

UNIVERSITÄT MISKOLC

Staats- und Rechtswissenschaftliche Fakultät

Ferenc Deák Staats- und Rechtswissenschaftliche

Doktorschule

István Mező

**SCHUTZ PERSONENBEZOGENER DATEN
IM RECHT DER EUROPÄISCHEN UNION UND IN UNGARN**

PhD-Dissertation

THESENHEFT

Ferenc Deák Staats- und Rechtswissenschaftliche Doktorschule

Leiter der Doktorschule: Prof. Dr. András Bragyova

Titel des Doktorprogramms: Weiterentwicklung des ungarischen Staats- und Rechtssystems,
der Rechtswissenschaft, mit besonderer Rücksicht auf die europäischen
Entwicklungstendenzen

Wissenschaftlicher Leiter: Prof. Dr. habil. András Bragyova

MISKOLC
2009

I.

ZUSAMMENFASSUNG DER FORSCHUNGSAUFGABE, ZIELSETZUNGEN DER FORSCHUNG

In dieser Arbeit möchte ich versuchen aufzuzeigen, welcher Vorgang zum aktuellen Stand der Dinge hingeführt hat, wo personenbezogenen Daten in den europäischen Ländern durch weltweit fast unikale strenge Vorschriften geschützt werden und in welchem Umfang sich das rechtliche Instrumentarium dieser Seite des Persönlichkeitsschutzes entwickelte. Ziel der Forschung ist es, einen Überblick zu geben, welche einheitlichen Grundsätze und Rahmenvorschriften es gibt im innerstaatlichen Recht der Mitgliedstaaten der Europäischen Union hinsichtlich des Schutzes persönlicher Daten. Als Ausgang für die historische Entwicklung gebe ich einen Überblick über die Entwicklungsgeschichte der nationalen Datenschutzrechte, die Entwicklung der Generationen von Datenschutzrechten, das im Rahmen des Europarates ausgearbeitete Datenschutzabkommen, die sekundäre Rechtsetzung der Europäischen Union zum Schutz personenbezogener Daten. Der Überblick über die sekundäre Rechtsetzung der Europäischen Union bedeutet einerseits eine detaillierte Analyse und die Vorstellung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Nach Auslegung und Überblick einzelner Abschnitte aus der Richtlinie 95/46/EG, ferner nach Darstellung der Tätigkeit der Datenschutzgruppe 29 wird die sektorielle Datenschutzregulierung detailliert dargelegt. Die bezüglich des Schutzes der Privatsphäre und der persönlichen Daten im Telekommunikationssektor spezielle Vorschriften festlegende Richtlinie 97/66/EG hat besondere Vorschriften über die Verarbeitung personenbezogener Daten erlassen mit dem Ziel, die in der Richtlinie 95/46/EG mit Grundsatzcharakter ausformulierten Bestimmungen auch in Bezug auf den Telekommunikationssektor durch detaillierte Vorschriften Geltung zu verschaffen. Auch die zweite Stufe der sektoriellen Rechtsetzung zum Datenschutz ließ nicht lange auf sich warten, denn die Missbräuche der persönlichen Daten in den Online-Informationssystemen haben zunehmende Ängste in der Gesellschaft ausgelöst. Die grundlegenden Vorschriften des Datenschutzes waren nur schwer anzuwenden bei der Umsetzung in die nationalen Rechte der Mitgliedstaaten in Bezug auf die neu entstandenen Bereiche der Informationstechnologien. Die Datenschutzrichtlinie 95/46/EG musste an die Bedingungen von Markt und Technologie der im Telekommunikationssektor speziell ausgestalteten Dienstleistungen angepasst werden. Ziel der Regulierung war es, dass die persönlichen Daten und das Recht auf Achtung des Privatlebens für Nutzer öffentlich zugänglicher elektronischer Telekommunikationsdienstleistungen – unabhängig von der angewandten Technologie - gleichwertigen Schutz erhalten. Die neuen modernen

digitalen Technologien, die für die breite Bevölkerung zugänglich sind, stellen hinsichtlich des Rechts auf Achtung des Privatlebens und der persönlichen Daten der Nutzer besondere Anforderungen. Das Internet umschmeißt die herkömmliche Marktstruktur dadurch, dass es eine weltweite Infrastruktur für ein breites Spektrum an elektronischen Telekommunikationsdienstleistungen bereitstellt, was für die Verbraucher neue Möglichkeiten schafft, aber gleichzeitig auch neue Gefahren in sich birgt bezüglich des Rechts auf die Achtung der personenbezogenen Daten und des Privatlebens der Benutzer. Eine Erneuerung der E-Commerce erfolgte 2002, hierbei trat an die Stelle der Telekommunikations-Datenschutz-Richtlinie die Richtlinie über den Datenschutz in der elektronischen Kommunikation, in der alle früheren Regulierungen beibehalten sind und durch neue spezielle technische Vorschriften ergänzt wurden, wie etwa der Begriff und die Verwaltung der Verkehrsdaten bzw. Standortdaten, ferner durch Vorschriften bezüglich der werterhöhten kommunikationsbezogenen Dienstleistung, des elektronischen Briefes, sowie der Cookies und SMS. Einen Überblick über die Entwicklung der datenschutzbezogenen Regulierungen zu geben ist deshalb von Bedeutung, weil die Datenschutzregulierung als eine Regulierung betrachtet wurde, die auf das Ziel der Bereitstellung von grenzüberschreitenden Dienstleistungen ausgerichtet und in den Sachbereich Regulierung des Binnenmarkts eingestuft war. Die rechtliche Beurteilung der Datenschutzregulierung ging über das Niveau der ausschließlich für die Binnenmarktregulierung erforderlichen rechtlichen Mittel hinaus, da die Datenschutzregulierung sich in ein grundrechtliches Rechtsverhältnis verwandelt hat. In meiner Arbeit möchte ich anhand des Urteils des EuGH im Fall Lindquist, durch Analyse der Entscheidungen des Europäischen Gerichtshofes für Menschenrechte in den Rechtsachen *Klaas und andere*, oder *Caroline von Hannover* veranschaulichen, dass es zur Ausgestaltung des Regulierungssachbereiches Datenschutz, wie eines binnenmarktbezogenen Regulierungsbereiches, nach Maßgabe der Anschauungsweise "Erforderlichkeit und Verhältnismäßigkeit" hinsichtlich der Grundrechte gekommen ist. Die Rechtsvorschriften betreffend Schutz und Verwaltung personenbezogener Daten erhielten Grundrechtscharakter, und diese Rechtsentwicklung fand eine klare Anerkennung in der Charta der Grundrechte der Europäischen Union im Bereich der individuellen Freiheitsrechte.

Die Rechtsentwicklung der Europäischen Union ist für die Entwicklung der ungarischen Datenschutzregulierung ein bestimmender Faktor, weil zur Erfüllung der Rechtsharmonisierungs-Verpflichtungen die Garantien für die Freiheit des Binnenmarktes auch im ungarischen Recht zur Geltung gebracht werden mussten. In meiner Arbeit gebe ich einen Überblick über die Anfänge der ungarischen Datenschutzregulierung, deren Vorgeschichte, die Vorschriften betreffend die Verwaltung von staatlichen Datensammlungen und Registern beginnend mit dem Gesetzesartikel Nr. XXXV vom Jahr 1897 über die Aufstellung des Königlich Ungarischen Zentralamtes für Statistik bis hin zu den

Gesetzentwürfen betreffend Informatik. Eingehend dargelegt werden die in der Parlamentsdebatte des Gesetzes Nr. LXIII vom Jahr 1992 über den Schutz personenbezogener Daten und die Publizität der Daten von öffentlichem Interesse ausformulierten verschiedenen Standpunkte und Änderungsanträge. Der historische Überblick wird erforderlich zur Untersuchung der Problematik, wie ein Rechtsverhältnis in der öffentlichen Verwaltung, das die staatliche Datenverwaltung regelt, zu einem Grundrecht bzw. im horizontalen Rechtsverhältnis sogar zu einer erzwingbaren grundrechtlichen Norm wird.

