USBILIM 1ST INTERNATIONAL CONGRESS ON FORENSIC SCIENCES AND LAW

CONGRESS BOOK

Issued: 15. 12. 2021

ISBN: 978-605-71182-2-6

USBILIM 1ST INTERNATIONAL CONGRESS ON FORENSIC SCIENCES AND LAW

Edited by

Dr. Gültekin GÜRÇAY

Issued: 15. 12. 2021
ISBN: 978-605-70910-7-9

ABOUT CONGRESS

USBILIM 1ST INTERNATIONAL CONGRESS ON FORENSIC SCIENCES AND LAW

DATE – PLACE

NOVEMBER 27 – 28, 2021
ANKARA - TURKEY

ORGANIIZATION

Academy Conferences

CONGRESS ORGANIZING BOARD

Head of Organizing Board: Dr Gültekin Gürçay
Organizing Committee Member: Dr. Leman Kuzu
Organizing Committee Member: Dr. Mehdi Meskini Heydarlou
Organizing Committee Member: Dr.Amaneh Manafidizaji
Organizing Committee Member: Dr. Nadire Kantarcıoğlu
Organizing Committee Member: Dr. Zehra Fırat
Organizing Committee Member: Tuğçe Biter

EVALUATION PROCESS

All applications have undergone a double-blind peer review process.

PRESENTATION

Oral presentation

Participated Countries

Spain – Ukraine- UK - South Africa- Iran – Hungary

LANGUAGES

Turkish, English, Russian

SCIENTIFIC & REVIEW COMMITTEE

Dr. Gulmira ABDİRASULOVA - Kazak Devlet Kızlar Pedagoji Üniversitesi

Prof. Dr. Yunir ABDRAHIMOV - Ufa State Petroleum Technological University

Doç. Dr. Nazilə Abdullazadə - Azərbaycan Dövlət Pedaqoji Universiteti

Dr. Maha Hamdan ALANAZİ - Riyad Kral Abdülaziz Teknoloji Enstitüsü

Dr. Dzhakipbek Altaevich ALTAYEV - Al – Farabi Kazak Milli Üniversitesi

Doç. Dr. Mehmet Fırat BARAN - Mardin Artuklu Üniversitesi

Dr. Amina Salihi BAYERO - Yusuf Maitama Sule Üniversitesi

Dr. Karligash BAYTANASOVA - Al – Farabi Kazak Milli Üniversitesi

Dr. Baurcan BOTAKARAEV - oca Ahmet Yesevi Üniversitesi

Dr. Ahmad Sharif FAKHEER - Ürdün Devlet Üniversitesi

Dr. Zehra FIRAT

Doç. Dr. Abbas GHAFFARI - Tebriz Üniversitesi

Prof.Dr. Ariz Avaz GOZALOV - oskova Devlet Üniversitesi

Prof. Dr. Gulzar İBRAGİMOVA - Bakü Avrasya Üniversitesi

Dr. Gültekin GÜRÇAY

Doç. Dr. Dilorom HAMROEVA - Özbekistan Bilimler Akademisi

Dr. Bazarhan İMANGALİYEVA - K.Zhubanov Aktobe Devlet Bölge Üniversitesi

Dr. Keles Nurmaşulı JAYLIBAY - Kazak Devlet Kızlar Pedagoji Üniversitesi

Dr. Mamatkuli Jurayev - Özbekistan Bilim Akademisi

Dr. Kalemkas KALIBAEVA- Kazak Devlet Kızlar Pedagoji Üniversitesi

Dr. Bouaraour Kamel - Ghardaia Üniversitesi

Dr. Nadire KANTARCIOĞLU

Prof. Dr. Ergün KOCA - Girne Amerikan Üniversitesi

Prof Dr. Bülent KURTİŞOĞLU - Ardahan Üniversitesi

Dr. Leman KUZU - İstanbul Kültür Üniversitesi

Sonali MALHOTRA - Delhi Balbahtri Academy

Dr. Alia R. MASALİMOVA - Al – Farabi Kazak Milli Üniversitesi

Prof. Muntazir MEHDI - Pakistan Language Academy

Dr. Amanbay MOLDIBAEV - Taraz Devlet Pedagoji Üniversitesi

Doç. Dr. Yeliz ÇAKIR SAHİLLİ - Munzur Üniversitesi

Dr. Aysulu B. SARSEKENOVA - Orleu Milli Kalkınma Enstitüsü

Dr. Gulşat ŞUGAYEVA - Dosmukhamedov Atyrau Devlet Üniversitesi

ACADEMY INTERNATIONAL CONGRESS
November 27 - 28 , 2021
Ankara - Turkey

CONGRESS PROGRAM

Online (with Video Conference) Presentation

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

IMPORTANT, PLEASE READ CAREFULLY

- To be able to make a meeting online, login via https://zoom.us/join site, enter ID instead of "Meeting ID
- or Personal Link Name" and solidify the session.
- The Zoom application is free and no need to create an account.
- The Zoom application can be used without registration.
- The application works on tablets, phones and PCs.
- Speakers must be connected to the session **10 minutes before** the presentation time.
- All congress participants can connect live and listen to all sessions.
- During the session, your camera should be turned on **at least** %70 of session period
- Moderator is responsible for the presentation and scientific discussion (question-answer) section of the session.

TECHNICAL INFORMATION

- Make sure your computer has a microphone and is working.
- You should be able to use screen sharing feature in Zoom.
- Attendance certificates will be sent to you as pdf at the end of the congress.
- Moderator is responsible for the presentation and scientific discussion (question-answer) section of the session.
- Before you login to Zoom please indicate your name surname and hall number,

exp. H-..., S- ... NAME SURNAME

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Health, Pharmacology and Veterinary

28. 11. 2021	10: 00 – 13:00
Meeting ID: 873 3586 1181	Passcode: 281121
HALL: 1 SESSION: 1	MODERATOR: FARAH BAKHISHLI
ADEM TEKE EBRU YILDIRIM	Hücre Kültürü Çalışmalarının Sitotoksisite Çalışmalarına Katkısı
SERRA ORAK MUSTAFA YAMAN ÖMER FARUK MIZRAK	Glutensiz Ürünlerin B Grup Vitamin Kompozisyonunun Belirlenmesi Ve Sağlıklı Beslenme Açısından Değerlendirilmesi
ASSIS. PROF. K.R. PADMA READER, K.R.DON	Nutritional Quality and Shelf life of Radiation processed Health mix for Anaemia
MELİKE ERDURAN CANSU AYDIN SERAP YALÇIN AZARKAN	Türkiye'nin İç Anadolu Bölgesinden Elde Edilen Inula helenium Bitkisinin İlaç Dirençli Meme Kanseri Hücre Hatlarında Sitotoksik, Metastatik Etkisinin 2d ve 3d Model Hücre Hatları Üzerinde Araştırılması
DURMUŞ BURAK DEMİRKAYA MEHMETHAN YILDIRIM SERAP YALÇIN AZARKAN	Sisplatin Dirençli Ve Duyarlı Meme Kanser Hücre Hatlarında Sodyum Azid'in Sitotoksik, Metastatik Ve Katalaz Enzim Aktivitesi Seviyesindeki Değişikliklerin Karşılaştırmalı Olarak Araştırılması
ARSLAN SAY DEMET ÇAKIR	Covid-19 Ve Gebelik

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

ARSLAN SAY DEMET ÇAKIR	Covid-19; Başlangıçtan Günümüze Kullanılan İlaçlar
DEMET ÇAKIR ARSLAN SAY	Covit-19 Pandemisi Boyunca Emzirme
DEMET ÇAKIR ARSLAN SAY	Covit-19 Ve Doğum Öncesi Bakım
SEVINJ FATULLAYEVA FARAH BAKHISHLI	Experimental Hygienic Study Of Washes From The Skin Of Students
FARAH BAKHISHLI SEVINJ FATULLAYEVA	Some Radiation Risks In Oil Production

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Health, Pharmacology and Veterinary

28. 11. 2021	10: 00 – 13:00
Meeting ID: 853 0711 8876	Passcode: 281121
HALL: 2 SESSION: 1	MODERATOR: KHANITTA NUNTABOOT
PRIYADHARSHINI. P	Prediction of Diabetes Mellitus using XG Boost-Gradient Boosting
RAJARSHI KAYAL DEBOJYOTI BHATTACHARJEE SUDIP K BANERJEE KRISHANU BANIK	Lipid Peroxidation Status in Type-2 Diabetic Population in Kolkata, India
B. PRAKASH BABU HUBAN THOMAS	Course of Maxillary Artery through Loop of Auriculotemporal Nerve and Deep to Posterior Division of Mandibular Nerve
S. ABED S. O'NEILL	Nurses' Views on 'Effective Nurse Leader' Characteristics in Iraq
DO THI HA, KHANITTA NUNTABOOT	Actual Nursing Competency among Nurses in Hospital in Vietnam
B. R. O. OMIDIWURA, A. F. AGBOOLA, E. A. IYAYI	Effect of L-Dopa on Performance and Carcass Characteristics in Broiler Chickens
HAMADA A. AHMED, KADRY M. SADEK AYMAN E. TAHA	Impact of Two Herbal Seeds Supplementation on Growth Performance and Some Biochemical Blood and Tissue Parameters of Broiler Chickens

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Forensic Sciences and Law

28. 11. 2021	10: 00 – 12:00
Meeting ID: 873 3586 1181	Passcode: 281121
HALL: 3 SESSION: 1	MODERATOR: NAZAKAT GAZİYEVA
METİN PEHLİVAN	Uzlaştırma Raporunun İş Kazasından Kaynaklı Tazminat Taleplerine Etkisi
NAZAKAT GAZİYEVA	Fonoskopik Çalışmalarda Keşfedilen Bireysel Konuşma Özelliklerinin Önemi
HİLAL İFAKET AKBAŞ	Adli Bilim Eğitimini Kıta Avrupası'nda Ve Türkiye Perspektifinde Değerlendirme
HİLAL İFAKET AKBAŞ	Suçlu Davranışının Açıklanmasında Suç Ve Çocuk
DR. ÖĞR. ÜYESİ BUKET ÇATAKOĞLU AYDIN	Elektronik Bono Ve Çek İle Kambiyo Senetlerinde Değişen Özellikler
TUĞÇE BİTER	Cinsel Saldırıda Adli Hemşirenin Rolleri
DOÇ. DR. AHMET ERTUĞRUL	Uluslararası Ticaret Hukuku Bağlamında Pandemi Dönemindeki İşletme Taahhütlerinin Analizi

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Forensic Sciences and Law

28. 11. 2021	10: 00 – 12:00
Meeting ID: 853 0711 8876	Passcode: 281121
HALL: 4 SESSION: 1	MODERATOR: ROXAN VENTER
MARIA LUBOMIRA KUBICA	Legal Doctrine on Rylands v. Fletcher: One more time on Feasibility of a General Clause of Strict Liability in the UK
NADIIA MAKSIMENTSEVA	Distinctive Features of Legal Relations in the Area of Subsoil Use, Renewal and Protection in Ukraine
FAHAD ALANAZI ANDREW JONES	A Method to Enhance the Accuracy of Digital Forensic in the Absence of Sufficient Evidence in Saudi Arabia
ROXAN VENTER	Enforcement of Decisions of Ombudsmen and the South African Public Protector: Muzzling the Watchdogs
MAHDI KARIMI	The Role of the Accused's Attorney in the Criminal Justice System of Iran, Mashhad 2014
ABDELHAFEZ ABDEL HAFEZ	Dependency Theory on Examining the Relationship between the United States and the Middle East: In the Case of Iran, Saudi Arabia, and Turkey

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Organizational Behavior Researches and Management

28. 11. 2021 Meeting ID: 873 3586 1181	10: 00 – 12:00 Passcode: 281121
HALL: 5 SESSION: 1	MODERATOR: Dr. ÖĞR. ÜYESİ ALAATTİN FIRAT
FAHRİ ALP ERDOĞAN MURAT SAĞBAŞ	Covid-19 Sürecinde Örgütlerin Dijital Liderlere Artan İhtiyacı
DR. ZEHRA FIRAT Dr. ÖĞR. ÜYESİ ALAATTİN FIRAT	Liderlik Özellikleri Ve Kurumsal Kimlik Arasındaki Ilişkinin Analizi Çalışması
DR. NADİRE KANTARCIOĞLU	Örgütsel Vatandaşlık Davranışı ve Duygusal Zeka Arasındaki İlişki; Bankacılık Sektöründe Bir Araştırma
WAFA GHONAIM	A Multi-Agent Smart E-Market Design at Work for Shariah Compliant Islamic Banking
DR. LEMAN KUZU	Kobilerde Etkin Liderlik Ve Etkin Liderliğin Çalışan Motivasyonu Üzerine Etkilerinin İncelenmesi: İstanbul İl Sınırları Avcılar İlçesinde Bulunan 5 Kobinin Çalışanları Üzerine Bir Araştırma
DR. GÜLTEKİN GÜRÇAY	Yönetici Ve Işverenlerin Dini Tutum Ve Davranışlarının Çalışanların Örgütsel Adalet Algısına Etkisi

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Organizational Behavior Researches and Management

28. 11. 2021	10: 00 – 12:00
Meeting ID: 853 0711 8876	Passcode: 281121
HALL: 6 SESSION: 1	MODERATOR: ELINA BAKHTIEVA
CHARITA JASHI	Applications of Social Marketing in Road Safety of Georgia
FEDDAOUI AMINA	UK GAAP and IFRS Standards: Similarities and Differences
ELINA BAKHTIEVA	Digital Marketing Maturity Models: Overview and Comparison
DINABANDHU MAHATA AMIT KUMAR AMBARISH KUMAR RAI	Female Work Force Participation and Women Empowerment in Haryana
ENELI KINDSIKO KULNO TÜRK	Detecting Major Misconceptions about Employment in ICT: A Study of the Myths about ICT Work among Females

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Interdisciplinary Congress on Intelligence and International Relations

