlük kurallarına uygun olarak işlenecek, belirli, açık ve meşru amaçlar için toplanacak ve bu amaçlara aykırı olarak yeniden işlenebilecek, toplandıkları amaçla bağlantılı, yeterli ve orantılı olacak, doğru olacak, gerektiğinde güncellenecek, belli süre öngörülmüşse ancak o süre için muhafaza edilebilecek, yani, rızasıyla işlenebilecek, bir takım hükümleri bu anlamda görmek mümkündür. Şunu da hemen ifade edeyim, kamuoyunda da var, sanki kişisel verilere ilişkin bir kanun çıktığında, bize ilişkin hiç artık, bizim rızamız olmadan veri işlenemeyecek diye böyle bir algı da söz konusu. Bu basında da yer almakla birlikte, hiç de öyle değildir. Bizim rızamız yok diye kişisel verilerin işlenememesi söz konusu değildir. Onun dışında, eğer Kanun öngörüyorsa, istisnalar vardır. Hiç bizim haberimiz olmasa dahi kişisel verilerimizin işlenmesi mümkündür. Yine Şeyda Hanım da kısmen bahsetti; yine bütün bu veri koruma kanunlarında "hassas kişisel veriler" diye bir kategori de söz konusudur. Buna ülkelerin farklı anlamlar verdiği olmuştur kanunlarında. Özel niteliği olan kişisel veriler, hassas kişisel veriler, sensitiv kişisel veriler. Bu ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, dernek, vakıf veya sendika üyeliklerimiz, sağlık ve özel yaşamımız, her türlü mahkûmiyete ilişkin verilerimiz, bir defa kuraldır işlenememesi, ama bunun dahi istisnaları vardır kanunlarda. Bu nitelikteki, hassas nitelikteki kişisel verilerimizin dahi bütün veri koruma kanunlarında işlenmesine ilişkin hükümler mevcuttur. Tasarıda veri sahibinin hakları düzenlenmiştir. Yine bütün kanunlarda olduğu gibi bizim Tasarımızda da kişisel verilerin, kendisiyle ilgili kişisel veri kaydedilip kaydedilmediğini öğrenmek, kaydedilmişse bunları talep etmek, bunun düzeltilmesini, silinmesini yahut da yok edilmesini talep etmek hakkı mevcuttur veri sahibinin. Bu istemlere, taleplere on beş iş günü içerisinde cevap verilmesi gerektiğini söylüyor tasarı. Eğer talebine cevap verilmezse yahut da yeterli olmaz ise düzenleyici ve denetleyici kamu kurumuna

itiraz hakkı getiriyor tasarı. Yirmi gün içerisinde itiraz hakkı getirmiştir. Kurulun da itirazı üç ay içinde karara bağlaması, tasarıda mevcuttur.