Neben der Analyse einzelner bedeutungsvoller Änderungen des ungarischen Datenschutzgesetzes werden die Begriffe betreffend den Schutz personenbezogener Daten so etwa die Definitionen von Angabe/Daten, Information, Geheimnis, persönlicher Charakter interpretiert. In den Mittelpunkt der Analyse des Datenschutzrechtes aus der Sicht der Rechtsdogmatik stelle ich die Deutung des Begriffes *privacy*. Aus den Aspekten der Achtung des Privatlebens wie etwa Alleinsein, Intimität, Anonymität und Zurückhaltung entwickelt sich ein grundrechtorientiertes Herangehen an die Problematik der Datenschutzregulierung. Durch Sicherstellung von Intimität und Anonymität wird gewährleistet, dass die Menschen die gesellschaftliche, politische Kommunikation freiwillig aufnehmen können ohne die Angst, beobachtet und identifiziert zu werden. Beim Aufzeigen des grundrechtlichen Charakters der Datenschutzregulierung versuche ich den Begriff *privacy* und das breite Spektrum der Möglichkeiten seiner Deutung darzulegen. Eine gewichtige Frage der rechtlichen Regulierung des Datenschutzes bedeutet, auf wen sich der Schutz erstrecken muss, das heißt die Bestimmung des Kreises der zu schützenden Subjekte bildet die Grundlage für die Anwendung der datenschutzbezogenen Rechtsvorschriften. Regulierung der personenbezogenen Daten erstreckt sich in erster Linie auf lebende natürliche Personen, aber in einzelnen Ländern auch auf juristische Personen, bzw. verstorbene Personen. Die Erfassbarkeit des an die Person geknüpften Charakters, das heißt die Möglichkeit eine Angabe zu einer Angabe zur Person umzuqualifizieren begründet den Umstand, dass im betreffenden Fall bezogen auf die Verwaltungsart dieser Daten die Materie des Datenschutzrechtes Anwendung findet, so versuche ich in meiner Arbeit die personenbezogenen Charakteristika einzelner Daten aufzuzeigen, Bezug nehmend auf die Rechtspraxis des Datenschutzbeauftragten. Eine andere Schlüsselfrage des Schutzes personenbezogener Daten ist die Reindividualisierbarkeit von persönlichen Daten, das heißt die Dauer des rechtlichen Schutzes. Kommt es zur Bereinigung einer Angabe vom persönlichen Charakter, und erfolgt eine Umformung zu einer statistischen Angabe, so fragt sich jedoch, ob dieser Vorgang als endgültig abgeschlossen zu betrachten sei? Es bestehen Risiken für den Fall, dass eine Angabe ihren persönlichen Charakter wiedergewinnen sollte, da die technischen Voraussetzungen da sind, mit anderen Worten, ob doch nicht die Möglichkeit gegen ist, eine statistischen Angabe mit einer persönlichen Angabe verbindet, indem man deren Entstehung

zurückverfolgen kann? Das Wesen der Datenschutzregulierung besteht nämlich darin, welche technischen Verfahren zur Dekodierung von rein statistischen Daten anwendbar sind, bzw. unter welchen Voraussetzungen und in welchem Umfang die Reindividualisierbarkeit von Daten reguliert werden soll. Ich bearbeite im Problemkreis "Begriff der persönlichen Daten" folgende Fragestellungen.

In der Arbeit befasse ich mich eingehend mit der europarechtlichen und ungarischen Regulierung des Datenschutzes und daher ist es unumgänglich, das institutionelle System des Datenschutzes zu überblicken. So befasse ich mich detailliert mit der Darlegung der Tätigkeit des Europäischen Datenschutzbeauftragten, bzw. mit Wahl, Rechtstellung, Befugnissen und rechtlichem Instrumentarium des ungarischen Datenschutzbeauftragten. In der Arbeit werden die wichtigsten Empfehlungen, Feststellungen der Datenschutzbeauftragten präsentiert. So versuche ich bei der Aufarbeitung des Themenkreises die Grundrechtsschutzfunktion der Datenschutzbeauftragten zu untermauern, indem ich rechtliches Instrumentarium und Spezifika des Funktionierens dieser Institution darlege. Die Aufgabe des Schutzes personenbezogener Daten obliegt nicht ausschließlich dem Datenschutzbeauftragten. Das ungarische Verfassungsgericht hat durch mehrere Entscheidungen von großer Tragweite, wie etwa die Entscheidung über das Verbot der universellen Personenkennzahl (15/1991) zur Entstehung des rechtlichen Schutzes personenbezogener Daten beigetragen. Das Verfassungsgericht gewährte Schutz dem Grundrecht auf Schutz personenbezogener Daten vor unnötigen und unangemessenen Einschränkungen auch in den sektoriellen Regulierungen durch seine Entscheidungen über verfassungskonforme Anwendung verdeckter Ermittlungsmaßnahmen (940/B/2003. AB), über die datenschutzbezogenen Erfordernisse bei Sicherheitskontrollen (16/2001), über die Publizität von Gerichtsverfahren, oder betreffend die Verpflichtung zur Abgabe von Vermögenserklärungen. Das Verfassungsgericht hatte durch eine Entscheidung (30/1997) hinsichtlich der Einschränkung der Privatsphäre öffentlicher Funktionsträger ausgesprochen, dass der Schutz personenbezogener Daten eingeschränkt werden kann im Blick auf andere verfassungskonforme Rechte, wie die Publizität der Daten von öffentlichem Interesse. Die gründliche Kenntnis der Rechtsprechung des Verfassungsgerichts ist erforderlich, wenn man sich einen Überblick über bestimmte Fragen des Schutzes personenbezogener Daten zu verschaffen will.

In der Arbeit habe ich mich besonders konzentriert auf die Analyse der sektoriellen Regulierung des Datenschutzes und besonders diejenigen Datenverwaltungshandlungen recherchiert, die nicht staatliche oder kommunale Datenverarbeitende Stelle vornehmen. Als Ausgangspunkt beim Überblick der sektoriellen Regulierung der Datenschutzfragen gebe ich einen Überblick über die Persönlichkeitsschutz-Vorschriften des Ung. Zivilgesetzbuches hinsichtlich des Schutz des Rechtes am

eigenen Bild betreffend Anfertigung und Verwendung von Bild- und Tonaufzeichnungen. In Bezug auf den Persönlichkeitsschutz und Schutz personenbezogener Daten werden Fragen wie Erteilung der Einwilligung, Verwendung bzw. Veröffentlichung von Daten behandelt. Neben dem zivilrechtlichen Schutz persönlicher Daten werden die im Strafrecht gewährten rechtlichen Mittel bei Verletzungen des Personendatenschutzes präsentiert. Eine der Schlüsselfragen des sektoriellen Datenschutzes ist es, bei Anwendung welcher Grundsätze und Vorschriften Personendatenschutz, Pressefreiheit und Publizität der Daten von öffentlichem Interesse besser miteinander vereinbar sein können. Das ungarische Datenschutzgesetz enthält keine speziellen Vorschriften hinsichtlich des Umganges mit Daten durch die Presse. Wenngleich zur Kenntnis der Presse auch Privatgeheimnisse, personenbezogene Daten gelangen können, deren Veröffentlichung unterschiedlich beurteilt werden muss, je nachdem ob es sich um die Veröffentlichung von Daten eines öffentlichen Funktionsträgers handelt, die dessen Wertung im Zusammenhang mit öffentlichen Angelegenheiten beeinflussen, oder um private Angelegenheiten, familiäre Angelegenheiten von Privatpersonen, oder Preisgabe seiner persönlichen Beziehungen.

Die Verwaltung personenbezogener Daten im Gesundheitswesen wird durch das Gesetz XLVII vom Jahr 1997 geregelt, das das Informieren der Patienten auf Grund des informationellen Selbstbestimmungsrechtes, die Verwaltung ihrer Daten, bzw. die Entzifferbarkeit einiger Patientendaten aus epidemiologischem öffentlichem Interesse gewährleistet. Das Gesetz bestimmt die Ziele der Datenverwaltung im Gesundheitswesen, so kann es beispielsweise zu Datenverwaltungshandlungen kommen für Zwecke der Aufbewahrung, Förderung, Verbesserung der Gesundheit, des Monitoring des Gesundheitszustandes, aber es sind auch Datenverarbeitungen legal, die für das Interesse des Volksgesundheitswesens und der Epidemiologie vorgenommen werden sollen. Die Verarbeitung von Gesundheitsdaten können auch andere Gesetze erlauben z.B. zwecks Berufsausbildung im Gesundheitswesen, für Zwecke wissenschaftlicher Untersuchungen, behördlicher Kontrolle von Organen des Gesundheitswesens, zur Finanzierung von Versorgungsleistungen im Gesundheitswesen, zur Feststellung von Versorgungsleistungen durch die Sozialversicherung, für Zwecke der Strafverfolgung, im Verwaltungsverfahren, im Ordnungswidrigkeitsverfahren, bei Durchführung von Verfahren durch die Staatsanwaltschaft und die Gerichte. So kann auf Grund besonderer gesetzlicher Bestimmung die Verwaltung gesundheitsbezogener Daten vorgenommen werden im Schulsystem, zur Feststellung der Tauglichkeit für Militärdienst, der Eignung für den Beruf. In der Arbeit werden präsentiert die beim Datenschutzbeauftragten im Zusammenhang mit Datenverwaltungshandlungen im Gesundheitswesen eingereichten typischen Beschwerden, in denen in erster Linie das nicht adäquate Informieren, die mangelhafte Verwaltung medizinischer Unterlagen, die unbegründete Einschränkung des Akteneinsichtsrechts der Patienten bemängelt wurden. Einen der spezifischen Bereiche der

Datenverwaltung im Gesundheitswesen stellen dar: der Umgang mit dem Daten von Drogenkonsumenten und die Übermittlung der Daten zum Gesundheitszustand ohne Anlass an die Polizeibehörden, die datenschutzbezogenen Bedenken entstehen ließ. Die Finanzkontrolle der Versorgungsleistungen im Gesundheitswesen auf die Begründetheit einer medizinischen Serviceleistung an den Patienten hin, durch die eine konkrete Person mit Daten über die eigene Krankheit und die erhaltene medizinische Leistung in Verbindung gebracht werden kann, warf ebenfalls datenschutzbezogene Bedenken auf angesichts der mangelhaften Regelung und wegen fehlender adäquater Garantien.