28. 11. 2021	10: 00 – 12:00
Meeting ID: 873 3586 1181	Passcode: 281121
HALL: 7 SESSION: 1	MODERATOR: PHATTHANAN CHAIYABUT
HACI MEHMET BOYRAZ	Hakikat-Sonrası Dönemde Türkiye Aleyhinde Dezenformasyon Faaliyetleri
HACI MEHMET BOYRAZ	Policy Of Greek Cypriot Administration Of Southern Cyprus Towards PKK
TAPAO KANYAPAT U.	The Operation Strategy and Public Relations Trend for Public Relations Strategies Development in Thailand
İBRAHİM BORA ORAN	Uluslararası Ekonomide Doğrudan Yabancı Yatırımların Bölgesel Dağılımının Analizleri
ZHANAR ALDUBASHEVA, MUKHTAR SENGGIRBAY, ELNURA ASSYLTAYEVA	The U.S. and Western Europe Role in Resolving the Religious Conflicts in Central Asia
DIMITRIS GEORGOUTSOS, PETROS M. MIGIAKIS	European and International Bond Markets Integration
SENIAN MALIE ORIAH AKIR	Determinants for Success in Expatriation of Malaysian International Corporations
PHATTHANAN CHAIYABUT	The Effect of the National Culture on the International Business

1st International Congress on Artificial Intelligence Studies

28. 11. 2021	14: 00 – 16:00
Meeting ID: 873 3586 1181	Passcode: 281121
HALL: 1 SESSION: 2	MODERATOR: DR. ÖĞR. ÜYESİ ASLI ÜNER KAYA
DR. ÖĞR. ÜYESİ ASLI ÜNER KAYA	**Felsefi Zombilerin Düşünülebilirliği Fizikalizm İçin Ne İfade Eder?**
BOUNSONG SORKEOMANY PHD PHONESAVANH THEPPHASOULITHONE SOULICHANH LUANGSOMBATH THIPPHAVANH KHANTHAPHONE SOMPHIEN MAHAPHOM THİPHACHANH NOUTHAPHONE	**The Language Learning Styles and Learning Strategies Relationship in Depart of English, Faculty of Education, Champasack University**
DAMLA TIPIOĞLU PH.D. AKIN ÖZKAN PH.D. HILAL KAYA PROF. DR. FATİH VEHBİ ÇELEBİ	**Automatic Segmentation And Counting Of Leukemia Cancer Cells On Hemocytometer With U-Net**
AYHAN TOKMAK DOÇ. DR. ÖVGÜ CEYDA YELGEL	**Yapay Sinir Ağları İle Yenilenebilir Enerji Kaynaklarından Elektrik Üretimi Tahmini**

1st International Congress on Artificial Intelligence Studies

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

28. 11. 2021	14: 00 – 16:00
Meeting ID: 853 0711 8876	Passcode: 281121
HALL: 2 SESSION: 2 MODERATOR: ZELJKO PANIAN	
ZELJKO PANIAN	A New Dimension of Business Intelligence: Location-based Intelligence
LIPENG ZHANG, LIMEI LI, YANMING PEARL ZHANG	Using Information Theory to Observe Natural Intelligence and Artificial Intelligence
MARTÍN AGÜERO, FRANCO MADOU, GABRIELA ESPERÓN, DANIELA LÓPEZ DE LUISE	Artificial Intelligence for Software Quality Improvement
KHALED M. ALHAWITI	Advances in Artificial Intelligence Using Speech Recognition
MAAMAR ALI SAUD AL TOBI, GERAINT BEVAN, K. P. RAMACHANDRAN, PETER WALLACE, DAVID HARRISON	Experimental Set-Up for Investigation of Fault Diagnosis of a Centrifugal Pump
DEEPIKA BHALLA, RAJ KUMAR BANSAL, HARI OM GUPTA	Application of Artificial Intelligence Techniques for Dissolved Gas Analysis of Transformers-A Review

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Education Studies

28. 11. 2021	14: 00 – 16:00
Meeting ID: 873 3586 1181	Passcode: 281121
HALL: 3 SESSION: 2	MODERATOR: DR. LEMAN KUZU
MELİKE ŞEN PROF. DR. AHMET ÜSTÜN	Üstün Yetenekli Çocukların Sınıf Ortamında Karşılaştıkları Sorunlara Yönelik Öğretmen Algılarının İncelenmesi
TAMER SARI	Sembolik Çerçevede Okul Müdürü Makam Odalarını Anlamak
CAHİT TAŞDEMİR	Lise Son Sınıf Öğrencilerinin Matematik Öğrenimi İle İlgili İnançları
HALİL TAŞ	Sınıf Öğretmenlerinin Hayat Bilgisi Dersindeki Sınıf İçi Öğretim Uygulamalarına İlişkin Bir İnceleme
SERDAR YEŞİL GÜROL ZIRHLIOĞLU AHMET YAYLA	Öğretmen Ve Öğretmen Adaylarının Sosyal Bilgiler Dersinde Adalet Değerine İlişkin Tutumu
SERDAR YEŞİL AHMET YAYLA GÜROL ZIRHLIOĞLU	Öğretmen Ve Öğretmen Adaylarının Sosyal Bilgiler Dersinde Adalet Algısı
HÜSEYİN ÇETİN DR. ÖĞR. ÜYESİ GÜLŞAH TURA	Sınıf Öğretmenlerinin Uzaktan Eğitime Yönelik Öz Yeterliklerinin İncelenmesi

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Education Studies

28. 11. 2021	14: 00 – 16:00
Meeting ID: 873 3586 1181	Passcode: 281121
HALL: 4 SESSION: 2	MODERATOR: DR. ÖĞR. ÜYESİ MUHAMMED SAİD AKAR
ÖZLEM ÇEVİK HAYRİYE SOYALP	Güncellenen Beşinci Sınıf Türkçe Ders Kitabının Değerlendirilmesi
CEMALETTİN YİĞİT PROF. DR. HATİCE KUMCAĞIZ	Lise Öğrencilerinin Akademik Erteleme Davranışları İle Okul Tükenmişliği Arasındaki İlişkinin İncelenmesi
FATMA TİRYAKİ DR. ÖĞR. ÜYESİ MUHAMMED SAİD AKAR	Öğretmen Adaylarının Sosyalleşme Taktiklerinin Farklı Değişkenler Açısından Belirlenmesi
MARTINA HOLENKO DLAB, NATASA HOIC-BOZIC	Student and Group Activity Level Assessment in the ELARS Recommender System
EDA YÜKSEL KARADAĞ DR. ÖĞR. ÜYESİ MUHAMMED SAİD AKAR	Öğretmen Adaylarının Analojiye Yönelik Tutumlarının Farklı Değişkenler Açısından Belirlenmesi
FİLİZ AYDIN DR. ÖĞR. ÜYESİ MUHAMMED SAİD AKAR	Öğretmen Adaylarının Yazmaya Yönelik Tutum Ve Kaygılarının Farklı Değişkenler Açısından Belirlenmesi

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

SERAP LALE IŞIK İBRAHİM KAYA	Tarih Öğretiminde Yenilikçi Etkinliklerle Materyal Hazırlama
PHONESOUDA VONGTHONG SOULICHANH LUANGSOMBATH THIPHACHANH NOUTHAPHONE BOUNMY PHALYCHAN SOULIYA KEOVILAYSACK THIPPHAVANHKHANTAPHONE CHANSY PHOMPHITHAK DAOVY PONGPANYA	Thriving Foundational Skills For Students In The Future Work

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Education Studies

28. 11. 2021	14: 00 – 16:00
Meeting ID: 853 0711 8876	Passcode: 281121

HALL: 5	SESSION: 2	MODERATOR:	REIKO YAMAMOTO

SANIA K. RAO	Relationship Between Time Management Behaviour,Job Satisfaction And Job Performance Of Teachers In Higher Education Institutions In India
OKESH GOWDA J K V VISWANATHA	A Approach In Fuzzy Sets For Feature Reduction
ROHINI KARUNAKARAN, SRIKUMAR P S	Item Analysis To Improve The Fairness Of Multiplechoice Questions
SWATI AGARWAL SHWETA JAIN	Evolution & Development Of Education For CWSN (Child With Special Needs) In India
RAMINDER PAL SINGH, SANGEETA ARORA	ERP Challenges In Higher Education
OMAR ALSHEHRI VIC LALLY	Students' Perceptions of the Use of Social Media in Higher Education in Saudi Arabia
REIKO YAMAMOTO	The Effect of Realizing Emotional Synchrony with Teachers or Peers on Children's Linguistic Proficiency: The Case Study of Uji Elementary School
SOBHY FATHY A. HASHESH	The Effect of an Al Andalus Fused Curriculum Model on the Learning Outcomes of Elementary School Students

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Mathematics, Engineering, Architecture

28. 11. 2021	14: 00 – 16:00
Meeting ID: 873 3586 1181	Passcode: 281121
HALL: 6 SESSION: 2	MODERATOR: ÖĞR. GÖR. DR. HÜSNÜ AYDEMİR
MELİH GÜZEL ÖZLEM AKPINAR	Ekmek Atıklarının Komagataeibacter hansenii GA2016 İle Bakteriyel Selüloz Üretiminde Kullanılarak Değerlendirilmesi
CHANSY PHOMPHITHAK SOULICHANH LUANGSOMBATH KHONGSOMBATH PHOMMATHEP PHOUTHONG VANHNIVONGKHAM SOMPHANE SYSAVATH PHONESOUDA VONGTHONG DALASOUK KHAMLUNVILAIVONG	Factors Associated With Road Accidents Among Motor Vehicle Drivers At Champasack Province, Lao PDR
ÖĞR. GÖR. DR. HÜSNÜ AYDEMİR DR. ÖĞR. ÜYESİ MÜSLÜM EROL	Influence Of Ambient Temperature On Diameter And Pore Size Of Electrospun Nanofibers
G. VIRANYA, G.SRIDEVI	Design Of Low Power And High Speed FIR Filter Using Koggestone CSLA

ACADEMY INTERNATIONAL CONGRESS
November 27 – 28, 2021
Ankara - Turkey

1st International Congress on Mathematics, Engineering, Architecture

28. 11. 2021	14: 00 – 16:00
Meeting ID: 853 0711 8876	Passcode: 281121
HALL: 7	SESSION: 2 MODERATOR: K. PRASANNA LAKSHMI
K. PRASANNA LAKSHMI	Motion Planning for Multiple Robots in Minimum Time Interval in Cluttered Environment
SAEED SAYYAD HAGH SHOMAR	Analysis and Evaluation of the Public Responses to Traffic Congestion Pricing Schemes in Urban Streets
CATHERİNE MAWARE, OLUFEMİ ADETUNJİ	Lean Impact Analysis Assessment Models: Development of a Lean Measurement Structural Model
FELİCİA MAGPANTAY KENZU ABDELLA	A Two-Species Model for a Fishing System with Marine Protected Areas
ALEXANDER Y. VANINSKY	Environmental Performance of the United States Energy Sector: A DEA Model with Non-Discretionary Factors and Perfect Object

UZLAŞTIRMA RAPORUNUN İŞ KAZASINDAN KAYNAKLI TAZMİNAT TALEPLERİNE ETKİSİ

Metin PEHLİVAN (Uzlaştırmacı)

Kırklareli ÜNİVERSİTESİ

Orcid No: 0000-0002-7214-9563

ÖZET

Ceza hukukundaki bazı düzenlemeler, hukuk davalarında bazı hakların talep edilmesini engelleyebilmektedir. Düzenlemelerden biri, CMK' nun 253/19'da hüküm altına alınmıştır. CMK 253.Madde hükmü, meydana gelen iş kazasının taksirle yaralama suçunu oluşturması halinde, tazminat hukuku açısından sonuç doğurucu niteliğe haizdir. Hükme göre taraflar arasında uzlaşma sağlanması durumunda soruşturmaya konu olan suçtan kaynaklı tazminat davası açılamayacaktır. Tarafların uzlaşma ile açılmış olan davalardan feragat ettiği kabul edilir. Uzlaştırmacı tarafından hazırlanan, taraflarca imzalanan rapor ilam niteliğinde olduğu için aksinin aynı kuvvete belge ile ispatlanması gerekecektir.[1] İş kazasından kaynaklı tazminatların uzlaştırma raporuna konu olduğu durumda; öncelikle meydana gelen kazanın iş kazası olduğu tespit edilecektir.[2] İş kazası tespitinden sonra uzlaştırma raporunda, talep edilen tazminat miktarlarının açık ve net bir şekilde belirtmesi gerekir. Talep edilen tazminat miktarının, uzlaşma tarafının talebine göre değil, objektif kriterlere göre belirlenecektir.[3] Uzlaştırma raporunda yer alan, objektif kriterlere göre belirlenen tazminat miktarlarının ödemesi halinde, uzlaştırmanın tarafı olan şüpheli veya sanık açısından borç ifa edilmiş olacaktır. Uzlaştırma raporunda kararlaştırılan miktar ile objektif kriterler göre tespit edilen miktar arasında açık orantısızlık olduğu varsa; ödenen miktar, objektif kriterlere göre belirlenen tazminat miktarlarından mahsup edilecek, kalan kısım tazminat talebine konu olabilecektir. İfanın gerçekleşmesiyle birlikte, soruşturmaya konu olan suç nedeniyle iş kazasından kaynaklı tazminat davası açılamayacaktır.