Evet, kişisel verilerin üçüncü ülkelere aktarılması. Yine bütün kanunlarda böyle bir madde veya maddeler de mevcuttur. Avrupa Birliği'ndeki bu konuda temel kriter üçüncü ülkede "eşdeğer ve etkin koruma" sağlanıyor mu sağlanmıyor mu. Bu eğer sağlanıyorsa, bu verilerin Avrupa Birliği'nden üçüncü ülkelere transferi, aktarılması mümkün olabilmektedir. Tabi sadece belge üzerine aktarma değil, bir internet ortamına aktarılması da, o çok geniş bir kavramdır kişisel verilerin transferi kavramı. Bu anlamda bu alanı düzenlemek de son derece zordur. Özellikle Anglosakson, Anglo-Amerikan ülkelerde birden fazla alanı düzenleyen düzenlemeler, kanunlar söz konusu olduğu için, tek tip veri koruma kanunu söz konusu olmadığı için alanın düzenlenmesi gerçekten, bu anlamda zordur. Avrupa Birliği'nin beyaz liste ve kara liste diye adlandırdığımız bir uygulaması vardır. Bildiğim kadarıyla bugüne kadar hiçbir ülkeyi Avrupa Birliği kara listeye almamıştır. Ama beyaz listeye aldığı, yani yeterli düzeyde veri koruma kanununa sahip olduğunu bizzat tescil ettiği ve bu kararlarını da Avrupa Birliği'nin resmi gazetesinde yayımladığı ülkeler vardır. İşte Yeni Zelanda, Uruguay, İsrail, Andorra, Faroe Adaları, Avustralya, Jersey, Arjantin, Kanada, Amerika Birleşik Devletleri, İsviçre bunlar arasında yer almaktadır. Macaristan kararda vardı ama Avrupa Birliği olduğu için onu da öyle söyleyelim. Bizdeki veri koruma kuruluna gelelim tasarıda. Tasarıyla, kanunla, "Kişisel Verileri Koruma Kurulu" oluşturulmaktadır. Yetkilerini bağımsız olarak kullanıyor. Hiçbir organ, makam, mercii ve kişiden emir veya talimat almıyor. Organlar emir ve talimat veremiyor. Görevleri ile ilgili olarak özel ve kamu kesiminden bilgi ve belge isteyebiliyor. Bu isteklerin yerine getirilmesi mecburi. Kurul üyelerini Bakanlar Kurulu seçiyor. Yedi kişiden oluşan bir kurul. Görev süresi altı yıl ve ayda en az iki defa toplanması düzenlenmiş tasarıda. Ve son başlık tasarıda, ceza hükümleridir. Kişisel verilerin hukuka aykırı olarak işlenmesini suç saymış tasarı. İşlenen verilerin korunması ve yok edilmesi görevi ihmali suç sayılmış. Tüzel kişiler hakkında güvenlik tedbiri uygulanması düzenlenmiş ve idari para cezaları kanunla getirilmiş. Aslında benzer ceza hükümleri Türk Ceza Kanunu'nda da mevcuttur. Her ikisinin birbiriyle uyum halinde olması, yahut da orada olmaması burada olması, burada olmaması orada olması şeklinde bir düzenleme belki daha isabetli olabilir. Sonuç olarak, tabii ki bu tasarının kanunlaşmasını dilemekten başka çok da fazla bir şey söylemek istemiyorum. Avrupa Konseyi'nin Sözleşmesi 28 Ocak 1981 tarihini taşıyor. Dolayısıyla bizim tasarımızın da ümit ediyorum ki en geç, 28 Ocak 2015'ten önce kanunlaşmasıdır. Hepinize teşekkür ediyorum.

Bilal ÇALIŞKAN- Cemil Hocama teşekkür ediyoruz. Ben de son derece gizli, hassas bir şey paylaşayım sizinle. Yarın sabahki oturum başkanı, bizim de

konuşacağımız, Cemil Hoca. Onun için kendisine torpil geçtim yani. Çok teşekkür ederiz, çok sağ olun. Kişisel verinin ne olduğu ve nasıl koruma altına alınması konusundaki çalışmalar idare hukuku açısından önemli. Ceza hukuku açısından Ceza Muhakemesi Kanunu'nda ve diğer bazı kanunlarda düzenlendi. Fakat hepsi bölük pörçük, herkes nereden ne alacağını çok iyi bilemiyor. Ve onun için de çok sağlıklı bir durum söz konusu olmuyor. Biz, mesela Hocam gösterdi, kırk altı tane Avrupa Konseyi üyesi ülke taraf 108 sayılı Sözleşme'ye. Uruguay dışarıdan taraf olmuş, yürürlüğe de koymuş. Avrupa Konseyi'nin öyle bir özelliği var, Rusya 2013 yılının sonlarına doğru, dokuzuncu ayda taraf oldu, yürürlüğe koydu ve Türkiye hala bekliyor, otuz üç yıldır. Bu Sözleşme neyi getirir, neyi götürür ama bir kere Türkiye'nin imajını kötü zedelediği bir gerçek. Umarım bu noktada daha ciddi bir çalışma olur ve Meclis de önemli bir görevi ifa eder. Teknolojik gelişmeler neticesinde bir takım haklarımızın nasıl daha iyi korunmasını sağlayabilirizi daha net ortaya koyarız yani. Siber Suçlar Sözleşmesine de bu bağlamda imza koyduk ama taraf olmamız ne zaman olur, onu bilemiyorum. Evet soruları alalım. Herkes pür dikkat. Evet Musa Bey, buyurun. Kendinizi tanıtırsanız.