Eines der bedeutsamen Gebiete des ungarischen sektoriellen Datenschutzes ist die Privacy am Arbeitsplatz, weil in diesem Rechtsbereich aus Ungeregeltheit heraus entstehende datenschutzbezogene Missbräuche weit verbreitet sind. Man verbringt einen erheblichen Teil seines Lebens in der Arbeitswelt, so entscheidet der Arbeitgeber über die Eignung für die auszuübenden Tätigkeitsbereiche anhand der persönlichen Daten. Es steht im Interesse des Arbeitgebers, gesundheitliche, familiäre, oder andere die Privatsphäre betreffende Informationen über den Arbeitnehmer zu sammeln, um die Eignung des Arbeitnehmers zu beurteilen oder gar zum Schutze von kommerziellen Interessen. Die Rechtsfälle betreffend die Verletzung von Privacy am Arbeitsplatz kann man in drei Gruppen einteilen. In die erste Kategorie gehören diejenigen Fälle, in denen der Arbeitgeber ohne legitimen Zweck, übertrieben viele oder vorräteweise persönliche oder sensible Daten vom Arbeitnehmer sammelt. In die zweite Gruppe können diejenigen Rechtsverletzungen eingestuft werden, in denen der betroffene Dateninhaber die ihm zustehenden Rechte nicht ausüben kann. Eine dritte Kategorie der Rechtsfälle bilden diejenigen Rechtsfragen, wo der Arbeitgeber ohne Anlass personenbezogene Daten der Arbeitnehmer weiterleitet oder öffentlich zugänglich macht. In der Arbeit präsentiere ich typische Fälle der Verletzung der Privacy am Arbeitsplatz mit dem Ziel, um auf Mängel in der sektoriellen Datenschutzregulierung hinzuweisen.

In der Regulierung nach dem Gesetz Nr. C von 2003 über das elektronische Telekommunikationswesen wird auf die rechtliche Grundlage der Verwaltung personenbezogener Daten bzw. auf die detaillierten Regeln der Verwaltung personenbezogener Daten im elektronischen Telekommunikationswesen eingegangen. Im Zusammenhang mit den elektronischen Telekommunikationsdienstleistungen werden vom Dienstleister/Provider verwaltet nicht nur die natürlichen Identifizierungsdaten der betroffenen Person, sondern gespeichert werden die Nummer des Abonnenten-Anschlusses oder seine übrigen Identifizierungsdaten: Adresse des Abonnenten und Typ des Anschlusses, die Zahl sämtlicher für den Zeitraum der Verrechnungsperiode verrechenbaren Einheiten, Nummern von Anrufern und

Angerufenen, Typ des Anrufs oder sonstige Dienstleistungen, Richtung, Anfangszeitpunkt und Zeitdauer der geführten Gespräche bzw. Volumen der übermittelten Daten, bei Mobilfunkgeräten Merkmale von Netz und Zelle des Dienstleisters sowie das International Mobile Equipment Identity (IMEI) des bei Inanspruchnahme der Dienstleistung benutzten Gerätes, im Falle der IP-Netze die dort verwendeten Identifizierungsdaten. Angesichts des Umstandes, dass in unserem Leben die leitende führende Tätigkeit oder die mobile Kommunikation immer mehr bestimmend wird, so hinterlassen wir auf diese Weise über die Kommunikation unseres Lebens Spuren bei den elektronischen Telekommunikationsdienstleistern, die dann im Stande sind, durch Verbinden unserer Daten das Netz unserer persönlichen Beziehungen zu erschließen. Deshalb ist es besonders wichtig, welchen Kreis unserer kommunikationbezogenen persönlichen Daten und auf wie lange Zeitdauer der Staat die Dienstleister im Hinblick auf die nationale Sicherheit zu erhalten verpflichtet. In der Arbeit gebe ich kurzen einen Überblick über die Regulierung des Datenschutzes hinsichtlich des elektronischen Telekommunikationswesens.

In der modernen Marktwirtschaft sind die geschäftliche kommerzielle Praxis, das Marketing oder die Kreditgewährung von der Verwaltung persönlicher Daten untrennbar. In jedem Fall wird der Erfolg dadurch fundiert, wie breites Spektrum an Informationen der Dienstleister über den Verbraucher Konsumenten besitzt, so beispielsweise über dessen Ansprüche, Möglichkeiten, Finanzlage, Zahlungsfähigkeit. In diese Beziehung sind die geschäftlichen Instrumente von Direktmarketing untrennbar von der Werbung für die in der modernen Konsumgesellschaft angebotenen Dienstleistungen. Zur Erreichung der kommerziellen Bestellungen/Aufträge verwenden die Versandfirmen bzw. Warenhandels-Unternehmen Methoden des Direktmarketing, dessen Wesen es ist, dass der Verbraucher auf seinen Namen Briefe, Pakete, Warenmuster zugesandt erhält, um sein Interesse für wecken die Ware bzw. Dienstleistung zwecks Bestellung zu erwecken. Unter den Instrumenten des Direktmarketing findet man telefonische oder unmittelbar persönliche Ersuchen, um mit ihren Vorschlägen die Adressaten zur Bestellung von Waren, zur Inanspruchnahme von Dienstleistung zu überreden. Im Falle der Dienstleistung Kreditgewährung ist das Geldinstitut darin interessiert, die persönliche und Vermögenslage seines Kunden vollständig aufzuklären, und sich über dessen Leistungsfähigkeit zu vergewissern. Hinsichtlich personenbezogener Daten kann eine „Drohung“ bedeuten die sich im Herbst 2008 entfaltende Kreditkrise, die die Einführung der positiven Schuldnerliste wahrscheinlich beschleunigen wird mit der Zielsetzung, die Stabilität Kreditgewährungssparte im Banksystem durch rechtliche Mittel zu verstärken dadurch, dass das kreditgewährende Geldinstitut den genauen Schuldstand des Kreditnehmers vollständig kennen lernen kann. In meiner Arbeit gebe ich einen Überblick über die Regulierung bezüglich negativer

Schuldnerlisten, bzw. über die datenschutzbezogenen Hindernisse der Einführung positiver Schuldnerlisten.

Ein erheblicher Teil der wirtschaftlichen Vorgänge verläuft in computergestützten weltweiten Netzen, die zum Sammeln, Speichern, und Veröffentlichung von persönlichen Daten, Angaben von öffentlichem Interesse, und statistischer Daten dienen. Das Internet kennt keine Staatsgrenzen, ist für jedermann zugänglich, und stellt eine uneingeschränkte Publizität dar. Die Verbreitung des Internet warf neue datenschutzbezogene Probleme auf, derer sich die Nutzer häufig gar nicht bewusst sind. Wichtiges Merkmal der Internet-Benutzung ist es, dass es beim Kontaktieren zwischen Dienstleistern und Benutzern des Internet zur Mittelung zahlreicher personenbezogener Daten kommt, da der Nutzer durch jede seine Fingerbewegung Spuren hinterlässt. So als personenbezogenen Daten wechseln den Besitzer E-Mail Adressen der Seiten, eventuell Identifikationskennzeichen der Internet-Nutzer, die IP-Adressen. Die Internet-Dienstleister speichern in ihren Korrespondenzservern den Inhalt der elektronischen Korrespondenz, ehe dazu der Nutzer Zugriff hat, andere können ihn überprüfen, lesen. An den Speicherplatzservern wird verzeichnet, von welcher IP-Adresse aus der einklickende Nutzer wie viel Zeit mit dem Aufblättern einzelner Internetseiten verbrachte, also letztendlich kann sämtliche Aktivität des Nutzers im Internet technisch kartiert werden. So stellen vor der Ausgestaltung der individuellen persönlichen und der vielfarbigen Nutzerprofilen richtige Hindernisse nur die Kosten. Deshalb muss zum Schutz personenbezogener Daten das Betreiben technischer Instrumente durch rechtliche Regulatoren reguliert werden. Erforderlich ist es auch zu bestimmen, unter welchen Voraussetzungen die einzelnen im Verwaltungs- oder Strafverfahren beteiligten Behörden, Zugriff für welche auf Festplatten gespeicherten Daten haben können. In den letzten Jahren lenkte eine auf der Internetseite halapenz.hu geführte Diskussion die Aufmerksamkeit auf die Datenschutz bezogene Schranken der Internet-Mitteilungen. Neben Konfrontierung der Grundsätze von Datenschutz und Meinungsäußerungsfreiheit befasse ich mich eingehend damit, welche rechtlichen Mittel dem Schutz personenbezogener Daten des Nutzers im Bereich der Internet-Dienstleistungen dienen.