Anahtar Kelimeler: İş Kazası, Uzlaştırma Raporu, Tazminat Talebi

[1] Yargıtay 17. Hukuk Dairesi 2016/13482 E., 2019/3613 K.T. 26.03.2019; Konya Bölge Adliye Mahkemesi 3. Hukuk Dairesi 2021/888 E., 2021/1071 K.T. 01.09.2021 www.legal.net

[2] Yargıtay 21. Hukuk Dairesi 2018/229 E, 2019/779 K.T. 11.02.2019 www.legal.net

[3] Yargıtay 13. Ceza Dairesi 2020/6353 E, 2020/10810 K.T. 03.11.2020 Www.Legal.Net

THE EFFECT OF THE CONCILIATION REPORT ON COMPENSATION FROM OCCUPATIONAL ACCIDENTS

Abstract

Some regulations in criminal law may prevent some rights from being claimed in civil cases. One of the regulations is stipulated in 253/19 of the CMK. The provision of Article 253 of the CMK has a consequential nature in terms of compensation law if the occupational accident that occurred constitutes the crime of injury by negligence. According to the provision, in the event that a compromise is reached between the parties, a lawsuit for compensation arising from the crime that is the subject of the investigation cannot be filed. It is accepted that the parties have waived the lawsuits opened by settlement. Since the report prepared by the mediator and signed by the parties is in the nature of a verdict, the opposite will have to be proven with the same forceful document. In cases where compensations arising from work accidents are subject to reconciliation report; First of all, it will be determined that the accident occurred is a work accident. After the work accident is determined, the amount of compensation requested should be clearly stated in the mediation report. The amount of compensation requested will be determined according to objective criteria, not according to the request of the conciliation party. In case the compensation amounts determined according to the objective criteria in the mediation report are paid, the debt will be fulfilled in terms of the suspect or the accused who is the party to the mediation. If there is a clear disproportion between the amount determined in the mediation report and the amount determined according to objective criteria; The amount paid will be deducted from the compensation amounts determined according to objective criteria, and the remaining amount may be subject to a claim for compensation. With the realization of the performance, a lawsuit for compensation arising from a work accident cannot be filed due to the crime that is the subject of the investigation.

Key Words: Occupational Accident, Conciliation Report, Compensation Claim

FONOSKOPİK ÇALIŞMALARDA KEŞFEDİLEN BİREYSEL KONUŞMA ÖZELLİKLERİNİN ÖNEMİ

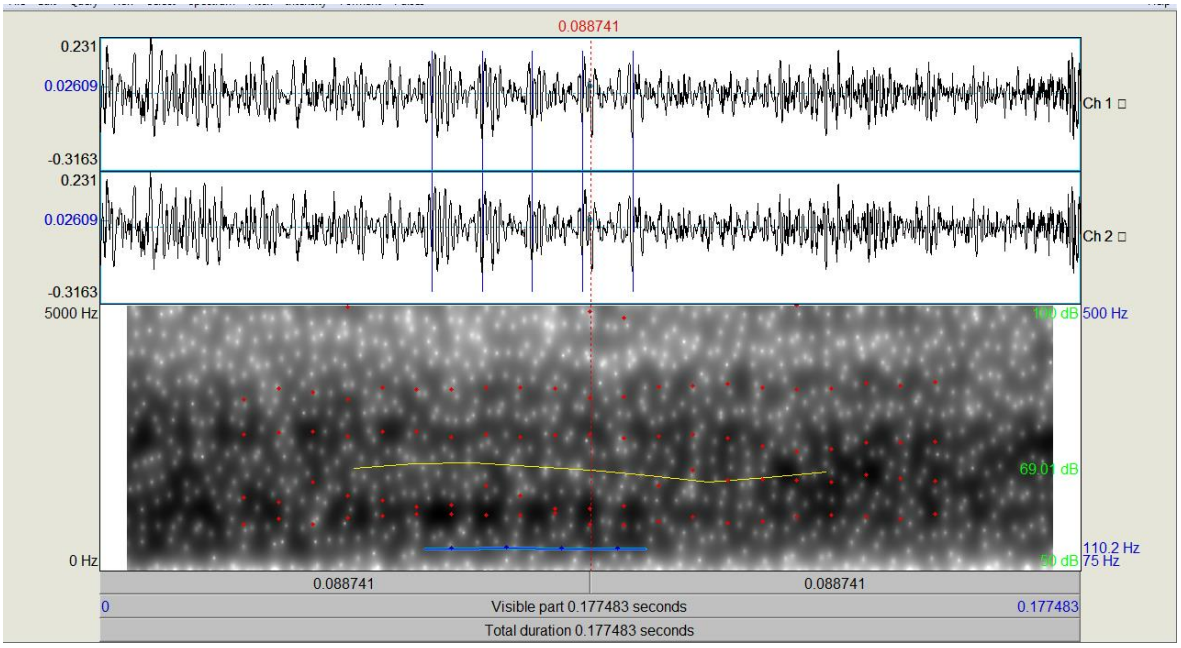
Nazakat Gaziyeva
Azerbaycan Milli İlimler Akademisi Dilbilim Enstitüsü, Azerbaycan, Bakü
+994 51 660 52 13

Özet

Modern zamanlarda, konuşma teknolojisi alanındaki araştırmalar, özel uygulamaları nedeniyle ilgili kabul edilir. Konuşma sinyali analizi, bu alanın modern teknolojilerin uygulanmasıyla gelişmesi, konuşma sentezi, konuşma tanıma, konuşma tabanlı tanımlama gibi birçok uygulamanın gelişimini teşvik eder. Modern fonoskopik araştırmalar, fonogramın sadece akustik analizine ve tanımlanmasına değil, aynı zamanda birçok farklı perspektiften yaklaşarak yaş, cinsiyet, mesleğin tanımlanmasına da izin vermektedir. Bu yaklaşımla araştırma, farklı kimlik sorunlarını - sosyal, ulusal, mesleki, cinsiyet ve yaş özellikleriyle ilgili faktörleri - belirlemek için yararlı materyaller sağlar.

Fonoskopik araştırma sırasında, konuşma sinyaline dayalı olarak kişiyi tanımlamak için özel "anahtarlar" kullanılır. Bu çalışmalarda anahtar konulardan biri, sesin akustik ve artikülatör özelliklerini dikkate alarak bu "anahtarların" tespiti için doğru metodoloji seçimidir. Adli muayenede fonoskopik inceleme için değerli bilgiler sağlayabilecek bu tür “anahtarlar” arasında ana sesin sıklığı, biçim göstergeleri, biçim göstergelerinin oranı, sesli harflere göre yoğunluk ve tonlama ile ilgili bazı özelliklerden söz edebiliriz. Fonoskopik çalışmalarda yaygın olarak kullanılan özellikler arasında ünsüz seslerle ilişkilendirilen işaretler yer almaktadır. Burun ünsüzlerinin telaffuzu sırasında hem ağız hem de burun boşluğu rezonatör görevi gördüğünden, burun boşluğunun bireysel geometrik boyutları, m, n ünsüzleri boyunca geliştirilen sesli harflerin biçim değerlerini büyük ölçüde azaltır. Ayrıca tanımlamada bir anahtar "anahtar" olarak kullanılır.

Ünsüzlerin dikkat çeken bir diğer özelliği de ünsüz ses içindeki tonun gözlemlenmesidir. Deney, bu özelliğin bireysel olduğunu ve farklı insanların konuşmalarında kendini farklı şekilde gösterdiğini gösterdi.



"X" sesinin içinde dört periyodik ton olduğu açıktır. Bu durum bireysel bir özellik olarak dikkat çekmektedir.

Anahtar Kelimeler: fonoskopi, deneysel fonetik, adli muayene, akustik analiz.

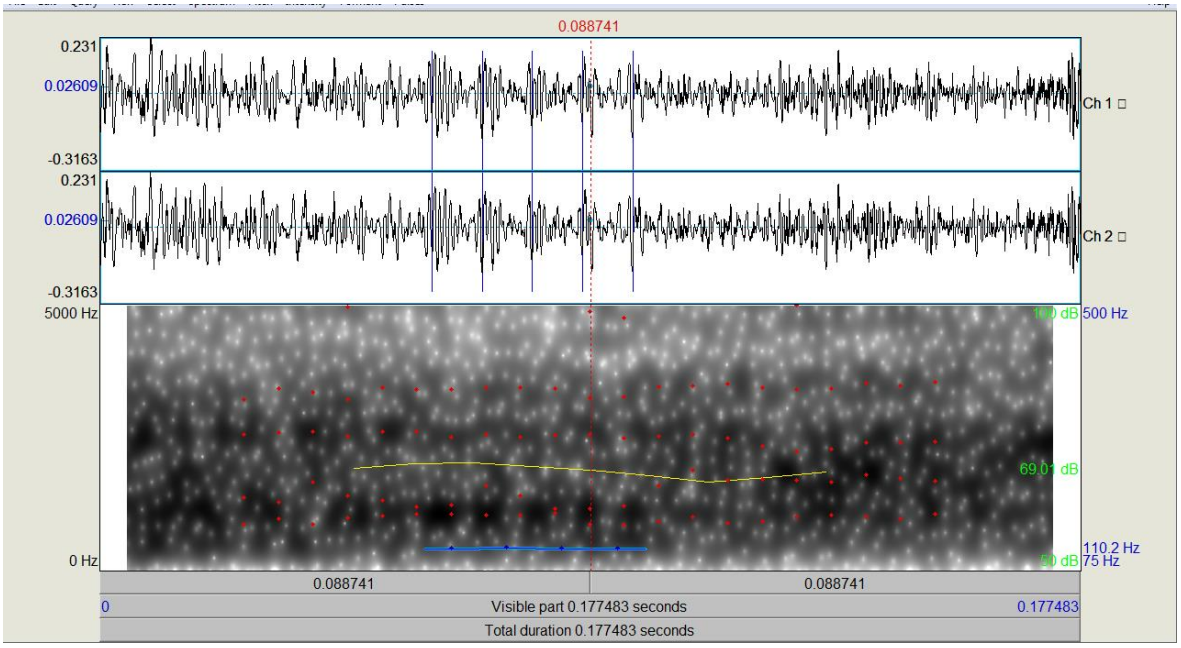
THE IMPORTANCE OF INDIVIDUAL SPEECH FEATURES DISCOVERED IN PHNOSCOPIC STUDIES

Abstract

In modern times, research in the field of speech technology is considered relevant because of its specific applications. Speech signal analysis, the development of this field with the application of modern technologies, stimulates the development of many applications such as speech synthesis, speech recognition, speech-based identification. Modern phonoscopic research allows not only the acoustic analysis and identification of the phonogram, but also the identification of age, gender, occupation by approaching it from many different perspectives. With this approach, research provides useful material for identifying different identity issues – factors related to social, national, occupational, gender and age characteristics.

During phonoscopic research, special "keys" are used to identify the person based on the speech signal. One of the key issues in these studies is the selection of the correct methodology for the detection of these "keys", taking into account the acoustic and articulatory properties of the voice. Among such “keys” that can provide valuable information for phonoscopic examination in forensic examination, we can mention some features related to the frequency of the main tone, morphemes, proportion of morphemes, density relative to vowels and intonation. Commonly used features in phonoscopic studies include signs associated with consonant sounds. Since both the oral and nasal cavities act as resonators during the pronunciation of nasal consonants, the individual geometric dimensions of the nasal cavity greatly reduce the morphology of the vowels developed along the m, n consonants. Also in identification a key is used as a "key".

Another remarkable feature of consonants is the observation of the tone in the consonant sound. The experiment showed that this trait is individual and manifests itself differently in the speech of different people.



It is clear that there are four periodic tones in the "X" sound. This situation draws attention as an individual feature.

Keywords: phonoscopy, experimental phonetics, forensic examination, acoustic analysis.

SUÇLU DAVRANIŞININ AÇIKLANMASINDA SUÇ VE ÇOCUK

HİLAL İFAKET AKBAŞ

Milli Savunma Üniversitesi ORCID: 0000-0002-9092-2169

ÖZET

On sekiz yaşından küçüklerin toplumsal norm ve değerlerden sapan davranışlar sergilemesi ve bu sapan davranışların yasalara göre suç sayılması çocuk suçluluğu olarak tanımlanmaktadır. Çocuk suçluluğu kaygı veren sosyal bir problemdir. Toplum da çocuk suçlu ve bireyin sayısının artması toplumu güven duygusunun azalmasına ve kaosa sürüklemektedir.

Dünyada yoksulluk, gelir dağılımı adaletsizliği, işsizlik, eğitimsizlik, göç ve düzensiz kentleşme gibi sorunlar sürmektedir. Bu sorunların süregelmesi çocukları suça iten ortamları hazırlamaktadır. Çocuklar çeşitli nedenlerle suça sürüklenmektedir. Ekonomik nedenler ve sosyal çevre bu nedenlerin başında gelmektedir. Çocuklar ise suçlu olarak doğmazlar. Suç öğrenilen bir davranıştır. Dolayısıyla çocuklar ancak içinde bulundukları sosyal çevrede suç davranışını öğrenerek suçlu çocuğa dönüşebilirler. Günümüzde ise çocukları korumak ve onların kişiliklerinin ve geleceklerinin zedelenmemesi için 'suça sürüklenen çocuk' kavramı kullanılmaktadır.

Bu çalışmada da suç öğrenilen bir davranış olduğu ve bireyin toplumla bağının zayıflamasının suç işleme olasılığını arttırdığı varsayımlarından hareket edildiği düşüncesi doğmaktadır. Literatür taraması yapılarak suçu açıklamaya yönelik olan biyolojik, psikolojik ve sosyolojik suç teorileri ışığında çocukları suç davranışına sürükleyen nedenleri bireysel ve çevresel çerçevesin de değerlendirerek suça sürüklenen çocuklar için bireysel ve toplumsal olarak neler yapılması gerektiğini veriler neticesinde açıklanacaktır.

Anahtar Kelimeler: Suça Sürüklenen Çocuklar, Suç ve Çevre, Suçla Öğrenilen Davranışlar, Suç.

1.GİRİŞ

Bireysel ve çevresel nedenler insanları suça sürüklenmesine etki etmekte, bireysel nedenlerin tek başına belirleyiciliği bulunmamaktadır. Çevresel nedenlerin başında aile gelmektedir, aile içerisin de yetişen çocuklar ise çevresinde yaşadığı olumsuzluklarla ileri de yaşadığı süreci oluşturmaktadır ve suçlu insanların mutlaka çocukluk döneminde yaşadığı travmaların etkisinde sosyalleşme sürecinin sekteye uğraması, bu sürecin okul, arkadaş grupları, çalışma yaşamı ve kitle iletişim araçlarının etkisiyle hatalı ve eksik bir şekilde devam etmesi çocukların suça yönelmesine neden olmaktadır. Suçu açıklamaya yönelik olarak biyolojik, psikolojik ve sosyolojik suç teorileri bulunmaktadır. Suç öğrenilen bir davranış olduğu ve bireyin toplumla bağının zayıflamasının suç işleme olasılığını arttırdığı varsayımlarından hareket edilmektedir.