Musa ALBAYRAK- Musa Albayrak, Danıştay 6. Daire Üyesi. Sayın Hocam sizi dikkatle dinledim. Kişisel Verilerin Korunması Hakkındaki Yasa Tasarısı'nı gayet güzel izah ettiniz. Yalnız ben mi kaçırdım bilemiyorum. Kişisel verileri toplama hak, görev ve yetkisinin hangi kuruma, kuruluşa ait olduğu noktasında, yani devlet kamu yönetim birimlerine mi, yoksa gerçek ve özel kişiler de bu şeyi kullanabilir mi? Örneğin, on bin işçi çalıştıran bir özel sektör kuruluşu, istihdam ettiği işçilerin sosyo-ekonomik yapılarını, aile yapılarını, istihdam şekillerini, sağlık sorunlarını, psikolojik sorunlarını test etmek için, daha iyi bir istihdam politikası geliştirmek için birçok veriyi istihdam ettiği işçilerden isterse, bu bir kişisel veri toplama mıdır? Aynı şey eğitim-öğretim kurumlarında da geçerli. Eğitim-öğretim faaliyetinin daha düzenli yürütülmesi bakımından öğrencilerden birçok bilgi isteniyor. Ekonomik yapısından, sağlık, aile, özel hayata varacak kadar bir takım sorular yöneltiliyor. Bu bir kişisel veri toplama olarak, tırnak içinde söylüyorum, bu bir fişleme midir?

Prof. Dr. Cemil KAYA- Teşekkür ediyorum sorunuz için. Tabi haklısınız, ben aslında Kanun Tasarısının amaç maddesini okuduğumda, orada kişisel veri işleyen gerçek ve tüzel kişilerin uyacakları esas ve usulleri düzenlemektir diyor. Dolayısıyla kişisel verilerin işlenmesi konusunda yetkili sadece kamu kesimi değil, özel kesimde yer alan gerçek ve tüzel kişiler de bu kanun kapsamında, bu sorumluluklara uymak zorundalardır. Bu anlamda, burada düzenlemeler ne ise, kişisel verilerin işlenmesinde hangi ilkeler söz konusuysa, güncellenmesi, hukuka uygun işlenmesi, değiştirilmesi, gerekli ise kişiye talebi üzerine bilgi verilmesi işlenip işlenmediğine ilişkin, fabrikalar olsun özel okullar olsun mutlaka bu kap-

samda yer alır. Sadece bizde değil, diğer Avrupa Birliği ülkelerinde de böyledir. Hem kamu kesimi hem özel kesim kısacası bu kanun kapsamı altındadır.

Musa ALBAYRAK- Bu kişilerin rızasına bağlı mıdır?

Prof. Dr. Cemil KAYA- Kişisel verilerin işlenmesindeki ilk şart odur. Tüm kanunlarda yine, ilgili kişinin açık rızasıdır. Hatta açık rızanın ne anlama geldiği bile tartışmalıdır. Mutlaka açık rıza acaba kişinin "ben bu verilerimin işlenmesine rıza gösteriyorum" şeklinde bir belge imzalaması mıdır? Yahut da internetten bilet alacağımızı düşünelim, orada yemek tercihini yaptığımızda, oraya bir tik attığımızda, ki bunun teknik adları var; opt in opt out, neyse oradaki işaretin, yahut da yazılı bir belgenin altında bir onay kutucuğu açıldığında, oraya imza açıldığında o da bir kişisel verilerin işlenmesine rıza anlamına geldiği kabul edilir.