Den Überblick der ungarischen sektoriellen Datenschutzregulierung schließe ich mit dem Fragenkomplex der für Sicherheitszwecke erfolgenden Datenbehandlungsmaßnahmen. Die für Zwecke der Personen-, Vermögens- und öffentlichen Sicherheit angewandte Videokameraüberwachung hat sich zum heutigen Tag zu einem gewaltigen Industriezweig entwickelt. In manchen demokratische Staaten wie beispielsweise In den Vereinigten Staaten und Im Vereinigten Königreich wird zwecks Erhöhung der öffentlichen und nationalen Sicherheit die weitere Entwicklung der Überwachungs-, Aufzeichnungs- und Datenabgleichungssysteme vom Budget finanziert. Die durch die Polizei betriebenen

Überwachungskameras auf öffentlichen Straßen und Plätzen vernetzen ganze Stadtviertel, man fragt sich, ob einige Systeme wohl fähig sind, mittels Gesichtserkennungs- Softwares einzelne Passanten zu identifizieren? Spielen Kameras in den Einkaufszentren nicht nur beim Vermögensschutz eine Rolle, sondern auch bei der Auswahl bestimmter Käuferkreise? Die Kameras an den Arbeitsstätten überwachen nicht nur die Aufbewahrung der Vorschriften der sicheren Arbeitsverrichtung, sondern sie sollten etwa die Effizienz der Arbeitsleistungen der Arbeitnehmer erhöhen? Im Alltag sollte man die Vermutung gelten lassen, dass man durch die explosionsartige Verbreitung der Kameraüberwachung in geschlossenen Netzen an fast jedem Schauplatz des sozialen Kontaktierens von einem vielfach unsichtbaren Auge beobachtet wird. Kann die Intimität des Privatlebens, die Beobachtungs-Freiheit, das Alleinsein, die Freiheit von einer grundlosen Personenidentifizierung zu Wirklichkeit werden, oder wir müssen uns endgültig von der privacy verabschieden, weil wir den Schutz unserer Daten und den Schutz der an die Person geknüpften Rechte aufopfern müssen im Interesse unserer persönlichen Sicherheit? Kann der Schutz persönlicher Daten, als grundlegendes Recht gewährleisten den Schutz unseres Privatlebens, unserer Persönlichkeit oder ist dieser rechtliche Schutz nur anscheinend, und gilt der Datenschutz als technisch überholt?

In meiner Arbeit wünsche ich durch einen Überblick der obigen Themenkreise auf die als Forschungszielsetzungen formulierten Fragen Antworten zu geben, indem ich die Antworten auf die als Hypothese gestellten Fragen anhand des Überblickes der historischen Entwicklung des Datenschutzes, der Darlegung seines rechtlichen und institutionellen Systems durch Schilderung der inneren Zusammenhänge und der Erfahrungen aus der Praxis untermauere .

Zielsetzung meiner Forschung

Theoretische Zielsetzung meiner Arbeit ist es, eine detaillierte Auslegungsmethodologie des informationellen Selbstbestimmungsrechtes in horizontalen Rechtsverhältnissen zu entwickeln. In meiner Arbeit versuche ich darzulegen, ob in den sektorellen privatrechtlichen Rechtsverhältnissen mit Datenschutzbezug deren horizontale Wirkung (Drittwirkung Effekt) erfassbar ist, und wenn ja, im Rahmen welcher Rechtsgrundsätze die Verfassungswerte durchsetzbar sind. Die wissenschaftliche Novität meiner Arbeit bildet die rechtsatzweise dogmatische Entfaltung des auf Grund der Drittwirkung-Theorie entfaltbaren Instrumentariums für Rechtsdurchsetzung und Rechtsschutz bei Verletzungen und Gefährdungen des informationellen Selbstbestimmungsrechtes.

Als Ausgangsthese meines theoretischen Standpunktes dient, dass die Datenschutznormen jeweils in den Kreis des öffentlich-rechtlichen und privatrechtlichen Schutzes eingestuft werden müssen je nachdem, ob die Parteien in vertikalen oder horizontalen Rechtsbeziehungen zueinander stehen. Die Datenverwaltung durch staatliche Stellen, durch Kommunalverwaltungen, Polizei und sonstige Behörden gehört in den Bereich des öffentlich-rechtlichen Datenschutzrechtes, und die Frage der Verfassungsmäßigkeit öffentlich-rechtlicher Datenverwaltung ist nach den Grundsätzen aus dem Grundrechtsschutz, wie etwa Notwendigkeit und Verhältnismäßigkeit, zu bewerten. Dahingegen kann bezüglich eines im Bereich des Privatrechtes tätig werdenden Datenverwalters während einer Auslegung im Rahmen des privatrechtlichen Datenschutzes eine effektive Lösung für das informationelle Selbstbestimmungsrecht, die mit der Technologieentwicklung des 21. Jh. hinsichtlich Rechtsschutz und Rechtsdurchsetzung im Einklang steht, nur gefunden werden, indem man sich zur Auslegung der datenschutzbezogenen Rechtsbeziehungen der allgemeinen Rechtsgrundsätze des Zivilrechts bedient. Die allgemeinen Rechtsgrundsätze liefern eine solide Basis für die Hineindeutung der verfassungsverankerten Rechtsgüter in die zivilrechtlichen Rechtsverhältnisse, ohne dass man gezwungen wäre, das System der strengen, langwierigen und umständlichen Anforderungen in Bezug auf die Grundrechteinschränkung anwenden zu müssen. So muss man bestimmte Norminhalte, die durch die im Zivilrecht in Erscheinung tretenden Grundsätze, wie guter Glaube, Ehrlichkeit, gegenseitige Mitwirkung, Verbot des Rechtsmissbrauchs, Erfordernis des allgemein zu erwartenden Verhaltens bestimmt sind, im Einklang mit den Verfassungswerten, wie Menschenwürde, Autonomie der Persönlichkeit, Selbstbestimmungsfreiheit im Rahmen des sektorellen Datenschutzes auslegen.

II.

METHODEN UND QUELLEN DER FORSCHUNG

Während meiner wissenschaftlichen Forschung hatte ich die Möglichkeit, in der Bibliothek des Deutschen Bundestages die mein Thema betreffende deutschsprachige Fachliteratur zusammenzutragen. Die Fachbibliothek der Nationalen Telekommunikationsbehörde (*Nemzeti Hírközlési Hatóság*) hat mir beim Sammeln und Aufarbeiten der Fachliteratur in englischer und ungarischer Sprache Hilfestellung geleistet. Ich habe die während der Forschung aufgearbeitete Fachliteratur katalogisiert, die wichtigsten Feststellungen auf die Katalogzettel eingetragen, dann den Katalog nach Themenkreisen neu geordnet. Neben der Aufarbeitung von Fachliteratur erörterte ich die Fragen des Datenschutzes mit Mitarbeitern des Amtes des Datenschutzbeauftragten (*Adatvédelmi Biztosi Hivatal*) und konnte Einblick in Abläufe der Bearbeitung der Beschwerden wegen Verletzung personenbezogener Daten bekommen, die beim Amt eingereicht wurden. Eine Sammlung der Stellungnahmen des Datenschutzbeauftragten habe ich zusammengestellt und Themenkreisen zugeordnet. In Bezug auf die Aufarbeitung des Fallrechtes des ungarischen Verfassungsgerichts hat mir mein Themenleiter ausführliche Ratschläge gegeben.

Verwendete Rechtsnormen

Ungarische Rechtsnormen

Gesetze

1869.évi. III. törvény a népszámlálásról / *Gesetz III von 1869 über die Volkszählung*

1897.évi XXXV törvény a m. kir. központi statisztikai hivatalról / *Gesetz XXXV von 1897 über das Königlich Ung. Statistische Zentralamt*

1952. évi III. törvény a polgári perrendtartásról / *Gesetz III von 1952 über die Zivilprozessordnung*

1959. évi IV. törvény a Polgári Törvénykönyvről / *Gesetz IV von 1959 über das Ung. Zivilgesetzbuch*

1972. évi V. törvény a Magyar Köztársaság ügyészségéről / *Gesetz V von 1972 über die Staatsanwaltschaften der Republik Ungarn*

1992. évi XXIII. törvény a köztisztviselők jogállásáról / *Gesetz XXIII von 1992 über die Rechtstellung der öffentlichen Beamten*

1992. évi XXXIII. törvény a közalkalmazottak jogállásáról / *Gesetz XXXIII von 1992 über die Rechtstellung der Angestellten im öffentlichen Dienst*

1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról / *Gesetz LXIII von 1992 über den Schutz personenbezogener Daten und die Publizität der Daten von öffentlichem Interesse*

1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról / *Gesetz LXVI von 1992 über die Registrierung der Personendaten und Wohnadressen der Bürger*

1993. évi XXXI törvény az emberi jogok és az alapvető szabadságok védelméről szóló, Rómában, 1950. november 4-én kelt Egyezmény és az ahhoz tartozó nyolc kiegészítő jegyzőkönyv kihirdetéséről / *Gesetz XXXI von 1993 über die Verkündung der Konvention zum Schutze der Menschenrechte und Grundfreiheiten abgeschlossen in Rom am 4. November 1950, und der der dazugehörigen acht Ergänzungsprotokolle*

1993. évi LIX. törvény az állampolgári jogok országgyűlési biztosáról / *Gesetz LIX von 1993 über den Parlamentsbeauftragten der staatsbürgerlichen Rechte*

1993. évi XCIII. törvény a munkavédelemről / *Gesetz XCIII von 1993 über den Arbeitsschutz*

1994. évi XXXIV. törvény a Rendőrségről / *Gesetz XXXIV von 1994 über die Polizei*

1995. évi LXV. törvény az államtitokról és a szolgálati titokról / *Gesetz LXV von 1995 über das Staatsgeheimnis und das Dienstgeheimnis*

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről / *Gesetz LXVI von 1995 über die öffentlichen Urkunden, die öffentlichen Archive und den Schutz von Material aus Privatarchiven*

1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről / *Gesetz CXIX von 1995 über die Verwaltung von Daten über Namen und Wohnadressen, die für Forschungszwecke und unmittelbar für kommerzielle Zwecke genutzt werden*