Çocuk suçluluğu kavramı sosyolojik ve hukuki olarak ele alınmaktadır. Hukuki açıdan "çocuğun fiili olarak suç sayılan bir eylem işleyerek yargının karşına getirilmesi" şeklinde tanımlanırken, suçlu çocuk " bir hukuku ihlal etmiş on sekiz yaşından küçük kimseler" olarak tanımlanmaktadır. Yalnız hukuksal olarak bu tanım doğru olsa da sosyolojik açıdan yeterli değildir. Sosyolojik görüşe göre, çocuğun sağlıklı gelişimi desteklenmelidir. Çünkü bu gelişim

desteklenmezse, çocukta davranış bozukluğu ortaya çıkabilir. Davranış bozukluğu önemsenmeyen ve ilgisiz olan çocuklar ise suç işlemeye eğilimli olabilir, korunması gerekmektedir. Bu durumdaki çocuklara ise çocuk mahkemelerine göndermek yerine çeşitli sosyal kurumlar aracılıyla topluma kazandırılması hem toplum hem de kendileri için daha çok fayda sağlayacaktır(Akyüz 2000,s.657, Balo 2003,s.480).

Bireylerin suçluluğunu önleyebilmek ve suça sürüklenmiş çocukları yeniden topluma kazandırabilmek için çocuk suçluluğunun nedenlerinin anlaşılması büyük önem taşımaktadır. Bu çalışmada da sosyolojik açıdan suça sürüklenmiş çocukların suç teorileri ve literatür taraması çerçevesinde nedenlerini ve nasıl önlenebileceği yorumlanmaya çalışılmıştır.

2.ÇOCUK SUÇULUĞUN NEDENLERİ

Dünyada yoksulluk, gelir dağılımı adaletsizliği, işsizlik, eğitimsizlik, göç ve düzensiz kentleşme gibi sorunlar sürmektedir. Bu sorunların süregelmesi çocukları suça iten ortamları hazırlamaktadır. Çocuklar çeşitli nedenlerle suça sürüklenmektedir. Ekonomik nedenler ve sosyal çevre bu nedenlerin başında gelmektedir. Çocuklar suçlu olarak doğmazlar. Suç öğrenilen bir davranıştır. Dolayısıyla çocuklar ancak içinde bulundukları sosyal çevrede suç davranışını öğrenerek suçlu çocuğa dönüşebilirler. Çocukları suç davranışına sürükleyen nedenler bireysel ve çevresel nedenler olmak üzere ikiye ayrılmaktadır.

2.1.BİREYSEL NEDENLER

Çocuk suçluluğunu bireysel nedenlere dayandıran görüşler çocukların biyolojik ve psikolojik nedenlerden dolayı suç işlediklerini ortaya koymaktadır. Biyolojik görüşü savunanlara göre çocukların fizyolojik, genetik ve yapısal farklılıklara sahip olması onları suç işlemeye yatkın hale getirebilmektedir. Zeka geriliği, epilepsi, akıl hastalıkları, psikopatoloji ile suça yatkınlık arasında tutarlı ilişkinin olduğunu iddia edilmektedir (Karagöz ve Demircin 1996,s.s.47,54).

Tabiî ki çocukların yaşamış olduğu bu bireysel nedenler tek başına çocuğun suç işlemesinde yeterli değildir.

2.2.ÇEVRESEL NEDENLER

Çocuğun suç işlemesinde çevresel nedenler, bireysel nedenlerden önce gelmekte, suç ortamına zemin oluşturmaktadır. Çocuk suçluluğunda çevresel nedenlerden kastedilen, çocuğun ailesi ve aile dışı çevresinden (okul, arkadaş ortamı, çalışma yaşamı ve kitle iletişim araçları) kaynaklanan nedenlerdir.

Aile çocuğun ilk gözünü açtığında tanıştığı toplumsal kurum olan ailedir. Anne ve babanın çocuğuna yönelik ilgi ve sevgisinin yetersiz olması, çocuğunu korumadan yoksun bırakması, çocuğuyla sağlıklı iletişim kuramaması, aile üyelerinin birbirlerine karşı olumsuz tutum ve davranışları, aile içi şiddete başvurulması gibi olumsuz aile içi ilişkiler çocuğun suça yönelmesine sebebiyet verebilmektedir(İçli,2016,s.90). Aile içi disiplin tarzı da çocuğun sosyalleşme sürecinin işleyişinde ve çocuğun suçluluğunda önemli bir etkendir. Disiplin, "bireylerin içinde yaşadıkları topluluğun genel düşünce ve davranışlarına uymalarını sağlamak amacıyla alınan önlemlerin tümüdür"(Dönmezer,2009,s.180).

Araştırmalarda suçlu çocukların evlerinde aşağıdaki koşullardan birine veya birkaçına rastlanmaktadır (İçli,1993,s.31)

- Ailenin diğer üyelerinin suçlu veya alkolik olmaları,
- Boşanma, ölüm veya terk nedeniyle ebeveynlerinden biri veya her ikisinin de yokluğu, İhmal, körlük veya bunun gibi fiziksel bir özür veya hastalık nedeniyle ebeveyn kontrolünün eksikliği,
- Evin çok kalabalık olması, aşırı baskı, kıskançlık, ihmal veya ebeveynlerinden birinin aşırı hakimiyeti, işsizlik, yetersiz gelir gibi ekonomik baskılar ve annenin dışarıda çalışması gibi etkenler çocuğa karşı ilgisizliği ve sevgisizliği arttıran nedenlerdir.

Aynı zaman da çocuğun ailesin de suçlu bireylerin bulunması onların özelliklerini benimserler Çocuğun ailesindeki suçlu kişiyi kendisine rol model seçmesi çocuğun kişiliğine olumsuz yansıyabilmektedir. Öyle ki çocuk ailesindeki suçlu kişiyi örnek göstererek suç işlemeyi kendince haklı gösterecek gerekçeler üretebilir.

Ayırıcı Birliktelikler Kuramının sahibi olan Sutherland özellikle, çocuk suçluluğu-aile ilişkisini incelerken ailede başka suçlu kişilerin bulunması, yetersiz ebeveyn kontrolü, ihmal, parçalanmış aile, işsizlik, geçim sıkıntısı gibi aile özelliklerine önem vermektedir (İçli,1993,s.180).

2.3.OKUL ÇEVRESİ

Okul ve eğitim düzeyi okul, çocuğun sosyalleşmesi yönünde olması gerekli bir kurumdur, aynı zamanda ilk deneme yeridir. Okul sistemi çocuğa ileride içinde yer alacağı bürokratik toplumun bir benzer modelini sunar(Uluğtekin 1991,s.224).

Okulun amacı sadece çocuğa belli bazı bilgileri vermek değildir. Okul çocuğu bugünkü topluma uyum sağlamakla birlikte gelecekteki topluma hazırlamakla da yükümlüdür. Aynı zaman da okul bireye kazandırdıkları ise şöyledir;

- Okul toplumsal değer ve normların biçimlenmesine de katkıda bulunur.
- Akran gruplarıyla etkileşime fırsat tanıyan bir ortam oluşturur, çocuğun model almaya ve taklit etmeye yönleneceği kişilerle karşılaşmasına olanak sağlar,
- Okul eğer başarısız olursa çocuk üzerindeki önemini yitirir, hatalı ve eksik toplumsallaşmaya neden olur.

Böylecilikle okul işlevini herhangi bir sebeple yerine getiremediğinde, bireyin başarısı, gelişimi, çevresine uyumu ve ruh sağlığı olumsuz yönde etkilenmektedir. Okul başarısızlığı, çocuğun okulla ilgili diğer anti sosyal davranışlara yönelmesinde ve suça yönelmesinde önemli bir göstergedir. Bunun tam tersine başarılı bir okul hayatı geçiren ve eğitim düzeyini arttıran bireyin ise suç davranışında bulunma eğilimi azalmaktadır.

2.4.ARKADAŞ ÇEVRESİ

Çocuğun sosyalleşmesinde etkili olan diğer bir unsur akran grubudur. Çocuğun içinde bulunduğu akran çevresi (akran grubu) suçluluğa eğilimi ve risk faktörleri içeren grup özellikleri göstermesi, çocuğun da bu davranışlara itilmesine neden olabilmektedir. Araştırmalar ailenin etkisi azaldıkça akran grubunun çocuk üzerindeki anti sosyal nitelikli etkisinin daha çok belirginleştiğini göstermektedir.

Akers'in sosyal öğrenme teorisi çerçevesinde akran gruplarının sosyalleşme sürecinde önemli bir etkisi bulunmaktadır. Ancak Akers burada sapmış ve yanlış değer ve normların öğrenildiği ve aktarıldığı aksi sosyalleşmeden bahsetmektedir. Bu bağlamda çocuklar sapmış akranların

bulunduğu çevrelerde suç işlemeye motive olmakla birlikte sapmış değerleri ve suçu rasyonelleştirmeyi de öğrenmektedirler.
Sonuç olarak Ailesinin ve öğretmenlerinin denetimi dışında, kötü arkadaş seçiminde bulunan çocuklar güvensiz ve sevgisiz büyüyerek korunaksız ortamında kalarak, alkol, uyuşturucu madde gibi kötü alışkanlıklar edinebilmekte, suça sürüklenebilmektedirler.

2.5.KİTLE İLETİŞİM ARAÇLARI

Kitle iletişim araçlarının yaygın hale gelmesiyle erken yaşlardan itibaren çocuklar suçla ilgili görsel ve işitsel yayınlara maruz kalmaktadırlar. Televizyon, internet, gazete, dergi ve kitaplar kitle iletişim araçlarının başında gelmektedir. Özellikle televizyonda şiddet içerikli programlar/diziler çocukların hatalı sosyalleşmesine neden olabilmektedir. Yine Akers'in sosyal öğrenme teorisi çerçevesinde çocukların televizyonda ve internette gördüklerini taklit ederek suç davranışına yönelebildiği söylenebilir. Gazete ve dergilerin de suçluluğu yaygınlaştırmada önemli rolleri bulunmaktadır. Örneğin Suç tekniğini öğretmek; suçu olağan, çekici, hatta heyecanlı, yararlı bir faaliyet olarak göstermektedir. Suçluya saygın bir kişilik vermek; suçluyu cana yakın, sempatik bir kişi olarak sunmak; adaletten kurtulmanın kolay olduğunu telkin etmek; adalet mekanizmasını ve polisi gülünç şekillerde göstermek; suçun adeta reklamını yapmak ve ücret aracı haline getirmek vb.(Yavuzer,1994,s.243).

2.2. SUÇ VE SOSYOLOJİK TEORİLER

Suçun nedenleri ve suçu önlemede muhtemel çareler hakkında akıl yürütmeler eskilere dayanır. Modern kriminoloji geçmişin bilgi birikimi üzerine inşa edilmiştir(İçli,2016,s.66).
Suça bilimsel yaklaşımı ilk defa 18. yüzyıl ortalarında "Faydacı Ekol" ile adlandırılan klasik ekolle olmuştur. Klasik ekol lideri olarak bilinen Beccaria'dir. Klasik ekol insanların kendi faaliyetlerinin sonuçlarını tarttıktan sonra suç işledikleri varsayımına dayanır yani bireyin yalnızca kendi rızası ile topluma bağlanmasını ve toplumu bireyden sorumlu tutmak gibi bireyi de toplumdan sorumlu kılmayı içerir. Klasik ekollün diğer bir temsilcisi olan Bentham'dır ve suçu sadece soyut olarak düşünmüştür. Beccaria gibi özgür iradeye inanır.18. yüzyılın bütün yazarları insan haklarıyla ilgilenmiştir. Klasik ekol için özellikle Montesquieu ve Voltaire'nin etkileri olmuştur.
Neo klasik dönem de cezanın suç uygun olması hakkında klasik prensip 19. yüzyıl sonu ile 20. yüzyılın başlarında evrensel olarak kabul edilmiştir. Buna rağmen klasik ekolün zayıflıkları ortaya çıkmıştır. Bunun üzerine 19. yüzyılın ortaların da bilim adamları suç nedenlerini pozitivist bir yaklaşımla incelemiş ve suçlu davranışlarının biyolojik, psikolojik,ve sosyal faktörlerinin bir sonucu olarak ortaya çıktığını savunmuşlardır.
Biyolojinin insan davranışlarında belirgin rol oynadığı fikri, Rafaelle Garofalo ile birlikte pozitif ekolü kuran Cesare Lombroso'nun yazıların da kendini gösterir. Lomboroso, suçlu davranışın açıklamasını, bilimsel metodun uygulanmasında gördüğü için kriminolojinin pozitif ekolünün kurucusu olarak adlandırılmıştır(İçli,2016,s.72).
Lomboros'nun teorisine göre, suç eğitimi özellikleri, akıl hastalığı, sağırlık, frengi, epilepsi ve alkolizmin sık sık görüldüğü yozlaşmış ailelerden kalıtım yoluyla geçebilir. Kalıtıma ek olarak alkolizm, eğitimsizlik, sinirlilik ile basın-yayın organları tarafından çok detaylı suç olaylarının taklit gibi nedenler suçluluğu teşvik edebilir(İçli,2016,s.72).
Lomboros aynı zamanda kalıtımsal biyolojik faktörlerin, suçun temel nedeni olduğunu kabul etse de çevrenin de anti sosyal davranışı etkileyeceğini dikkatte almıştır.

Pozitif ekolün diğer bir önde gelen ismi Enrico Ferri'dir.25 yaşında profesör olan Ferri ise biyolojik olarak Lomboros'a katılsa da kişilerin suç işlemeyi seçmezler, yaşam koşulları nedeniyle suça itildiğini savunarak bu noktada ayrı düşünmüştür. Yine pozitif ekollün için de yer alan ilk "sosyal kriminolog" olarak bilinen Outelet ise coğrafi faktörlerin insan davranışları üzerindeki etkilerini incelemiştir.