Bilal ÇALIŞKAN- Teşekkür ederiz. Başka bir soru; mesela bizim güvenlik soruşturmalarımız yapılır. Üst düzey görevlerde belirli bir yere aday olduğunuz zaman. Sorulur ilgili yerlere ve ilgili bilgiler alınır. Buna ilişkin şu anda mevzuatta hüküm var ve bu konuda da herhangi bir şey yapılmaz, itiraz da yok. Herhangi bir sorun çıkarsa itiraz oluyor, o zaman idare mahkemesine bununla ilgili gelmiş bir şey hatırlamıyorum ben, var mı bunu hatırlayanınız? Yani idari bir işlem olarak değerlendirilir bu. Ama bir aralar hatırladığımız var; yani yönetmeliğin durumuyla ilgili olarak, daha ciddi yerlere sorulması. Mesela bir bakkala sorulurmuş eskiden gittiğinde, mahallede oturan bir komşusuna sorulurmuş işe alımlarda adayken, daha sınava girmeden. Bunun doğru olmadığı noktasında bir iptal kararı hatırlıyorum Danıştay'a açılmış stajla ilgili ya da stajdan önce mi, öyle bir karar vardı.

Prof. Dr. Cemil KAYA- Bu konuya ilişkin, güvenlik soruşturmalarının hukuken geçerli, hukuken destekleyen bilgi ve belgeler olmadığı müddetçe geçerli olmadığı yönünde Danıştay'ın çok sayıda kararını hatırlıyorum. Hatta yakın tarihte yanılmıyorsam Anayasa Mahkememizin de MİT'e ilişkin bir raporun herhalde, ilgili kişinin dosyasına gönderilmesi ve bu şekilde aleni hale gelmesinin, o kişinin haklarının ihlal edildiğine ilişkin bir karar verdi diye biliyorum. Masumiyet karinesine aykırı olarak adlandırıldı. Bir de eski tarihli bir Danıştay kararı hatırlıyorum, Susurluk Raporu nedeniyle kişinin zarar gördüğünden bahisle Danıştay'da açmış olduğu bir tam yargı davası, tazminat davası, orada Danıştay İdari Dava Daireleri Genel Kurulu bugünkü adı, İdareyi manevi tazminata hükmetmiştir kişisel verileri ifşa oldu gerekçesiyle. Danıştay'da böyle bir tabir kullanılmıyor ama "özel yaşamın gizliliğini ihlal" olarak bir karar verdi diye hatırlıyorum.

Dr. Alparslan ALTAN- Alparslan Altan, Anayasa Mahkemesi Başkanvekili. Hocam söyledi, bireysel başvuru yoluyla kişiye ait istihbarat bilgilerinin ki,

somut olaydaki kişi bir öğretmendi, öğretmenlerin geçmişiyle, daha önceki siyasi eğilimleriyle ilgili istihbarat notunun ceza davasında kullanılması, dosyaya konulması nedeniyle kişi masumiyet karinesinin ihlal edildiğini ileri sürmüştür. Anayasa Mahkemesi burada gerçekten kişinin iddia ettiği gibi masumiyet karinesinin ihlal edildiğini ve bu nedenle bu hakkının bu şekilde ihlal edildiği sonucuna vardı. Anayasa Mahkemesi Genel Kurul dosyalarında da, şu anda tam şey olarak hatırlayamayacağım ama, Türkiye İstatistik Kanunu'nda kişilerin, kendilerinden istenen her türlü belgeyi ve bilgiyi İstatistik Kurumu'na vermesine ilişkin düzenlemeyi "her türlü" ibaresi yönünden iptal etti. Yine benzer Sermaye Piyasası Kanunu'nda kişinin, sermaye piyasasında işlem yapan kişinin kendisiyle birlikte belirli derecedeki yakınlarının da her türlü bilgi ve belgeyi verme zorunluluğunu öngören bir düzenleme vardı. Bu düzenlemeyi de benzer gerekçeyle iptal etti. Anayasa Mahkemesi bu konuda hassas ve Genel Kurul kararlarından da epey buna örnekler bulabiliriz. Teşekkürler.