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról / *Gesetz CXXV von 1995 über die nationalen Sicherheitsdienste*

1997. évi XXXII. törvény a határőrizetről és a Határőrségről / *Gesetz XXXII von 1997 über den Schutz der Staatsgrenze und die Grenzpolizei*

1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről / *Gesetz XLVII von 1997 über Verwaltung und Schutz der Gesundheitsdaten und der damit verbundenen personenbezogenen Daten*

1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről / *Gesetz VI von 1998 über die Verkündung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, abgeschlossen in Strassburg am 28. Januar 1981*

1998. évi XI. törvény az ügyvédekről / *Gesetz XI von 1998 über die Rechtsanwälte*

1998. évi XIX. törvény a büntetőeljárásról / *Gesetz XIX von 1998 über das Strafverfahren*

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről / *Gesetz CVIII von 2001 über einzelne Fragen der elektronischen kommerziellen Dienstleistungen sowie der mit der Informationsgesellschaft zusammenhängenden Dienstleistungen*

2003. évi III. törvény az elmúlt rendszer titkosszolgálati tevékenységének feltárásáról és az Állambiztonsági Szolgálatok Történeti Levéltára létrehozásáról / *Gesetz III von 2003 über die Aufdeckung der geheimdienstlichen Tätigkeit des vergangenen Systems und die Errichtung des Historischen Archivs der Staatssicherheitsdienste*

2003. évi C. törvény az elektronikus hírközlésről / *Gesetz C von 2003 über das elektronische Telekommunikationswesen*

2004. évi XIX. törvény a Vám- és Pénzügyőrségről / *Gesetz XIX von 2004 über die Zoll- und Finanzwache*

2005. évi XC. törvény az elektronikus információszabadságról / *Gesetz XC von 2005 über die elektronische Informationsfreiheit*

Regierungsverordnungen

17/1999 (II.5) Korm. Rendelet a távollévők között kötött szerződésekről / *Über Verträge zwischen Abwesende*

233/2001. (XII. 10.) Korm. rendelet a közszolgálati jogviszonnyal összefüggő adatkezelésre és a közszolgálati nyilvántartásra vonatkozó szabályokról

Über die Vorschriften bezüglich der mit dem Rechtsverhältnis im öffentlichen Dienst zusammenhängenden Datenverarbeitung und über das Register des öffentlichen Dienstes

226/2003. (XII. 13.) Korm. rendelet az elektronikus hírközlési szolgáltató adatkezelésének különös feltételeiről, az elektronikus hírközlési szolgáltatások adatbiztonságáról, valamint az azonosítókijelzés és hívásátírányítás szabályairól

Über besondere Bedingungen für die Datenverarbeitung durch elektronische Telekommunikationsdienstleister, über die Datensicherheit der elektronischen Telekommunikationsdienstleistungen, sowie Regeln der Anzeige der Anrufidentifizierung und Anrufumleitung

257/2000. (XII. 26.) Korm. rendelet a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvénynek a szociális, valamint a gyermekjóléti és gyermekvédelmi ágazatban történő végrehajtásáról

Über die Durchführung des Gesetzes XXXIII von 1992 über die Rechtstellung der Angestellten im öffentlichen Dienst bezüglich der sozialen sowie der Kinderwohlfahrts- und Kinderschutz-Branche

180/2004. (V. 26.) Korm. rendelet az elektronikus hírközlési feladatokat ellátó szervezetek és a titkos információgyűjtésre, illetve titkos adatszerzésre felhatalmazott szervezetek együttműködésének rendjéről

Über die Ordnung des Zusammenwirkens zw. elektronische Telekommunikationsaufgaben erfüllenden Organisationen und zum geheimen Informationssammeln bzw. zu geheimer Datenbeschaffung ermächtigten Organisationen

Ministerialverordnungen

11/1990. (VI. 13.) IM rendelet az egyházak nyilvántartásának ügyviteli szabályairól
über die Sachbearbeitungsvorschriften bei der Registrierung der Kirchen

15/1989. (X.7) KeM rendelet az egyes kereskedelmi tevékenységek gyakorlásáról
über die Ausübung einzelner kommerzieller Tätigkeiten

33/1998. (VI. 24.) NM rendelet a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről

Über die ärztliche Prüfung und Begutachtung der tätigkeitsbereichsbezogenen und berufsbezogenen bzw. persönlichen hygienischen Eignung

Beschlüsse / Entscheidungen des ung. Verfassungsgerichtes

2/1990. (II.18) AB határozat veröffentlicht in Magyar Közlöny 1990. évi 16. szám

11/1990. (V.1.) AB határozat veröffentlicht in Magyar Közlöny 1990. évi 40. szám

18/1990 (VIII.1) AB határozat veröffentlicht in Magyar Közlöny 1990. évi 74. szám

20/1990. (X.4.) AB határozat veröffentlicht in Magyar Közlöny 1990. évi 98. szám

15/1991 (IV.13) AB határozat veröfentlicht in Magyar Közlöny 1991. évi 39. szám

74/1992. (XII.28) AB határozat veröfentlicht in Magyar Közlöny 1992. évi 133. szám, AB közlöny, I. évf. 11-12. szám

21/1993 (IV.2.) AB határozat veröfentlicht in Magyar Közlöny 1993. évi 38. szám, AB közlöny, II. évf. 3. szám

29/1994. (V.20.) AB határozat veröfentlicht in Magyar Közlöny 1994. évi 55. szám, AB közlöny, III. évf. 5. szám

34/1994. (VI. 24.) AB határozat veröfentlicht in Magyar Közlöny 1994. évi 55. szám, AB közlöny, III. évf. 5. szám

60/1994. (XII.24.) AB határozat veröfentlicht in Magyar Közlöny 1994. évi 124. szám, AB közlöny, III. évf. 12. szám.

46/1995 (VI.30.) AB határozat veröfentlicht in Magyar Közlöny 1995. évi 56. szám, AB közlöny, IV. évf. 6-7. szám

58/1995 (IX.15) AB határozat veröfentlicht in Magyar Közlöny 1995. évi 76. szám, AB közlöny, IV. évf. 8-9. szám

30/1997. (IV.29.) AB határozat veröfentlicht in Magyar Közlöny 1997. évi 37. szám, AB közlöny, VI. évf. 4. szám

16/2001. (V.25.) AB határozat veröfentlicht in Magyar Közlöny 2001. évi 59. szám, AB közlöny, X. évf. 5. szám

35/2002. (VII.19.) AB határozat veröfentlicht in Magyar Közlöny 2003. évi 69. szám, AB közlöny, XII. évf. 6-7. szám

940/B/2003. AB határozat veröfentlicht in Magyar Közlöny 2007. évi. 7. szám, AB közlöny, XVI. évf. 1.

12/2004. (IV. 7.) AB határozat veröfentlicht in Magyar Közlöny 2004. évi 63. szám, AB közlöny, XIII. évf. 5.

36/2005. (X.5) AB határozat veröfentlicht in Magyar Közlöny 2005. évi 130. szám, AB közlöny, XIV. évf. 9.

Grundsatzentscheidungen des ungarischen Obersten Gerichts

BH2006. 280 Az előzetes letartóztatás egy év utáni fenntartására ad okot - egyebek mellett - ha az ügyben a sértett és (vagy) a tanúk - a vádlottak részéről történő - megfenyegetésére adatok merülnek fel, s emiatt a bizonyítási eljárás folytatása veszélybe kerül

Die Aufrechterhaltung der vorläufigen Festnahme über ein Jahr gilt als begründet - unter anderem - wenn in der Rechtssache bezüglich der Bedrohung des Verletzten und (oder) der Zeugen - seitens der Angeklagten - Hinweise/Daten auftauchen und hierdurch die Durchführung des Beweisverfahrens gefährdet wird [1998. évi XIX. törvény 132. § (1) bek. b) pont, 129. § (2) bek. c) pont].

BH2004. 170 I. Magántitok minden olyan bizalmas, - csak szűk körben, illetve beavatottak előtt ismert személyi, családi, vagyoni helyzetre, egészségi állapotra, szokásokra vonatkozó tény vagy adat, amelynek nyilvánosságra hozatala a sértettre érdeksérelemmel jár.

Als Privatgeheimnis gilt jede vertrauliche - nur im engen Kreis, bzw. nur Eingeweihten bekannte Tatsache oder Angabe, die persönliche, familiäre, Vermögenslage, Gesundheitszustand, Gewohnheiten betrifft, deren Veröffentlichung die Interessen des Verletzten verletzt .

BH2000. 293 A közszereplőről készült, karikatúrának minősülő fényképfelvétel nyilvánosságra hozatala nem sérti a képmáshoz való jogot, és az ezáltal kifejezett vélemény sem sért becsületet vagy emberi méltóságot, ha a véleménynyilvánítás nem indokolatlanul bántó, sértő vagy lealacsonyító

Die Veröffentlichung eines als Karikatur geltenden Fotos über einen öffentlichen Funktionsträger verletzt nicht das Recht am eigenen Bild und die hierdurch geäußerte Meinung verletzt nicht Ehre oder Menschenwürde, wenn diese Meinungsäußerung nicht grundlos kränkend, beleidigend oder erniedrigend ist [1959. évi IV. törvény 76. §, 80. § (1)-(2) bekezdés].