19. ve 20. yüzyıl başlarında araştırmacılar insan zihninden çok insan vücuduyla ilgilenmişler ve suçun psikolojik açıklaması ile ilgili bazı katkılar getirmişlerdir. Bu dönem de bazı psikologlar, anti sosyal davranışa psikoanalitik perspektifinden bakarlar ve onların odak noktaları ilk çocukluk deneyimlerinin kişilik üzerindeki etkileridir. Davranışçılar, sosyal öğrenme ve davranışın etkilenmesinin suçlulukta anahtar olduğuna inanırlar(İçli,2016,s.79).

Psikanalist David Abrahamsen, suçluyu id'in yönettiği, güdüleri kontrol etmekten aciz, zevk verici dürtüleri arayan kişi olarak görür. Bu kişiler genelde ailelerinde yeterince ilgi ve şefkat görmemiş, çocukluklarında mutsuz deneyimler yaşamış kişilerdir(İçli,2016,s.81).

Yine psikanalistler, evrensel bir tanım yapmalarına karşılık suç türlerini açıklamakta zorlukla karşılaşmışlardır. Akıl hastalıklarının suçla ilgisini belirterek psikoz, nevroz, organik beyin hastalığı, sara, alkolizm ve uyuşturucu maddenin suça etki eden faktörler olduğunu ileri sürmüşlerdi ki suçun çevreyle ilişkisini yine söz konusu olduğu anlaşılmaktadır.

Araştırmalar da psikobiyolojik ekolün içersinde görülüyor ki bireylerin IQ ve suç ilişkisinin önemini yeniden Travi, Hirschi ve Michael hindelang'ın yaptığı çalışmalar da önemini canlanmıştır. Düşük IQ'deki bireylerin okul performansının etkisiyle suçlu davranış olasılığının arttırdığını kabul etmişlerdir. Yani düşük IQ'ye sahip çocukların okul başarılarının düşüklüğü, çocuk ve daha sonrada yetişkin suçluluğu ile ilişkilidir(İçli,2016,s.91).

Bireysel teoriler de suçun kalıtımla geçmediğini tartışılmış, Onlara göre, davranış öğrenilir ve çevre tarafından şekillenir.

Çocuk ve yetişkin suçluluğunda suçun nedenleri ile ilgili en sistematik açıklamalar sosyolojik teorilerle getirilmiştir. Suç nedenleri ile ilgili temel teoriler, sosyal normlar, sosyal organizasyonlar, sosyal yapı, sosyal değişme, sosyal süreçler ve sosyal çatışma ile sapmış davranışın ilişkisine yoğunlaşmıştır(İçli,2016,s.96).

Siegel (1989) tarafından yapılan sosyal yapı, sosyal süreç ve çatışma teorileri şeklindeki üç gruplu sınıflandırma temel alınmaktadır. Sosyal yapı teorileri kendi içinde dört alt gruba ayrılmaktadır. Bunlar; fonksiyonalist teoriler, gerilim teorileri, alt kültürel teoriler ve sosyal ekoloji teorileridir. Sosyal süreç teorileri içinde sosyal öğrenme ve davranış teorileri, kontrol teorileri ve etiketleme teorisi yer almaktadır(İçli,2016,s.s.96,97).

Durkheim'ın suçun yapısal-fonksiyonel sınırlanması teorisi, ilk sosyolojik suç teorisi olarak kabul edilmektedir(Demirbaş,2016,s.140). Durkheim'a göre suç evrenseldir; bütün toplumlarda görülür. Suç 'normal' bir olgudur. Toplumun heterojen bir yapıda olmasından dolayı bazı bireylerin toplumun ortak değer ve normlarından sapma göstermesi ve suç davranışında bulunması kaçınılmaz olmaktadır. İnsanların sapan ve suç teşkil eden davranışlarına ceza uygulanmaktadır. Durkheim, cezalandırmanın işlevinin suçu ortadan kaldırmak olmadığını, ortak duyguların güçlenmesi için gerekli olduğunu düşünmektedir. Bu nedenle suç işlevseldir. Suç bazen yararlı da olabilir. Suç oranlarının yükselmesi toplumun sosyal değişmeye ihtiyacı olduğunu göstermektedir(İçli,2016,s.96).

Merton' un geliştirdiği gerilim teorisinde Durkheim' dan ödünç aldığı anomi kavramı kilit rol oynamaktadır. Durkheim'ın anomi kavramı bir tür kuralsızlık ve normsuzluk durumuna işaret

etmektedir. Merton'a göre anomi, "kültürel amaçlar ve bu amaçlara ulaşmayı sağlayacak kurumsal araçlar arasındaki bir kopukluğun sonucudur" (İçli,2016,s.98).

Suçun nedenlerini alt kültür ile ilişkilendiren teoriler, Durkheim ve Merton'un anomi teorisinden etkilenmekte; çocuk suçluluğunu açıklarken, suçun özellikle alt sınıfa mensup erkek çocuklar arasında yaygın olduğunu ve çetelere katılımla kendini gösterdiğini vurgulamaktadır. Alt kültürel teorilerin öncüleri arasında yer alan Cohen, kişileri suç işlemeye yönelten gerilimin kaynağının kültürel amaçlara ulaşamamak kadar, orta sınıf statüsünden de yoksun kalmalarından kaynaklandığını ortaya koymaktadır. Alt sınıfa mensup çocuklar orta sınıf değerlerine göre yetişmiş olmalarına rağmen, bu sistem içinde başarılı olamazlar. Bu nedenle orta sınıfa düşman olurlar. Elde edemedikleri statüye suç işleyerek ulaşmaya çalışırlar(Demirbaş,2016,s.143).

Suç ekolojisi yaklaşımı, insanların suçluluğuna içinde yaşadıkları sosyal ortam ve koşulların neden olduğunu öne süren yapısal bir yaklaşımdır. Bu yaklaşımın öncülerinden olan Park ve Burgess yoğun göç alan Şikago kentinde yaptıkları araştırmada, kentin fabrikalarda çalışan göçmenlerin ve yoksul işçilerinin yaşadığı, nüfus hareketliliğinin hızlı yaşandığı, sosyo-ekonomik düzeyi düşük olan bölgesinde suç oranlarının yüksek olduğunu tespit etmişlerdir. Yani etnik heterojenlik, yoksulluk, nüfus hareketliliği, işsizlik ve sağlıksız etkileşimin birlikteliğinin bölgenin temel sorunu olan sosyal düzensizliği açıkladığını ve bireyleri suça iten en önemli unsurlar olduğunu saptamışlardır.

Etiketleme teorisyenlerine göre suçluluk, suçlular ile suçlu olmayanların karşılıklı sosyal etkileşiminin bir ürünüdür. Onlar, sosyal etkileşimde bulunulan öğretmen, polis, komşu, ebeveyn, arkadaş gibi insanların bireye suçlu etiketini yapıştırdıkları için bireyin suçlu olduğunu öne sürmektedirler. Etiketlenen insanlar yapmış olduğu suçtan dolay cezasını çekmesine ve bir daha o davranışı göstermemesine rağmen toplum tarafından fişlenmiş olmuştur ve bu toplumu olumsuz etkilemektedir. Sosyal çatışma anlayışında, sapma ile sosyal eşitsizliğin ekonomik alt yapı doğrultusunda ilişkilendirilmesi söz konusu olmaktadır. Toplumda norm ve değerler ile yasalar güçlüler tarafından belirlenmektedir. Güçsüzler ise sapkın olma riskiyle karşı karşıyadır. Dolayısıyla sapmanın kaynağı sosyal eşitsizliktir.

Çocuk suçluluğunun diğer bir teorisi sosyal kontrol teorisi olan sosyal bağ sosyal kontrol teorisini geliştiren Hirschi, teorisini Durkheim'ın ifadelerinden hareketle formüle etmektedir. Durkheim'a göre, kişinin ait olduğu grup zayıfladıkça birey giderek daha az bağımlı olur ve sadece kendine bağımlı hale geldiğinde başka kural tanımaz(İçli,2016,s.138).

Sağlıklı bir sosyalleşme süreci yaşayamayan çocukların toplumla bağı zayıflar ve onlar topluma karşı sorumsuz davranışlar sergilemeye başlarlar. Toplumsal norm ve değerlerden sapma gösteren bu çocuklar için toplumda kontrol mekanizması etkin bir şekilde işlemezse onların suç işlemesinin önüne geçilemez.

Hirschi gençlerin güçlü bir şekilde ebeveynlerine, akranlarına ve okula bağlandığında, eylemin geleneksel çizgilerine kendilerini adadığında, geleneksel aktivitelere katıldığında ve toplumun ahlak kurallarının geçerliliğine inandığında suç işleme ihtimallerinin daha az olacağını öne sürmektedir.

Sosyal öğrenme teorisi, sosyal süreç teorileri arasında yer alan bir diğer teoridir. Sturheland ve Aker's öne çıkan isimlerdir. Sutherland'e göre, suçlu davranış öğrenme sürecinin bir ürünüdür. Sutherland, suçlu davranışın karşılıklı iletişim içinde ve bireye yakın gruplar içinde öğrenildiğini belirtmektedir. Birey, karşılıklı iletişimde suçun nasıl işleneceğine ilişkin

teknikleri ve suç işlemesini haklı çıkaracak tanımlamaları öğrenir. Birey, suç işlemeyi uygun gören tanımlamalara, suç işlemeyi uygun görmeyen tanımlamalardan daha fazla maruz kalırsa suç işler. Sutherland, suçlu davranışın çocuklukta öğrenildiğini, suça uygun ortam meydana geldiğinde, bireyin suçlu davranış kalıplarıyla ve suçlu gruplarla görüşme sıklığı ve yoğunluğuna bağlı olarak ortaya çıktığını belirtmektedir(İçli,2016,s.129).

Akers, Sutherland'in Ayırıcı Birliktelikler Teorisinden hareketle kendi sosyal öğrenme teorisini geliştirmiştir. Akers'in kuramı ayırıcı birliktelikler, tanımlamalar, ayırıcı pekiştirme ve taklit olmak üzere dört bileşene dayanmaktadır. Bunlar ise;

Ayırıcı birliktelikler, birinci referans grubu olarak yakın ilişki içinde bulunulan insanlarla etkileşimler ile ikinci referans grubu olan otorite figürlerinden okul, öğretmen vb. gruplarla olan etkileşimlerden oluşur.

Tanımlamalar, kişinin davranışlarının nedenini açıklayan ve neyin doğru neyin yanlış olduğuna dair gerekçelendirmeler, ahlaki değerler ve eğilimlerdir.

Ayırıcı pekiştirme, bir davranış sonucunda alınan şeyin ödül ve ceza oluşuna göre, o davranışın tekrarlanıp tekrarlanmayacağıdır.

Taklit ise, suçun diğer kişilerden veya TV-internet gibi iletişim araçlarından gözlem yoluyla öğrenilmesidir(İçli,2016,s.134).

Sosyal çatışma teorilerine göre de suçun tanımı güç, servet ve yüksek statüye sahip olanlar tarafından kontrol edilmektedir. Suç,tüm insanların ihtiyaçların yansıtan objektif ahlaki fikir birliği tarafından değil yöneten sınıfın değerleri yoluyla şekillendirilmiştir(İçli,2016,s.149).

Bu araştırmalar da incelendiği üzere bireyin suç işlemesinin altında birçok etken vardır.

3.SONUÇ

Suç araştırmaları 18. yüzyıldan başlamış günümüze süregelen önemli bir sosyal problemdir. Tarihin her döneminde suçla mücadele edilmiştir. Suç işlemenin belli bir yaşı olmadığı, çocuk yaşlardan yetişkinliğe kadar her yaş grubunda suça karışan bireyler olduğu sosyal bir gerçekliktir. Toplum da işlenen suçlara bakıldığında bireylerin çocukluk dönemlerinde yaşamış oldukları deneyimlerle olduğunu ve çocukların kendileri isteyerek değil, çeşitli nedenlerle suça sürüklendiğini görüyoruz.

Çocuk suçluların özelliklerine bakıldığında onları suça sürükleyen öncelikli nedenlerin aile başta olmak üzere sosyal çevre ve ekonomik nedenler olduğu görülmektedir.

Bu çocukların aile ve arkadaş çevrelerinde suçlu bireylerin olması Sutherland'in Ayırıcı Birliktelikler Kuramında öne sürdüğü gibi suçun öğrenilen bir davranış olduğunu Göstermektedir. Ayrıca Çocuk suçluların tekrar suç işlemesinin önüne geçebilmek için çocuklara, Akers'in ayırıcı pekiştirme olarak belirttiği, suç davranışının karşılığında ceza alacaklarının bilincinin verilmesi gerekmektedir.

Çocuk suçluların aileleriyle ilişkilerine bakıldığında ise ailelerin çocuklarına karşı yeterli ilgiyi göstermediği, aile içi iletişimin sağlıklı olmadığı, ailenin çocuğa karşı ya aşırı baskıcı ya aşırı hoşgörülü ya da umursamaz bir şekilde tutarsız disiplin uyguladığı görülmektedir. Hirschi'nin kuramıyla örtüşen bir durum söz konusu olmaktadır. Çocuklarla aileleri arasında sevgi ve güven ortamının olmaması çocuğun aileye karşı olan sorumluluk duygusunu yok eder, çocuk suç davranışında bulunmaktan kaçınmaz.

Çocuk suçluluğunda eğitim değişkeninin son derece önemli olduğu görülmektedir.

Çocuk suçluların düşük eğitim düzeyine sahip olması ve okul başarısızlıkları onların suçlu

bireye dönüşmesinde etkili olmaktadır. Hirschi'nin Sosyal Bağ Teorisine göre kendilerini ideal ve kariyerlerine adayan bireyler daha az suç işlerler. Dolayısıyla çocukların eğitim düzeyleri yükseltilmeli ve kariyer sahibi olabilecekleri mesleklere yönlendirilmeleri gerekmektedir. Böylelikle onların gelecekten umutlu olmaları ve suç davranışından uzak durmaları sağlanabilir.

Mason ve Wilson'un (1988) belirttiği gibi, boş zaman etkinlikleri çocukların suça sürüklenmesini engelleyebilmektedir. Bu sayede çocukların toplumla bağı güçlenir ve suç davranışında bulunmalarının önüne geçilebilir.