Bilal ÇALIŞKAN- Biz de teşekkür ederiz. Tabi bütün bunlar sözleşmede güvenceye alınan, AİHS'te güvenceye alınan 8. maddede güvenceye alınan özel hayatın gizliliği, özel hayata saygı çerçevesinde değerlendirilmesi gereken; İnsan Hakları Mahkemesi'nin de bu noktada ülkemizle ilgili bir hayli kararı mevcut. Benim hatırladığım bir tanesi var mesela, bunu diyor muhakkak böyle bir durumu, yapacaksan inceleme, gözaltına aldıkları birisini jinekolojik muayeneye tabi tutmuşlar, bundan sonra işkence yapıldı iddiasını önlemek için. Neye dayandın diyor yani. E biz kendi keyfimize dayandık; yok öyle diyor, her şeyi yapamazsın. Böyle bir şeyi yapmak için dayanacağın bir kanun çıkarman lazım. Yönetmelik de yetmez diyor, kanunla sınırlanabilir ancak. Yönetmeliğe koyduk efendim yönetmelikte var; kendisinin tacize maruz kalıp kalmadığını tespit etmek zorundayız. Yok diyor, sınırlamaları yönetmelikle yapamazsın, kanunla yapmak zorundasın.

Mustafa GÖKÇEK- Mustafa Gökçek, Danıştay İdari Dava Daireleri Kurulu Üyesi. Şimdi, 6. Daire üyemiz Musa Albayrak Bey'in Hocama sorduğu ikinci soru belki eksik kaldı da, bir katkı olarak onu söylemek istiyorum. Zannediyorum 2013'ün son döneminde, milli eğitimdeki öğrencilerden çok detaylı, böyle mahrem sayılacak bilgilerini dahi, mesela ne gibi desek, hatırladığım kadarıyla annenizin babanızın ilk evliliği mi, işte ilk evliliği değilse falan çok özele giren sorular var. Belki kökenini, yani çok değişik, meşrebini falan araştırıcı çok değişik şeyler gelmişti. Öyle bir genelge miydi, yoksa ona yönelik bir formdu zannediyorum. İdari Dava Dairelerinde tam belki bunun üzerine oturmasa da, özel bilgileri, mahremleri ifşa edici, belki toplumda bir kaosa yol açıcı, şu anda karar yazıldı çıktı mı onu tam hatırlamıyorum ama oyçokluğuyla öyle bir iptal kararı verildi. Onu da belirtmek isterim bir katkı olarak. Özellikle Musa Bey bir

fişleme sayılır mı deyince, tam da belki öyle denmese de o mahiyette bir karar verildi kanaatindeyim. Teşekkür ediyorum.

Bilal ÇALIŞKAN- Biz de çok teşekkür ederiz. Başka soru var mı? Mesela Defne Samyeli ile ilgili bir şey vardı hatırlıyor musunuz? TÜİK buna sormuş, demişler ki şu şu cevapları vereceksiniz kişisel verilerle ilgili. Vermediğiniz takdirde ceza yazarız. Kadın kendisinin ceza tehdidiyle kişisel verilerinin alınmasının büyük bir ayıp olduğunu söyledi, hak ihlali olduğunu söyledi. Sonrasında ne oldu bilemiyorum. Herhalde TÜİK bir açıklama yaptı onunla ilgili; biz kendisini zorlama değil, ikna etmeye çalışıyoruz gibi bir ifade vardı yanlış hatırlamıyorsam. Buyurun Mehmet Ali Bey.

Mehmet Ali CERAN- Mehmet Ali Ceran, Danıştay 14. Daire Üyesiyim. Telekomünikasyon İletişim Başkanlığı var biliyorsunuz. Bu kişisel verilerin korunması, özel hayatın gizliliği konusunda bu kurumun yeri nedir?