BH2000. 485 A birtokháborító magatartásról készült videofelvétel bizonyítékként való felhasználása nem minősül visszaélésnek, és nem sérti a személyhez fűződő jogokat [1959. évi IV. törvény 80. § (1)-(2) bekezdés].

Die Verwertung einer Videoaufnahme über ein Besitzstörendes Verhalten als Beweismittel kann nicht als Missbrauch bewertet werden und verletzt nicht die Personenrechte

BH1994. 27. Ügyvédek és ügyvédi irodák névhasználatával kapcsolatos jogvita elbírálásának szempontjai [Ptk. 86-87. §, 1969. évi IX. tv. (Vt.) 7. §, 1983. évi 4. tvr. 2. § (1) és (7) bek., 31. § (1) bek., 40. § (1) bek., 50. §, 1989. évi II. tv. 1-2. §, 10. §, 6/1983. (VII. 28.) IM. r. 4. §].

Gesichtspunkte für die Beurteilung der Rechtslage in Rechtsstreitigkeiten über Namensführung von Rechtsanwälten und Anwaltskanzleien

BH1985. 57. I. A személyhez fűződő jogok megsértése megvalósulhat a képmás vagy hangfelvétel visszaéléssel történő elkészítésével is. Ha a lakó a falon áthallatszó hangos kijelentéseket tesz a szomszédos lakás lakójának személyével kapcsolatban, és ez utóbbi erről a saját lakásában elhelyezett hangfelvevő berendezéssel felvételt készít, ez a magatartás nem jelent más jogvéde érdekkörében történő illetéktelen behatolást (jogsértést).

I. Eine Verletzung der Personenrechte kann verwirklicht werden auch durch missbräuchliche Anfertigung einer Bild- oder Tonaufnahme. Wenn der Bewohner durch die Wand hörbare laute Äußerungen macht über die Person des Bewohners einer benachbarten Wohnung, und dieser hierüber mittels eines in seiner eigenen Wohnung inatallierten Tonaufzeichnungsgerätes Aufnahmen macht, dieses Verhalten gilt nicht als unbefugtes Eindringen in ein geschütztes Rechtsgut eines anderen (Rechtverletzung).

Beschlüsse und Entscheidungen des ung. Obersten Gerichts

LB Pfv. IV.21. 327/1993. Bírósági Határozatok Közleménye 1994

Lef. Bír. Pfv.IV.22.415/1999. Bírósági Határozatok Közleménye 1999

III.

ZUSAMMENFASSUNG DER WISSENSCHAFTLICHEN ERGEBNISSE UND MÖGLICHKEITEN DEREN NUTZUNG

ERGEBNIS: Methodenwechsel im Datenschutz

In meiner Arbeit habe ich detailliert aufgezeigt die Entwicklung der Regulierung der personenbezogenen Daten im Rechtssystem der Europäischen Union, das - die letzten 30 Jahre Revue passiert - weltweit eines des höchsten Schutzniveaus dem Schutz der personenbezogenen Daten garantiert. Im Gemeinschaftsrecht schuf man Rahmenvorschriften, bzw. für einzelne Bereiche sektorielle Vorschriften um den einheitlichen Schutz der persönlichen Daten und für die freien Datenbewegungen über die Binnengrenzen hinweg abzusichern. Die mit dem Ziel der Verwirklichung des einheitlichen Binnenmarktes verabschiedeten Normen zur Verwaltung personenbezogener Daten wurden während der 10 Jahre nach dem Inkrafttreten auf Verfassungsebene erhoben, und das Grundrecht des Schutzes personenbezogener Daten wurde in die Grundrechtscharta der Europäischen Union aufgenommen. Das informationelle Selbstbestimmungsrecht wurde zu einem europäischen Grundrecht, welches in den nationalen Rechtsordnungen ohne Vorhandensein eines gemeinschaftsrechtlichen Tatbestandes auch unmittelbar aufrufbar ist. Ein funktionsfähiges System von Garantien für den Personendatenschutz ist dadurch entstanden, dass hinsichtlich der europäischen Institutionen die Einhaltung der Vorschriften zum Schutz der personenbezogenen Daten vom Europäischen Datenschutzbeauftragten beaufsichtigt werden. Das 21. Jh. wird von Anfang an gekennzeichnet durch eine beschleunigte Technologieentwicklung, zunehmende Globalisierung sowie durch die Internationalisierung des Terrorismus, im diesem Umfeld ist der Schutz personenbezogener Daten besonders sensibles Gebiet geworden, da markante Interessen aufgetreten sind, die das informationelle Selbstbestimmungsrecht in bisher nicht bekanntem Ausmaß einschränken wollen.

Während der letzten zwanzig Jahre der Entwicklung des ungarischen Rechtssystems ist das Recht auf Schutz personenbezogener Daten zu einem integralen Bestandteil unseres Systems der Grundrechte geworden und garantiert heute das gleiche Schutzniveau für personenbezogene Daten wie das Gemeinschaftsrecht. Das ungarische Verfassungsgericht ebnete mit mehreren Entscheidungen von großer Tragweite den Schutz personenbezogener Daten, wie etwa über die universelle Personenkennzahl, die Abgabe von Vermögenserklärungen, die geheime Observation oder die Anfertigung von Bildaufzeichnungen bei Sportveranstaltungen. Der ungarische Gesetzgeber hat in

mehreren Bereichen wie Gesundheitswesen, Direkt-Marketing, oder in den Vorschriften betreffend das Strafverfahren detaillierte Regelungen zum Schutz personenbezogener Daten geschaffen. In einigen Bereichen gingen die Regelungen nicht über die Mindestanforderungen des Gemeinschaftsrechts hinaus, wie etwa hinsichtlich der elektronischen Telekommunikation oder E-Kommerz. In anderen Rechtsgebieten wie etwa beim privacy am Arbeitsplatz, wo es keine gemeinschaftsrechtliche Regelung gibt, ist es nicht gelungen mit ausführlichen Vorschriften den Schutz der persönlichen Daten an Garantien zu binden. Nach meiner Auffassung muss man aussprechen, dass die Rechtsetzung im Bereich des Datenschutzes der technologischen Entwicklung dahinter hinkt, jedoch mit der Frage, ob dies definitiv so bleiben wird.

Aufrechterhaltung des Grundrechtsschutzes kontra technologische Rückständigkeit

Das in der Verfassung verankerte, Jedermann zustehende Grundrecht auf den Schutz der persönlichen Daten kann in der Welt der Technologie des 21. Jh. nur dann "lebendes Recht" bleiben, wenn die Methodik des Datenschutzes hinsichtlich der Rechtsbeziehungen zu den Datenverwaltern, die im Bereich des Privatrechts tätig sind sich ändert. In privatrechtlichen Rechtsverhältnissen, wo die betroffene natürliche Person dem Datenverwalter ausgeliefert, in einem System der gesellschaftlichen, sozialen Beziehungen untergeordnet ist, so in den arbeitsbezogenen Beziehungen, bei Inanspruchnahme elektronischer Telekommunikationsdienstleistungen, beim Erfüllen der Pflichten aus einem Kreditvertrag, in der elektronischen Medienwelt, muss man die Methodik der datenschutzbezogenen Regulierung umgestalten. Meines Erachtens sollte man auf Grund der vom Parlament geschaffenen Rahmenrechtsnormen neben der Geltendmachung des Grundsatzes der Selbstregulierung der Ausformulierung spezieller branchenspezifischer Datenschutzregeln freie Bahn geben.

Hält man das Regime der Regulierung des Datenschutzes ausschließlich auf der Basis der Grundrechtsdogmatik aufrecht, d.h. reguliert den Umgang mit persönlichen Daten als Gesetzgebungsgegenstand ausschließlich das Parlament, so verlieren diese Regelungen gleich an Lebensnähe, an Anwendbarkeit im Hinblick auf die technologische Entwicklung des 21. Jh. Meiner Meinung nach wenn man den Effekt der Drittwirkung des Grundrechtes bezüglich personenbezogener Daten in den horizontalen Rechtsverhältnissen erkennt, so kann man erreichen, dass das Instrumentarium des Datenschutzrechtes modernisiert wird. Man muss zugestehen, dass die Durchsetzung des informationellen Selbstbestimmungsrechtes als Grundrecht in den privatrechtlichen Verhältnissen aufgegeben werden muss, und stattdessen soll man die Entfaltung des Grundsatzes der

Ehrlichkeit in den Vordergrund stellen mit der Wirkung, dass die schutzwürdigen Verfassungswerte, nämlich die freie Entfaltung der Persönlichkeit, die informationelle Selbstbestimmung, die bewusste Einwilligung, die Zweckgebundenheit der Datenverwaltung beibehalten bleiben. Meines Erachtens ist der Grundsatz der Datensparsamkeit, der sich aus dem Grundsatz der Verhältnismäßigkeit ableiten lässt, wonach in den vertraglichen Rechtsbeziehungen unter Privatpersonen ausschließlich eine zur Erreichung eines bestimmten Zweckes erforderliche Datenverwaltung erfolgen darf, auch in den horizontalen Rechtsbeziehungen anwendbar.