Akers'in Sosyal Öğrenme Teorisine de olduğu gibi, bireyin aynı şekil de T.v. ve günümüz de çocukların büyük bir bölümünün interneti kontrolsüz kullanmaları ve şiddet içerikli oyunlar oynayarak vakitlerini geçirmesi taklit ederek öğrenen çocuğun hayatına uygulaması ise kaçınılmaz oluyor.

Suça sürüklenmiş çocukların tekrar suça yönelmesi istenmiyorsa onlara suçlu etiketini yapıştırarak dışlayıcı tutum sergilenmemeli onları yeniden topluma kazandırmaya çalışmak gerekmektedir. Bu çocukların eğitimlerini sürdürmeleri ve meslek sahibi yapılması büyük önem taşımaktadır.

Böylece suçun nedenlerini açıklamaya yönelik sosyolojik teoriler, kimi zaman suçun nedenlerini biyolojik, kimi zaman sosyal yapıda aramakta, suç davranışını sosyal sınıf, sosyal ve fiziki çevre, alt kültür değişkenlerini kullanarak açıklamaya çalışmaktadır. Kimi zaman da suçun sosyal etkileşimin bir ürünü ve öğrenilen bir davranış olduğunu belirtmekte, suç davranışını bireyin toplumla olan bağıyla ilişkilendirmekte ya da suçun nedenini bireye suçlu etiketi taşımaktadır.

Anlaşıldığı üzere bireyi suça sürükleyen birçok etken mevcuttur ancak birey için birincil grup ilişki içinde olan aile çok çok önemlidir. Toplumun en küçük yapı taşı olan aile ve onun yetiştirdiği çocuk ailenin anlayışı çocuğa göstereceği sevgi ve ilgisini hiç üzerinden eksik etmemesiyle suça sürüklenmez. Hiç bir çocuk suçlu doğmadığı gibi hiçbir çocuk, birey suç işlemek istemez. Toplum olarak sadece kendi çocuğumuza değil geleceğimizi oluşturan tüm çocuklara sahip çıkmalıyız.

KAYNAKÇA

Akyüz, E. 2000. Ulusal ve uluslararası hukukta çocuğun haklarının ve güvenliğinin korunması. Milli Eğitim Yayınevi, Ankara.

Akduman, G.G., Suça Karışan 12-15 Yaş Grubundaki Çocuklarda Akran İstismarı Ve Kendilik Algısının Karşılaştırmalı Olarak İncelenmesi, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi.

Bağış R. C., Çocukları Suça Sürükleyen Çevresel Nedenler Sosyal Bağ ve Sosyal Öğrenme Teorileri Işığında Bir Değerlendirme, Humanitas, 2019; 7 (14): 203-221 e-ISSN: 2645-8837

Balo, Y.S. 2003. Çocuk Ceza Hukuku. İlksan Matbaası, Ankara.

Dönmezer, İ. Ana-Baba Tutumlarının Aile İçi Demokrasi ve Çocuğa Yönelik Şiddetle İlişkisi, Hegem Yayınları, Ankara,2009.

Demirbaş, T., Kriminoloji (6. baskı), Ankara, Seçkin Yayıncılık, 2016

Karagöz,Y.M. ve Demircin S.1996. Antalya'da çocuk suçluluğu. Akdeniz Üniversitesi Tıp Fakültesi Dergisi, 13(1), 47-54

Ereş F., Toplumsal Bir Sorun: Suçlu Çocuklar ve Ailenin Önemi, Aile ve Toplum Yıl: 11 Cilt: 5 Sayı: 17 Nisan-Mayıs-Haziran 2009 ISSN: 1303-0256.

İçli, T.G, Kriminoloji, Seçkin Yayınları, Ankara 2016.

İçli, T.G., Türkiye'de Suçlar, Atatürk Kültür, Dil Ve Tarih Yüksek Kurumu, Atatürk kültür Merkezi Yayını, Ankara 1993.

Uluğtekin, S. 1991. Hükümlü çocuk ve yeniden toplumsallaşma. Bizim Büro Yayınevi, Ankara.

Yavuzer, H.,Çocuk ve Suç, Ankara: Remzi Kitabevi. 1993

ULUSLARARASI DÜZEYDE SİBER UZAYIN GÜVENLİĞE TÜRKİYE'YE PERSPEKTİFİNDE ETKİSİ

Hilal İfaket AKBAŞ[1]

Öz

İnsanlığın varoluşundan beri süregelen güvenlik kavramı Soğuk savaş sonrası bilim ve teknolojideki gelişmelerle güvenlik teriminin ivme kazanmasına neden olmuştur. Soğuk Savaş dönemindeki savaşan tarafların netliği, tehditlerin açık oluşu ve uygun karşılığın alınma ihtimali günümüzde teknolojinin gelişimiyle tüm dünyadaki güvenlik kavramında bir dizi değişimleri zorunlu hale getirmiştir. Özellikle savaş teknolojisindeki değişim, gelişim ve istihbarat yapısına ilişkin genel değişiminler siber güvenlik kavramına dair yaklaşım ve Uluslararası ilişkiler konusunda bir takım değişimleri hızlandırmıştır. Siber güvenlik alanındaki bu değişmelerin en önemlisi ise artık düşmanın belirsiz oluşu, saldırıların her yerden gelebilmesi, tehditlerin ve saldırıların sınırlarının olmayışı bireyleri, kurumları ve neticesinde Ülkeleri siber güvenlik alanında farkındalığını arttırmasına sebep olmuştur. Siber güvenlik alanın da yaşanan gelişmeler Ulus ve Uluslararası arenalar da bir takım güvenlik tedbirleri alınmasına neden olmuştur. Bu çalışmada ise siber uzay, siber tehdit ve siber güvenlik gibi kavramlar, siber saldırı çeşitleri, Türkiye'nin siber güvenlik tedbirleri ile ilgili genel literatür taraması yapılarak siber saldırılara karşı nasıl önlemler alması gerektirdiği yorumlanmaya çalışılmıştır.

Anahtar Kelimeler: Güvenlik Kavramı, Siber Güvenlik, Siber Uzay, Siber Tehdit, Siber Saldırı Çeşitleri, Türkiye'nin Siber Tedbirleri.

Abstract

The concept of security, which has been going on since the existence of humanity, has caused the term security to gain momentum with the developments in science and technology after the Cold War. The clarity of the warring parties in the Cold War period, the openness of the threats and the possibility of receiving the appropriate response have made a series of changes in the concept of security all over the world mandatory with the development of technology today. Especially the change in war technology, development and general changes in the intelligence

[1] MSÜ Atatürk Araştırma Enstitüsü Askeri Eğitim Yönetimi Yüksek Lisans Öğrencisi; JSGA, Güvenlik Bilimleri Enstitüsü Suç Araştırmaları Özel Öğrencisi; İzmir Tersanesi K.lığı IT Uzmanı; hilal.akbas@msb.gov.tr; ORCID: 0000-0002-9092-2169

structure have accelerated some changes in the approach to the concept of cyber security and international relations. The most important of these changes in the field of cyber security is that the enemy is now uncertain, attacks can come from anywhere, threats and attacks have no borders, and this has caused individuals, institutions and, as a result, countries to increase their awareness in the field of cyber security. The developments in the field of cyber security have caused some security measures to be taken in the national and international arenas. In this study, concepts such as cyber space, cyber threat and cyber security, types of cyber attacks, general literature on Turkey's cyber security measures have been searched and it has been tried to interpret how measures should be taken against cyber attacks.

Keywords: The Concept of Security, Cyber Security, Cyber Space, Types of Cyber Attacks, Turkey's Cyber Measures.

GİRİŞ

Dijitalleşen dünyanın büyümesi ile kamu ya da özel sektör elektronik işlem hacmini her geçen gün artırtırmıştır. Nitekim İnternet kullanan kişi sayısının Uluslararası Telekomünikasyon Birliği(ITU) verilerine göre 4,1 milyar insanın olduğunu bunun da yaklaşık dünya nüfusunun %53,6'sını oluşturduğunu düşünülmektedir. Ülkemizin geniş bant abone sayısına bakıldığında ise Bilgi Teknolojileri ve iletişim Kurumu (BTK) ve Türkiye Elektronik Haberleşme Sektörü 2020 ve 2008 yıllarını kıyasladığında abone sayısı 2020 yılı ikinci çeyreğinde 78,4 milyona ulaşmıştır. Veriler kıyaslandığında ve Türkiye İstatistik Kurumu (TÜİK) verilerine bakıldığında ise 16-74 yaş aralığındaki kişilerin internet kulanım oranı ise %79 ulaştığı görülmektedir(Ulusal Stratejik Eylem Planı, 2020,s.11).

Bu veriler neticesinde dijitalleşen toplum ve ülkeler siber uzayın gelişmesiyle siber tehditlere ve siber saldırılara maruz kalmaktadır. Teknolojinin gelişmesinin tamamına siber uzay olarak nitelendirilir. Siber uzayda yaşanan suçların faillerinin kolayca bulunamaması ve tespitin zorluğu teknolojik gelişmelerinin olumsuz tarafı olarak siber ortamı kötü niyetli kişilerin hedefi haline getirmektedir. Ayrıca siber uzayda yaşanan suçların eyleminin belirsizliğinden ziyade siber silahların konvansiyonel silahlara göre daha ucuz olması ve sonucunun yıkıcı etkilerinden dolayı siber saldırı, siber tehdit ve siber terör gibi siber suç işleyen kişilerin iştahını kabartmaktadır.

Nitekim oluşan siber tehdit ve siber saldırılar sonucunda siber güvenlik ve savunma faaliyetlerin önemi artmıştır. Bu bağlamda siber uzayda yaşanan kötü amaçlı saldırılar sadece bireylerin değil kurum, kuruluş ve uluslararası arena da birçok devletin siber güvenlik farkındalığını arttırmıştır.

Geleneksel güvenlik anlayışından uzaklaşmak zorunda kalan kurumlar ve devletler, kendi kritik altyapı sektörleri ile bilgi, iletişim veri ve teknolojilerinin bu tehditlere karşı koruyabilmek için siber güvenlik ve savunma konusunda faaliyetlerini

hızlandırmış ve hukuki tedbirlerin geliştirilmesi zorunda kalınmıştır. Ulus devletlerin ve ülkemizin teknoloji, bilgi ve iletişime olan bağımlılığı devam ettikçe siber güvenlik, öncelikli güvenlik alanı olacak ve siber güvenlik tedbiri almayan taraflar da bertaraf olmak zorunda kalacaklardır.

Kamu yada özel Kurumların ve devletlerin kendi kritik alt yapı sektörlerinin korunması için geleneksel güvenlik anlayışından uzaklaşmak zorunda kalan

Bu çalışma da literatür taraması yapılarak üç bölümden oluşmaktadır. İlk bölüm de temel kavramlar ele alınarak siber uzay, siber güvenlik, siber saldırı, siber tehdit ve siber terör kavramları incelenerek uluslararası düzeyde yeri ve önemine değinecektir. İkinci bölümde siber uzay da yaşanan siber saldırı türleri olarak kullanılan kötücül yazılımlar ile ilgili genel bilgiler verilerek, bu saldırı ve tehditlere karşı alına bilenecek önlemlerle ile uluslararası arena da önemli yer işgal etmiş siber saldırı örneklerine değinilecektir. Üçüncü bölümde ise Türkiye'nin siber güvenlik durumu ve politikaları hakkından bilgi verilerek, siber güvenlik ve siber saldırılara karşı siber güvenlik farkındalığının oluşması amaçlanmıştır.

BİRİNCİ BÖLÜM

1.Siber Güvenlik İle İlgili Temel Kavramlar

İnsanoğlunun var olduğu günden bugüne güvenlik kavramı her zaman önemli olmuştur. Türk Dil Kuruma(TDK)'a göre "toplum yaşamından yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" olarak tanımlanmıştır (https://sozluk.gov.tr/). Aynı zamanda güvenlik terimi ünlü ABD'li psikolog Abraham Maslow 'un ihtiyaç teorisi ile de açıklana bilinir. Maslow 'un ihtiyaçlar hiyerarşinin temellini temel fizyolojik ihtiyaçlar olan yeme, içme ve uyuma gibi temel ihtiyaçlarından sonra güvenlik ihtiyacı yer gelmektedir(Jerome, 2013, s.s.39,45). İnsanın kendini gerçekleştirebilmesi, ait olma, saygınlık

ve sevgi gibi ihtiyaçların karşılanması ve yaşamını daha huzurlu sürdürebilmesi adına öncelikli insanoğlu için güvenlik ve fizyolojik gibi temel ihtiyaçların karşılanması gerekmektedir.

Şekil-1- İhtiyaç Hiyerarşisi

Güvenlik insanoğlunun yaşamını sürdürmek için önemli olduğundan, geleneksel güvenlik anlayışı kapsamında ordu, polis teşkilatı gibi silahlı unsurların kurulması sağlanmıştır. Ancak içinde bulunduğumuz bilişim çağın da yaşanan ekonomik, kültürel, politik ve sosyal değişimlerle yaşanan hızlı değişimlerle geleneksel güvenlik anlayışı yetersiz kalmıştır.

Gelişen ve hızlı değişen bilgi ve iletişim teknolojilerin 2000'li yıllarda tüm dünya da yayılmasıyla kritik altyapı sektörlerinin uygulamalarını sayısal ortam denilen siber uzaya aktarılmasıyla insanların bilgi, iletişim ve teknolojiye daha bağımlı hale gelmiştir. Nitekim teknolojideki bu bağlamlılık kötü amaçlı grup, kişi ya da örgütler tarafından kullanılması sonucu ise masum kişi, kuruluş, kurum hatta devletler birçok zarara uğratılmış bulunmaktadır.

Teknoloji, iletişim ve dijitalleşen toplum ile geleneksel güvenlik anlayışındaki yaşanan ve zorunlu hale gelen değişimler sayesinde siber güvenlik kavramı güç kazanmıştır. Siber güvenlik kavramı genel hatlarıyla siber alanda bilginin mahremiyetinin, bütünlüğünün ve ulaşa bilirliğinin korunması şeklinde tanımlanmaktadır(Güvenlik Terimleri Sözlüğü,2017,s.621).