Prof. Dr. Cemil KAYA- Güncel bir kurum olması hasebiyle pek fazla ayrıntıya girmek istemiyorum ama nihayetinde bir yasal düzenleme herhangi bir kuruma, bunun adı TÜİK olsun TİB olsun fark etmez, herhangi bir yetki vermişse, Anayasa Mahkemesi'nde iptal edilmediği müddetçe bu yetkisini kullanabilir. Buna herhangi bir yasal engel var mıdır yok mudur onun değerlendirmesi takdir edersiniz ki Anayasa Mahkemesi tarafından yapılacaktır. Sadece bizim ülkemize mahsus değil, Avrupa Birliği hatta Amerika olsun, Kanada olsun bu tip ülkelerde o tip yapılanmalar, kurumların da olduğunu biliyorum. Onun dışında, bilmiyorum çok genel şeyler söyledim ama yeterli oldu mu.

Dr. Alparslan ALTAN- Alparslan Altan, Anayasa Mahkemesi Başkanvekili. Şimdi TİB'in mevzuatı açısından bakıldığında, TİB kendiliğinden bir şey yapan bir kurum değil. Özellikle bu dinlemeler, tespitlerle ilgili. TİB'in şu andaki mevzuat açısından yetkisi mahkemeler tarafından kendisine gönderilen talimat üzerine, dinlemeyi de kendisi yapmıyor ve bu konuyla ilgili işlemleri başlatmış oluyor. Yani, evet koordinatör bir kurum mahiyetinde. Dolayısıyla yani burada dinlemeyle ilgili TİB'in mevzuat gereği yaptığı işlemler, mahkeme kararına dayalı işlemler. Burada yetki tamamen mahkemenin.

Cüneyt YILMAZ- Cüneyt Yılmaz, İstanbul İdare Mahkemesi Başkanı. Şeyi sormak istiyorum ben, tüzel kişilerde de mesela mesai saatlerinin takibi için çalışan personelin parmak izi, yüz taraması gibi şeylerini takip için alıyorlar girişlerde çıkışlarda belli bir disiplin sağlamak için. Bu da bu kişisel veri kapsamında sayılıp aslında yasal altyapısı da olmadığı için ne kadar hukuka uygun? Ve o arkadaşlar başvurularını yahut da yasal haklarını nasıl arayabilirler?

Prof. Dr. Cemil KAYA- Bir işyerine girişlerde kimlik kartı uygulaması dışında bir takım hem kamu hem özel kuruluşlar, yanılmıyorsam Türkiye'de bir belediye böyle bir uygulama yaptı diye biliyorum, bu tip uygulamalar yapmaktadırlar. Tabi avantajları söz konusu, dezavantajları söz konusu. Kimlik kartıyla yapılan bir uygulamanın bir başkasına kimlik kartımızı verdirmek suretiyle, sanki mesaiye başlamışız gibi bir sonuç doğurma durumu söz konusudur. Ama parmak izi her kişiye özel, mahsus olduğu için, parmak izimizi de bir başkasına veremeyeceğimize göre bu şekilde bir uygulama işin teknik mantığı açısından uygundur ama hukuka uygun mudur? Kişisel kanaatim bunun parmak izi yoluyla yapılmasının ne pahasına olursa olsun hukuka uygun olmayacağı yönündedir. Bu konuda bildiğim kadarıyla idare mahkemesi kararları da söz konusudur hukuka uygun olmadığı yönünde. Ama batı ülkelerinde de bu tip uygulamaların olduğunu biliyorum. Yani parmak izi yoluyla mesai takibinin olduğu uygulamaları biliyorum. Yasal zemini, tabi gönül ister ki bütün bu yasal zemin veri koruma kanunlarına dayansın. Veri koruma kanunu olmadığı için buna ilişkin genel bir madde de söz konusu değildir. Uygulayan kurum açısından, özel sektör açısından bildiğim kadarıyla İş Kanunu, İş Mevzuatı çerçevesinde bir hüküm yok diye de biliyorum. Öyle söyleyeyim.

Bilal ÇALIŞKAN- Çok teşekkür ederiz. Son derece hassas verilere sahip olduk, burada yaptığımız hepsi kamera altına alındı arkadaşlar. Onayınız yoksa çıkışta söylersiniz. Çok teşekkür ederiz, sağ olun.