Der ungarische Gesetzgeber muss bezüglich jener horizontalen Rechtsbeziehungen, bei denen angesichts der technologischen Entwicklung dies begründet ist, überprüfen, ob er seine Rechtssetzungsbefugnis im Regelungsbereich Datenschutz ausschließlich auf Gesetzgebungsebene beibehalten will. Nach meinem Standpunkt lässt der Gesetzgeber durch die Beibehaltung des bestehenden Systems die Lebensrealität des Datenschutzrechtes mitten in der Welt von Internet, digitalen Bildgebungsverfahren und massenweise Online-Telekommunikation dahinschwinden. Deshalb muss sich der Gesetzgeber die Regulierung des rechtlichen Instrumentariums des Datenschutzes zum Teil mit den Technologienawendern teilen, indem man der branchenspezifischen Selbstregulierung Möglichkeit gibt. Es genügt aber nicht, vorzuschreiben, dass die Datenverarbeiter interne Satzungen zu elaborieren haben, sondern man muss solche Regelinstrumente schaffen, die ein angemessenes rechtliches Umfeld für die Entwicklung der Informatik absichern. Der Gesetzgeber sollte vielmehr die Grundsätze für die branchenspezifischen Selbstregulierung festschreiben unter Berufung zum einen auf die allgemeinen Rechtsgrundsätze, auf die Ausübung von Treu und Glauben, das Verbot des Rechtsmissbrauchs, zum anderen durch die Geltendmachung der Datenschutzgrundsätze: Zweckbindung, Datensparsamkeit, bewusste und aufgeklärte Einwilligung des Verwenders.

Während der Regulierung des Datenschutzrechtes einzig aus technologischem Aspekt wurde die auf Notwendigkeits- und Verhältnismäßigkeits-Schranken aufgebaute Rechtsauffassung des Grundrechts anachronistisch, da hierbei die technologiegebotenen Möglichkeiten nicht berücksichtigt werden. Nach meiner Auffassung lässt sich die Grundrechtsauffassung des Datenschutzes in vielen Fällen mit der Technologie nicht vereinbaren, die man hier zu regulieren bestrebt ist. Auch der EuGH wurde mit dieser Frage konfrontiert in der Rechtsache Lindqvist, als er den Begriff Datenübermittlung in Bezug aufs Internet auslegen musste. Die Verbreitung elektronischer Technologiemedien, Infrastrukturen, die Entstehung von e-Kommerz, und die Internetnutzung durch die breite Masse, muss zwangsläufig zur Verbreitung der Datenschutzregulierungen unter Bevorzugung der technologischen Aspekte im Datenschutzrecht führen. Die Regulierung des Datenschutzes aus einer technologiezentrischen

Herangehensweise heraus (Datenschutz durch Technik) macht nicht mehr einen Unterschied zwischen staatlichen und privaten Datenverarbeitern, da die IT-Technologien unabhängig von horizontalen oder vertikalen Rechtsbeziehungen Anwendung finden. Dieser Richtung der Technologieentwicklung folgend hat auch die datenschutzrechtliche Regulierung solche Lösungswege zu gehen, die geeignet sind, die technologische Entwicklung rasch nachzuverfolgen. Eine den technologischen Möglichkeiten angepasste Regulierung des Datenschutzes könnte zu einem realen, den wirtschaftlichen Wettbewerb fördernden Faktor werden, weil sie die Einführung von neuen Technologien ermöglichen würde, die zur informationstechnischen Modernisierung des ganzen Landes beitragen könnten.

Aus der branchenspezifischen Selbstregulierung sollte sich der Gesetzgeber im Interesse des Schutzes der Grundrechte nicht entziehen, sondern er kann für bestimmte Bereiche in Form von Rahmenvorschriften diejenigen verbotenen Verhaltensformen, welche er für dem Grundsatz der Fairness widerstrebend hält, festlegen. Es könnte ebenso die im Verbraucherschutz etablierte regulatorische Methodik "schwarze Liste / graue Liste" angewandt werden. Der Gesetzgeber könnte bestimmte Vertragsbedingungen oder Verhaltensweisen als von vornherein unlautere betrachten, weil diese schwerwiegend gegen die Verbraucher- und Nutzerrechte verstoßen, diese könnte man in der schwarzen Liste aufführen. In die graue Liste kämen die Vertragsbedingungen, Praktiken, bei denen es sich nicht eindeutig um eine Rechtsverletzung handelt oder die unter den beteiligten Parteien für die betroffene Partei es durch realen Nutzen nicht kompensieren, wenn diese seine persönlichen Daten dem Datenverwalter freigeben, der Gesetzgeber sollte die Datenverarbeitung als unehrlich/unredlich werten solange, bis der Datenverwalter das Gegenteilige nicht bewiesen hat.

Gleichzeitig mit dem Methodenwechsel im Datenschutz sind auch weitere Schranken der branchenmäßigen Selbstregulierung notwendigerweise zu definieren, da man in dem grundrechtbasierten Schutz für Daten und der Durchsetzung dieses Rechtsschutzes in den vertikalen Rechtsbeziehungen, d.h. gegenüber dem Staat nicht zurückweichen darf. Vielmehr findet man einen wachsenden staatlichen Hunger auf Informationen, was die Beibehaltung und Fortbildung des Grundrechtcharakters für den Datenschutz gegenüber dem Staat gerechtfertigt.

Unter anderem sollte man ausschließen, dass die staatlichen Stellen unter dem Deckmantel der branchenmäßigen Selbstregulierung ihre Befugnisse, Daten zu erfassen, an private Datenverwalter als deren Obliegenheit übertragen, bzw. sollte es dennoch zur Normierung auf Gesetzesebene kommen, so nur in Fällen, wenn dies absolut notwendig ist, wenn dies durch Schutz des menschlichen Lebens, Gefahr für die öffentliche Sicherheit gerechtfertigt ist. Meiner Meinung nach sollten die privaten Datenverwalter nur ausnahmsweise als verlängerter Arm des Staates, zu Erfassern persönlicher Daten

werden. Wie den Ausführungen hervorgeht, ist es möglich, gleichzeitig das grundrechtbasierte Schutzsystem des Datenschutzes aufrechtzuerhalten und die Grundsätze des Datenschutzes der Technologieentwicklung anzupassen.

Datenschutzbeauftragter kontra Datenschutzbehörde

Meines Erachtens scheint zur Zeit der Datenschutzbeauftragte eine anachronistische Rolle einzunehmen, da er zum Schutz des informationellen Selbstbestimmungsrechtes als parlamentarischer Beauftragter in privatrechtlich geregelten vertraglichen Beziehungen er behördliche Rechtsanwendungsinstrumente einzusetzen hat, als eine Behörde, die über keine reellen rechtlichen Mittel verfügt. Der Datenschutzbeauftragte hat ein relativ karges rechtliches Instrumentarium, denn er kann zwar derzeit Löschungspflichten anordnen, aber er hat keine Sanktionsbefugnisse, wie sie in der behördlichen Rechtsanwendung im Einzelfall in Form von Rechtsnachteilen üblicherweise vorhanden sind. Neben dem Datenschutzbeauftragten erhielt die Nationale Telekommunikationsbehörde in einem datenschutzverwandten Bereich, bei unerwünschter E-Mail-Korrespondenz, Befugnisse aber dieser Fall wird von mir als ein allein stehendes Beispiel genannt. Meiner Meinung nach fehlt ein behördlicher Schutz des Datenschutzrechtes aus dem komplexen System des staatlichen Rechtsschutzes. Ich will damit nicht sagen, dass man Befugnisse des Datenschutzbeauftragten einer staatlichen Zentralbehörde für Datenschutz übergeben sollte, sondern man sollte eine staatliche Aufsicht über privatrechtliche, das Recht auf informationelle Selbstbestimmung betreffende Beziehungen einrichten. Es wäre nicht nötig, eine weitere Staatsbehörde für diesen Zweck aufzustellen, sondern es sollten Kompetenzen bereits bestehender Staatsverwaltungsorgane wie etwa solche für Verbraucherschutz, Telekommunikation, Bildung, Arbeitsmarkt, Krankenversicherung auf bestimmte Regelungsbereiche des Schutzes personenbezogener Daten systematisch ausgeweitet werden. So würde der Datenschutz-Ombudsmann in seine verfassungsmäßige Funktion zurückgelangen, so dass er als „offenes Auge“ des Parlamentes die Tätigkeit staatlicher Stellen kontrollieren und durch seine Stellungnahmen und Hinweise die Förderung des datenschutzbezogenen Rechtsbewusstseins dienen würde. So kann als Lösung angesehen werden, wenn die Arbeit des Datenschutzbeauftragten und die Ausübung der Befugnisse der Datenschutzbehörden in Einklang gebracht werden, indem beide Organisationssysteme während ihres Tätigwerdens das jeweils charakteristische Instrumentarium anzuwenden haben.

Persönlichkeitsschutz kontra datenschutzbezogene Gerichtsbarkeit

Ein grundlegender Zusammenhang zwischen den zivilrechtlichen Vorschriften zum Schutz der Persönlichkeitsrechte und dem Schutz personenbezogener Daten besteht darin, dass in beiden Fällen der Rechtsschutz den Schutz der Freiheit der Persönlichkeit deren Entfaltung und die Selbstidentität des Einzelnen und die Sicherung eines effektiven Auftritts gegen die Rechtsverletzenden bezweckt. Sollte es nun zu einem Methodenwechsel innerhalb des Datenschutzes kommen, so muss auch der Datenschutzgerichtsbarkeit eine wichtigere Rolle zukommen etwa dadurch, dass dem Datenschutzbeauftragten das Recht zustehen könnte, einen Prozess im öffentlichen Interesse anzustrengen, falls einzelne branchenspezifische Regelungen einer Rahmenvorschrift nicht entsprechen sollten oder wenn zum Schutz eines breiten Kreises der Betroffenen erforderliches effektives Sanktionensystem im Bereich des Datenschutzes Anwendung finden sollte.