Güvenlik ve siber güvenlik arasındaki değişimlerin en önemlisi artık düşmanın belirsiz oluşu, saldırıların her yerden gelebilmesi, tehdit ve saldırıların sınırlarının olmayışı bireyleri, kurum ve ülkelerin siber güvenlik alanındaki farkındalığının artmasına sebep olduğunu düşünülmektedir.

Siber güvenliğin temel prensipleri olarak sistemlerin sürekliliği ve devamlılığı için mahremiyetinin korunması, erişim hızı, bilginin gizliliği, bilgiye erişimi ve kalitesinin korunması için bilgi sistemlerinde işlenen, transfer edilen ve depolanan veriler bilgi sistemler için de temel prensip oluşturmaktadır(Sağıroğlu,2011; Atalay,2012 s.43). Aynı zaman da siber güvenlik için gizlilik (Confidentially), erişebilirlik (Integrity) ve bütünlük (Availability) kavramları "CIA üçlüsü" olarak da bilinmektedir(Singer ve Friedman,2015, s.57).

CIA Üçlüsü

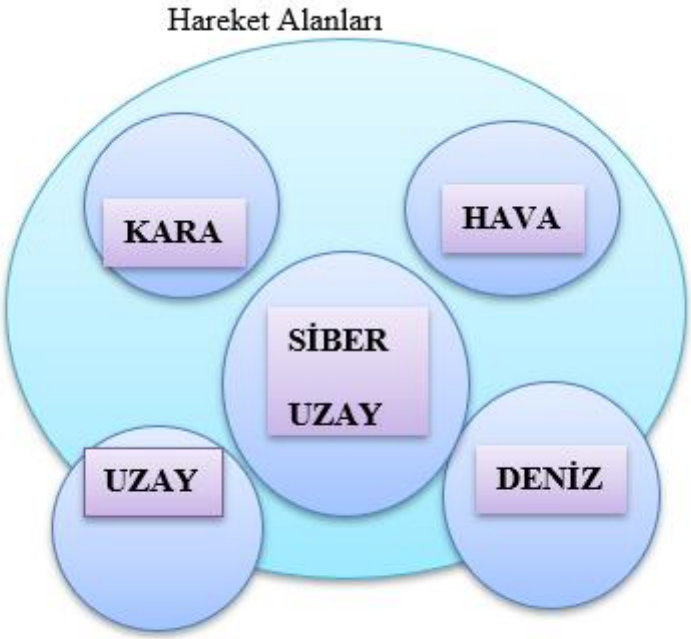
Şekil-2 – CIA

Şekil-2 den anlaşıldığı üzere siber güvenlik için temel prensip olarak yer alan gizlilik kavramı verinin sadece alıcı ile gönderici tarafından muhafaza edilmesini ifade etmektedir. Erişe bilirlik kavramı veriye kesintisiz bir şekilde erişmenin ve bu süreçte hız ve kalitesinin kayıplarını engellemeyi ifade eder. Bütünlük kavramı ise, kaynak ya da verinin sistem içerisinde izinsiz bir biçimde önlenmesi, bütünlüğünün sağlanması ve değiştirilmesidir. Bu bağlam da siber güvenlik, siber uzay da yaşanabilecek her türlü her türlü siber tehditti ve siber saldırılarla mücadelenin yani sıra her türlü güvenlik riskini en aza indirmeyi hedeflemektedir.

1.1.Siber Uzay (Siber Alan, Siber Ortam)

Siber uzay İngilizce "cyberspace" olarak anılmakta ve tıpkı fiziksel uzay gibi boyutu ve derinliği bilinmemektir. Siber uzay kavramı literatürde sürekli gelişmekte ve gelişmektedir. Siber uzay genel hatlarıyla interaktif bir alan olup, internete, bilgisayar ağlarına ve elektronik haberleşme ağına doğrudan ya da dolaylı olarak bağlı tüm sistem ve hizmetlerdir(Ulusal Güvenlik Stratejileri,2020-2023,s.10).

Siber uzayın başlıca aktörleri, kötü amaçlı kişiler, teröristler, grup yada bireysel olan suçlular yada uluslararası örgütler rakiplerini bertaraf etmek, bilgi sızdırmak isteyen ekonomik avantaj ya da savaş aracı olarak kullanmak isteyen ülkeler, ülkelerin istihbarat örgütleri ya da silahlı kuvvetleridir(Çifçi,2013,s.5).



Şekil-3- Hareket Alanı

Sonuç olarak, siber uzayın genişlemesi, bilgi iletişim sistemlerinin ve teknolojinin ivme kazanmasıyla deniz, hava, kara ve uzay hareket alanına siber uzay hareket alanını eklemiş ve siber uzay da hareket eder hale gelinmiştir. Dünyanın güçlü ve etkin ordularınca beşinci boyut olarak kabul edilmiştir. Devletlerin iç ve dış politikalarını belirleyen temel öğelerden bir haline gelen siber uzay aynı zaman da askeri alanda önemli bir dinamik haline gelmiştir(Çeliktaş,2016,s.7).

1.2.Siber Saldırı ve Siber Tehdit

Günümüzde bahsettiğimiz gibi bilgi, iletişim ve teknolojinin hızla yayılmakta, siber uzay kullanımı hızla yaygınlaşmakta, bunların neticesinde ise kritik altyapı sektörleri başta olmak üzere bilgi ve iletişim teknolojilerine yapılan saldırılar artmaktadır.

2020-2023 Ulusal Siber Güvenlik Stratejisi (2020,s.10)'ye göre siber uzayda işlenen siber saldırı, bilişim sistemlerine kasıtlı olarak yapılan ve verinin/bilginin bütünlüğü, gizliliğini veya erişe bilirliğinin ortadan kaldırmak amacıyla yapılan işlemler olarak tanımlanmaktadır.

Ülkeler için önemli olan ve bir siber saldırı da büyük ölçekli ekonomik ve can kayıplarına neden olan alt yapı sektörleri başta, su yönetimi, ulaştırma, finans, elektronik haberleşme, kritik kamu hizmetleri, enerji, sağlık, tarım, gıda ve kültür ve turizm sektörlerini kapsamaktadır.(Ulusal Siber Güvenlik Stratejisi,2020,s.9).

Tüm bu kritik alt yapı sektörlerine saldırma, tehdit oluşturma, veri çalma, değiştirme, hizmet dışı bırakma, devlet ve ticari kuruluşlara maddi açıdan büyük zararlar verme eylemleri genellikle planlı ve koordineli olabildiği gibi zaman zaman bilinçsiz kullanıcılar tarafından da siber tehdit ve siber saldırılar olabilmektedir. Siber tehditlerin ve siber saldırıların yöntem, kullanıcı hedefleri benzerlik göstermektedir.

1.3. Siber Terörizm

Siber terörizm kavramı için birçok yaklaşım bulunmaktadır. Genel çerçeveyi çizmek gerekirse, siber terörizm politik amaç güderek, toplumu ve devleti bu amaçlara kabul etmesi için zorlamak amacıyla dijital kritik altyapıların parçaları olan bilişim sistemlerine, sanal ağ ve iletişim alt yapılarına karşı yapılan eylemlerdir(Güvenlik Terimleri Sözlüğü,2018,s.624).

Çoğu zaman büyük maddi kayıplar ve 11 Eylül saldırılarında ya da kritik altyapılarına olan saldırılar gibi sivil ölümlerle sonuçlanabilen siber terörizmin en tehlikeli saldırı tipi ise ulusal kritik altyapılara ve finans sistemlerine karşı yapılan saldırlar kabul edilmektedir(TASAM,201). Örneğin Ulusal kritik altyapıları arasında sayılan Danışmalı Kontrol ve Veri Toplama Sistemleri (SCADA) terör örgütleri için potansiyeli yüksektir. SCADA sistemler elektrik ve su dağıtım şebekeleri gibi sistemlerin takibi ve kontrolünü sağlamaktadır. Kasıtlı olarak baraj kapaklarının açılması, su dağıtım hizmetlerin biranda kesilmesi ve elektrik kesintileri veya bu sistemler de oluşabilecek sorunlar siber terör saldırı sonucu gerçekleşebilir (Güvenlik Terimleri Sözlüğü,2018,s.625).

Aynı zamanda siber terörizm, sadece insanların mal ve can güvenliğini tehdit etmekle kalmayıp, ideolojik ve psikolojik etki yaratmak için yasadışı eylemlerle dini, siyasi, iletişim alt yapısı, bilgisayar ağları ve kritik altyapılara yapılan terör eylemleridir (Çifçi, 2013,s.6).

1.4. Siber Güvenliğin Uluslararası Düzeyde Yeri Ve Önemi

Uluslararası ilişkiler düzeyinde siber güvenlik kavramının önemi ve yeri her geçen gün arttığı düşünüldüğünde siber uzay da yaşanan gelişmeler, uluslararası arenada yeni aktörlerin doğmasını sağlamış ve yeni güvenlik riskleri meydana getirmiştir(Gürkaynak ve İren, 2011,s.265). Ülkeler için hayati önemi olan kritik altyapı sektörlerinde meydana gelebilecek siber tehdit, siber saldırı, siber terörizm gibi meydana gelecek eylemler için izlenecek diplomasi ve politikalar oluşturulma ihtiyacı doğmuş ve uluslararası gündemi işgal etmektedir.

Siber güvenlik ve altyapısının korunması ve güçlendirilmesi konusunda yapmak için G8, BM, NATO, Avrupa Konseyi gibi kuruluşlar çalışmalar yapmaktadırlar. Avrupa Konseyi 2004'te yürürlüğe giren ve uluslararası bir siber suç sözleşmesine ilişkin bir anlaşmaya varmıştır. Bu anlaşma ile siber suç konusunda ilk ve tek uluslararası sözleşme olan bu sözleşme ile Avrupa birliği Siber Suçlar Konvansiyonu'nda siber suçlara karşı mücadele de için önemli bir önemli adım daha atılmıştır. Anlaşmayı Avrupa Konseyi'ne üye devletlerden kırk ikisi sözleşmeyi imzalamış ve bunlardan yirmi beşi kanunu onaylamıştır(Turhan, 2010, s.s. 71-72).

Ülkelerin siber güvenlik yapılanmaları birbirlerinden zaman zaman farklılık gösterse de genel hatlarıyla benzemektedir. Siber uzayda yaşanan muhtemel siber güvenlik olaylarına adapte olabilmek için bazı ülkeler siber güvenlik ile ilgili yeni kurumlar oluştururken bazı kurumlar ise bu alanda yetkinliklerini genişletmekle yetinmektedir(Ada, 2018, s. 61).

İKİNCİ BÖLÜM

2.Siber Saldırı ve Siber Saldırı Türleri

Siber saldırılara karşı siber güvenliği sağlayabilmek için siber saldırı anatomisinin bilinmesi gerekmektedir. Saldırılara karşı teknik olarak hazır bulunmak şarttır. Saldırganların internetten en ufak açık kaynak bilgi elde etmesi saldırganlar için son derece önemlidir(Kiraz,2021,s.61).

Siber uzayın genişlemesi ve siber saldırılarla bir güvenlik açığıyla altyapı sektörlerinin, şirket ve devletlerinin uğradıkları ekonomik ve sivil kayıplarla kara, deniz, havadan sonra siber uzay beşinci hareket alanı olarak kabul edilmiştir. Nitekim bu siber saldırılarda kullanılan siber silah tanımının uluslararası hukuk kurallarına ve insani standartlarda uygunluğunun denetlenmesi

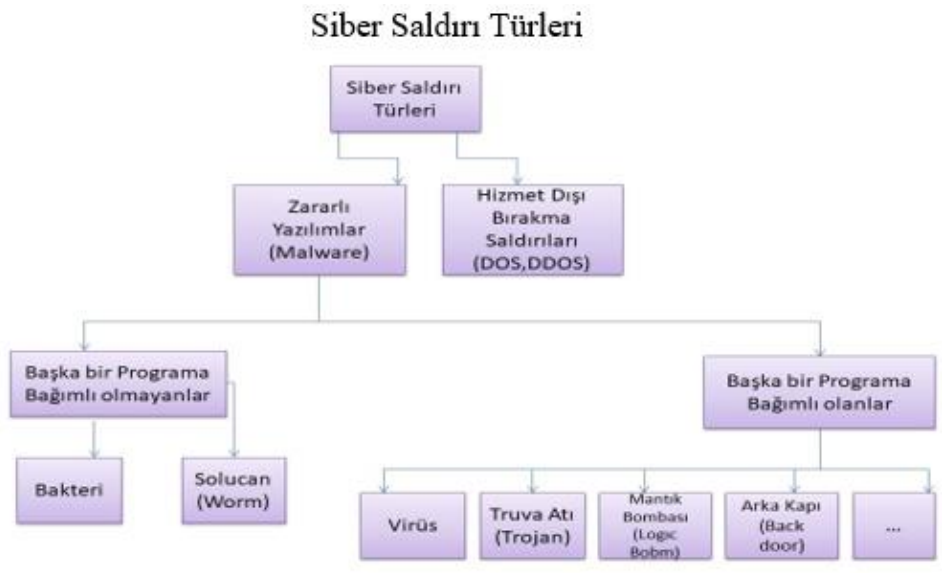
için siber silah tanımı için daha özelle indirilmesi gerekmektedir (Brown ve Metcalf, 2014, s.137).

Siber uzayda kullanılan savunma ve saldırı amaçlı her türlü araç olan siber silahlarla ilgili birçok tanım bulunmaktadır. NATO'ya ve genel olarak tanımlamak gerekirse, kötü amaçlı yazılım yada kod parçasıdır(Sağıroğlu ve Alkan, 2018, s.25).

Siber uzayda kurum, kuruluş ve devletleri zarara uğratmak amaçlı kullanılan siber saldırı yöntemlerinin bilinmesi ve tedbirlerin alınması ve güvenliğin arttırılması artık elzemdir. Günümüzde teknolojinin gelişmesi karışılabilecek tehdit türlerinde azalma beklenirken maalesef saldırılar da artış olmuştur. Artık yüzbinlerce saldırı türü, on binlerce siber silah aracı, milyarın üzerinde kötücül yazılımla berber yüz binin üzerinde yeni saldırı ve yüze yakın ileri düzey kalıcı saldırı yaklaşımları vb. bulunmaktadır(Sağıroğlu ve Alkan, 2018, s.38).