Meines Erachtens werden Persönlichkeitsrechts-Verletzungen, so Identitätsdiebstahl, Bildnismissbrauch, Beleidigungsdelikte im 21. Jh. vielfach bereits in der Informatikwelt begangen, etwa durch Versendung falscher E-Post, Ergattern von Zugangspasswörtern, Veröffentlichung digitaler Bilder oder Verbreitung unwahrer Tatsachen im Internet. In diesen Fällen ist das rechtliche Instrumentarium des herkömmlichen Persönlichkeitsrechtsschutzes machtlos, da eine solche Beweislast auf die Unrecht erlittene Partei aufgebürdet wird, wodurch bei Rechtsverstößen die Unrecht erlittene Partei von der Geltendmachung seiner Ansprüche zurückschreckt. Da der Persönlichkeitsrechtsschutz sich auf die persönlichen Daten ebenfalls erstreckt, sofern diese computergestützt oder durch Datenerfassung und -verwaltung in anderer Weise bearbeitet werden, eröffnet sich die Möglichkeit dafür, dass man sein persönlichkeitsrechtliches Unrecht als Anspruchgrundlage auf Datenschutz definiert. Nach meiner Auffassung kann bei Verletzung der im ung. ZGB verankerten Persönlichkeitsrechte das ung. Datenschutzgesetz (Avtv.) Anwendung finden gemäß dem Grundsatz "lex specialis derogat legi generali". Rechtsschutzmittel, die auf Grund des Datenschutzgesetzes eingesetzt werden können, gewähren bei Verstößen gegen das Persönlichkeitsrecht rechtlichen Schutz, wenn es um die im Datenschutzgesetz festgelegten Fälle der Datenverwaltung handelt, ohne bestimmten Rechtsgrund oder gesetzlich festgeschriebenen Zweck. In den letzten Jahren hat sich die Datenschutzgerichtsbarkeit im ungarischen Recht zunehmend eingebürgert, und immer mehr Rechtsfälle findet man vor, wo in einem Persönlichkeitsschutzprozess Bestimmungen des ung. Datenschutzgesetzes angewendet werden. In der höchstgerichtlichen Rechtsprechung von Oberstes Gericht und Tafelgerichte wird der Begriff personenbezogene Daten in einem breiten Auslegungsspektrum interpretiert bzw. die Gerichte

sind geneigt, eine Datenübermittlung zwischen Behörden ohne gesetzliche Ermächtigung als rechtswidrig zu werten. Nach meiner Ansicht werden die Gerichte in Zukunft in zunehmender Zahl der Fälle die Vorschriften des ung. Datenschutzgesetzes anwenden müssen, da die Rechtsverstöße immer mehr mittels digitalen Mitteln, in Informatikumfeld begangen werden, wie etwa unberechtigte Observation oder Abhören, Datenübermittlung ohne gesetzliche Ermächtigung, bzw. wegen rechtswidriger Behandlung personenbezogener Daten. Eine gebündelte Deutung des Schutzes persönlicher Daten und des persönlichkeitsrechtsschützenden rechtlichen Instrumentariums sowie eine immer bewusstere Anwendung dieser Auslegungspraxis durch die Gerichte kann dazu führen, dass im 21. Jh. ein effektives Rechtsschutzsystem unser informationelles Selbstbestimmungsrecht schützen wird.

Möglichkeiten der Nutzung der wissenschaftlichen Ergebnisse:

Eine große Herausforderung für den Datenschutz im 21. Jh. Jahrhundert ist es, ob es gelingt, ein Gleichgewicht zwischen den Prinzipien die dem Schutz der Privatsphäre dienen, wie die Zweckgebundenheit der Datenverwaltung, Verhältnismäßigkeit, Verbot der Vorratsspeicherung von Daten, informationelle Selbstbestimmung und informationelle Gewaltenteilung, auf der anderen Seite öffentliche und private Datensammlung, Vorrang der Berufung auf Sicherheitsinteressen, Informations hunger der privaten Geheimdienste und unseren eigenen faulen Zugeständnissen zu finden. Im Datenschutz bedarf es eines Methodenwechsels, um auch angesichts der Anforderungen des 21. Jh. die echte Durchsetzung unseres Rechts auf Selbstbestimmung sicherzustellen. Ein Methodenwechsel im Datenschutzrecht kann Wirklichkeit werden, wenn in den privatrechtlichen Rechtsbeziehungen eine Möglichkeit gegeben sein wird mittels des Instrumentariums der branchenspezifischen Selbstregulierung ein technologieorientiertes rechtliches Umfeld auszugestalten, das im Einklang mit den Grundsätzen des Datenschutzes steht, und auch neben dem Datenschutzbeauftragte auch die öffentliche Verwaltung sich anreihet, um gemeinsam das informationelle Selbstbestimmungsrecht zu schützen, und wenn auch in der Gerichtspraxis es gelingt die klassischen Prinzipien des Persönlichkeitsrechtsschutzes und den Schutz personenbezogener Daten aufeinander abgestimmt anzuwenden.

Debrecen, 01. 03. 2010.

Dr. István Mező

IV.

VERZEICHNIS DER PUBLIKATIONEN ZUM THEMENKREIS DER DISSERTATION

MEZŐ István, A dokumentumokhoz való hozzáférés az Európai Unió jogában [*Zugang zu den Dokumenten im Recht der Europäischen Union/ in Vorbereitung auch eine World Wide Web Online Version*] eVilág : az információs társadalom folyóirata. - 2 : 11 (2003), p. 14-19.

MEZŐ István, Az információs szabadság és a computerprogramok szerzői jogi védelme [*Informationsfreiheit und urheberrechtlicher Schutz von Computerprogrammen*] In: Studia iurisprudentiae doctorandorum Miskolciensium = Miskolci doktoranduszok jogtudományi tanulmányai /[szerk. Stipta István]. - Miskolc :Bíbor, 2004. - p. 29-44. - (Miskolci Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskola Kiadványsorozata ; 5/2.)

MEZŐ István, Információs hatalommegosztás; [*Informationsgewaltenteilung*] ; Doktoranduszok fóruma : Miskolc, 2002. november 6. /[szerk. LehoczkyLászló]. - Miskolc : Miskolci Egyetem Innovációs és Technológiai Transzfer Centruma, 2003. - p. 148-154

MEZŐ István, Információs szabadságjogok a magyar alkotmánybíróság gyakorlatában [*Informationsfreiheitsrechte in der Rechtsprechung des ungarischen Verfassungsgerichts*] in: Studia iurisprudentiae doctorandorum Miskolciensium = Miskolci doktoranduszok jogtudományi tanulmányai /[szerk. Stipta István]. - Miskolc :Bíbor, 2002. - p. 23-58. - (Miskolci Egyetem Deák Ferenc Állam- és Jogtudományi Doktori Iskola Kiadványsorozata ; 2/2.)

MEZŐ István, Áttekintés az információs szabadság kialakulásáról és hazai fejlődéséről [*Überblick über die Entstehung der Informationsfreiheit und deren Entwicklung in Ungarn*] in: Studia iurisprudentiae doctorandorum Miskolciensium = Miskolci doktoranduszok jogtudományi tanulmányai /[szerk. Stipta István]. - Miskolc :Bíbor, 2002. - p. 111-133. - (Miskolci Egyetem Deák Ferenc Állam- ésJogtudományi Doktori Iskola Kiadványsorozata ; 1/2.)

MEZŐ István, Vázlat a környezeti információkhoz való hozzáférés európai és hazai szabályrendszeréről, tekintettel az adatvédelmi biztos gyakorlatára [*Skizze des europäischen und ungarischen Systems der Regulierungsvorschriften zum Zugang zu Umwelt informationen, mit Rücksicht auf die Praxis des Datenschutzbeauftragten*] in: A környezetvédelmi szabályozás elmélete és gyakorlata : a környezeti adatokhoz való hozzáférés lehetőségei a magyar közigazgatásban című konferencia előadásai *Beiträge der Konferenz Zugriff Möglichkeiten des Zuganges zu Umweltdaten in der ungarischen öffentlichen Verwaltung* /[szerk. Fodor László]. - Debrecen : Lícium-Art, 2004. - p. 161-178. - (Debreceni konferenciák ; 2.)

MEZŐ István, A dokumentumokhoz való hozzáférés az Európai Unióban [*Zugang zu den Dokumenten in der Europäischen Union*] in: Collectio Iuridica Universitatis Debreceniensis. - 4 (2005), p. 151-180.

MEZŐ István, Vázlat az információs szabadságjogok kialakulásáról, [*Skizze zur Entstehung der Informationsfreiheitsrechte*] : Doktoranduszok fóruma *Doktoranden Forum*: Miskolc : 2001. november 6. /[szerk. LehoczkyLászló]. - Miskolc : Miskolci Egyetem Innovációs és Technológia Transzfer Centrum, 2002. - p. 189-194.

Debrecen, 01.03.2010.

Dr. Mező István