2.1.Siber Saldırı Türleri

Siber uzay da siber saldırıların tespitinin zorlaşması, etkilerinin artması için kötü amaçlı yazılımların atası olarak kabul edilen virüsler sürekli yöntem ve şekil değiştirmektedir. Kendini yenileyen ve gelişen bu kötü amaçlı yazılımlar geleneksel den öteye yeni nesil kötü amaçlı yazılımları meydana getirmişlerdir. Sık sık değişik gizlenme teknikleri kullanan yeni nesil kötü amaçlı yazılımlar analiz ve tespitin zorlaşması hem de daha ileri düzeyde siber saldırılar başlatmaktadırlar. Bu nedenle kötü amaçlı yazılımların oluşturdukları zararı en aza indirmek ya da önlemek adına kötü amaçlı yazılımları analiz etmek son derece önemlidir (Sağıroğlu ve Alkan, 2018, s.234).



Şekil-4- Siber Saldırı Türleri Şeması

2.1.1.Zararlı Yazılım (Malware - Malicious Software)

Siber saldırı türü olarak nitelendirdiğimiz ve bilgi sistemlerine zarar verme, çalışmayı sekteye uğratma ve bilgi çalma için özel olarak üretilmiş, Truva atı, casus yazılımlar, solucan ve virüslere genel olarak zararlı yazılım denmektedir(USOM,2014,s.9).

2.1.2Bakteri

Yapı itibarıyla solucana benzeyen ve kendi kendine çoğalabilen ve kullanıcının bilgisayar performansını düşüklüğüne neden olan işlem gücü, disk alanı ve hafızayı engelleyen yazılımlar olup ve bu tarz bir sınıflandırma genellikle tercih edilmemektedir(Çifçi, 2013, s.150).

2.1.3.Solucanlar (Worm)

Virüsler bir programın çalışması ile bulaşırken solucanlar bağımlı olmadan kendi kendine bulaşabilen yazılımlardır. wormlar sistemin açıklıklarını kullanmakta ve bilgisayar hafızasını kullanıp kendini çoğaltabilir(Burlu, 2013: 115).

2.1.4.Virüs

Virüslerin çalışabilmesi için bir programa ihtiyaç duyarlar. Programın içerisinde gömülü olarak bulunan virüsler bir dosya ya da programdan diğerine yayılabilen, dosyaların paylaşması ya da kaplanmasıyla bulaşabilen dosyalara zarar veren yazılımlardır(Çifçi, 2013, s.152)

2.1.5 Tuva Atı(Trojen)

Mitoloji geçen Truva atının armağan şeklinde sunulup fakat Troyayı istila eden Yunan askerini taşıdığı gibi Trojanlar da bilgisayar sisteminde kullanışlı ve eğlenceli görünüp arka plan da sistemde gizli bilgilere ulaşıp bunları dışarıya göndermeye yarayan casus yazılımlardır. Trojanlar ile kişisel belgelere, ekran görüntülerine, resim, şifre ve ortamdaki ses ve web kamerasına gizlice ulaşabilmek mümkündür(Burlu, 2013, s.125).

2.1.6 Mantık Bombası (Logic Bomb)

Çalışan yazılımın içerisine monte edilmiş ve belirli bir zamanda, belirli bir şartta ve durumların oluşumu ile çalışan aksi durumda çalışana kadar program içerisinde bekleyen sisteme zarar vermek için bekleyen kod parçası ya da programdır(Çifçi, 2013, s.154).

2.1.7.Arka Kapı (Back door, Trap Door)

Genellikle gizli yollarla şifreli sistemlere ve bilgisayarlara girebilmek için standart kullanılan kimlik doğrulama yöntemlerini kullanmadan, sadece saldırganlar tarafından bilinen yöntem ve giriş noktalarıdır (Çifçi, 2013, s.154; Keleştemur, 2015, s.225).

2.1.8 Kök Kullanıcı Takımı (Rootkit)

Bilgisayar sistemine bulaşıp aktif işlemler sırasında kendini gizleyen ve işletim sisteminden değişiklik yapan yazılım paketlerine denmektedir. Kötü niyetli kişilerce sistemde varlığını gizlemeyi amaç edinir (USOM Siber Güvenliğe İlişkin Temel Bilgiler, 2014, s.11).

2.1.9 Casus Yazılım (Spyware, Adware)

Casus faaliyetlerini yapmak üzere geliştirilen, kullanıcının rızası olmadan, bilgisayarın kontrolünü sağlayarak etkinliklerini takip edebilir, kurum ve kuruluşlar hakkında bilgi toplayabilir hatta e-posta ile başka kişilere gönderebilir, sms atabilir, ftp'ler ile topluca gönderimler de bulunup birçok işlemi yapabilen kötücül yazılımlardır(Sağıroğlu ve Alkan, 2018, s.28).

2.1.10 Köle Bilgisayarlar (Botnet, Zombie)

Büyük çaplı saldırılar da kullanabilen, köle bilgisayarlar olarak adlandırılan ve asıl saldırıyı yapanlar tarafından her an kullanmayı bekletilmekte ve bir program tarafından uzaktan kontrol edilerek kullanılan kötücül yazılımlardır(Güngör, 2015, s.45).

2.1.11 Gelişmiş Siber Tehditler (Advanced Persistent Threats, APT)

Hedefe yönelik yapılan, dikkatli ve sistematik bir çalışmanın ürünü olan, uzmanlığa ihtiyacı olan keşfedilmesi zor ve uzun zaman olan yazılımdır. Bu saldırı türü sıfır gün saldırılarında bulunan, geleneksel metot bulunamayan ve anti-viral yazılımların tespit etmesinin zor olduğu casus yazılımlardır. Bu saldırılara en iyi örnek Stuxnet olarak verilebilir. Yapay zeka yaklaşımlarını içinde barındıran 100'e yakın bu saldırı türüne örnek saldırılar mevcuttur(Sağıroğlu ve Alkan, 2018, s.30).

2.1.12 Fidye Virüsü (Ransomware)

Son dönemler de oldukça geniş kitleleri etkilen ve gündem de olan zararlı yazılım türüdür. Truva atı gizlice bilişim sistemine giren ve güvenlik açıklıklarından faydalanarak program ya da dosyanın çalıştırılması sonucu aktif olmaktadır. Kullanıcının dosyaları gelen virüsle

açılamaz hale gelir ya da kullanıcının dosyaları çözülemeyecek şekilde şifrelenir. Kullanıcı şifrelerin çözülmesi için karşı taraftan belli bir süre içerisinde fidye talep eder aksi takdir de dosyaları silmektedir (Symantec, 2015, s.s.3-28).

2.1.13. DoS ve DDoS Saldırıları

DoS saldırıları server (sunucu) bilgisayara aynı anda ve çok fazla paket göndererek mağdurun hizmeti kesintisine uğramasına, iş göremez hale gelmesi sonucu oluşur. DDos saldırıları ise güvenlik açıklarından faydalanarak ele geçirilmiş ve uzaktan yönetilen köle bilgisayarlar (zombi,bot) yönetilen yani bilgisayar kullanıcısının devre dışı bırakıldığı durumlar için ifade edilmektedir(Keleştemur, 2015, s.307). DDos saldırıları hedef bilgisayar on binlerce bilgisayarın saldırınsa maruz kalacağı için uzun süre hizmet kesintisine sebep olmakta etkilidir.

2.1.14. Sosyal Mühendislik

Teknoloji kullanmaktansa mağduru, hediye, para önermek, güvenirliğine ikna etme, sahte senaryolarla özellikle sosyal paylaşım sitelerinde yakınlık kurarak, telefon, e-posta ile iletişim geçilip, zor durumda olduğu ve bu sebeple yardım ediyormuş izlenim vererek buna benzer senaryolarla mağdurdan bilgi alma yada işleri yapmasını sağlamak olarak tanımlanmaktadır(Çifçi, 2013, s.147).

2.1.15.Yemleme, Oltalama (Phishing)

Bu saldırı da genellikle kötü amaçlı kişiler e-posta yolluyla resmi kurum yada kuruluşlardan kişisel bilgilerini öğrenmek isteyerek gerçekleştirileceği gibi güvenilir web sitelerin birer kopyasını oluşturularak gönderilen e-posta da sahte siteye girmesi sağlanıp kredi kartı ve kişisel bilgilerinin çalma eylemine oltalama yada yemleme saldırısı denmektedir (Çifçi, 2013, s.149).

2.1.16.IP Aldatmacası, Gizlemesi(IP Spoofing)

Kişi ve kurumların önemli verilene ulaşabilmek için bu saldırı türünde ise güvenli IP adresinin arkasına gizlenerek yapılmaktadır(Gürkaynak ve İren, 2011, s.272). Bu nedenle IP kandırmacası saldırganlar tarafından gönderilen paketlerin başlık bilgilerindeki kaynak IP kısmında değişiklik yapılarak hizmet veren sunucu ya da sistemlerin gerçek kaynağının gizlenerek adresin gizlenerek kullanıcının mağdur olmasıdır (Ünal, 2011,s.27).

2.1.17 İnternet Servis Saldırıları

İnternet servis Saldırıları, saldırganların kendi aralarında iletişim sağlayan dosya Transfer Protokolü (FTP), Elektronik Posta Gönderme Protokolü (SMTP), Hyper Metin Transfer

Protokolü(HTTP), İletim Kontrol Protokolü ve İnternet Protokolü (TCP/IP), Alan Adı Sistemi (DNS), Sınır Geçit Protokollü (BGP) gibi internet veya servislerinin zayıf noktalarından yada açıklıklarından faydalanarak yapılan saldırılardır(Çifçi, 2013, s.s.143,144, Keleştemur, 2015, s.301).

2.2. Uluslararası Siber Saldırı Örnekleri

Teknolojinin, bilgi, iletişim ve internettin yaygınlaşması ve gelişmesiyle birlikte sistemler de olumlu birçok avantaj sağlandığı gibi sistemlerin açıklık ve zafiyetlerinden faydalanarak sistemlerin çalışmasını ve engellenmesini karşı girişimler de artmıştır. Özellikle kritik altyapı olarak nitelendirdiğimiz sektörlere karşı yapılan saldırlar devletlerin önemsemesi gereken tehditler arasında yerini almıştır. Son zamanlar da dünya da yaşanmış önemli siber saldırlar incelendiğinde, siber saldırıların etkileri daha net görülmüş olmaktadır. Dünya da yaşanan siber saldırıların diğer bir önemi ise, sebeplerinin neler olabileceğini ve gelecekte yaşanacak muhtemel siber saldırı ihtimalli ile siber saldırılara karşı hazırlık, farkındalık ve güvenlik seviyelerini belirlenmesinde faydalı olunacağını değerlendirmektedir.

2.2.1 Rus-Çeçen Harbi (1999)

Bilgi savaşının(information War) ilk örneği niteliğinde olan Rus-Çeçen harbi ile Rus birliklerinin ağır silahlarla Grozni'ye girdiklerinde Çeçenler için direnişin çok kısa olduğunu umsalar da tüm medya imkânlarını kullanana Çeçenler için durum aynı değildir. Çeçenler internet ortamına ölen Rus askerin resimlerini yaymışlardır. Çocukların resimlerini gören anneler ise hareket geçmişlerdir. Bu nedenle savaş ortamında internettin kullanıldığı ilk örnek olarak kaydedilen bu olay sonrası internettin gücü fark edilmiş ve uluslararası aktörler internet merkezli saldırılara karşı daha tedbirli olup karşı hazırlık yapılmaya başlanmıştır(Aydın,2013, s.30).

2.2.2. Hainan Adası Olayı (2001)

Hainan Adası'na zorunlu inişe zorlanan ABD uçağının, Çin uçağıyla Güney Çin Denizi çarpışması sonucu yaklaşık 80000 Çinli siber saldırgan da ABD hükümetine karşı kendi savunmasını başlatmıştır(Çifçi, 2013, s. 164). Birinci İnternet Savaşı (World wide Web War I) olarak nitelendirilen bu olay ünlü The New York Times gazetesinde yer almıştır(Smith,2001).

2.2.3. İkinci Irak Savaşı (Körfez Harbi 2003)

İkinci Irak Savaşı'nda ABD askeri konvansiyonel savaşa başlamadan önce siber saldırı da bulunarak Irak ağına sızmıştır. Irak Savunma Bakanlığı sistemi üzerinden çok sayıda Iraklı

subaya e-postalar göndererek savaşmadan teslim olmalarını sağlamışlardır. Siber saldırı ile psikolojik savaş yürütmüş, düşmanın moralini bozarak savunmasını zayıflatmıştır(Çifçi, 2013, s.165).

2.2.4.Estonya Olayı (2007)

Estonya hükümeti İkinci Dünya Savaşı sırasında Sovyet askerlerini simgeleyen heykelin şehir dışına taşınması kararına karşın üç hafta süreyle DDos saldırına maruz kalmıştır. Resmi internet sitelerine, kolluk hizmetleri, bankacılık ve medya hizmetleri yoğun olarak kaldığı bu DDos saldırıyla büyük zarara uğramış, hizmet kesintileri ve çalışamaz hale gelmiştir.(Çakmak ve Soyoğlu, 2009, s.121).

2.2.5. Stuxnet (2010)

Siber uzayda gerçekleşen en büyük saldırılardan kabul edilen Stuxnet saldırısının yayılma alanı çok geniş olmasına rağmen en çok bu durumdan en çok İran etkilenmiştir. İran hükümetini Stuxnet solucanı uranyum zenginleştirme programın sızarak yaklaşık 2 yıl, nükleer tesisinde yine yer alan yaklaşık 1000 santrifüjü da çalışmaz hale getirerek büyük ölçekli maddi kayıplara yol açmıştır(Mueller ve Yadegari,2012, s.10).

Siber güvenlik tarihin de bu olayla sadece ağa değil aynı zaman da dış dünyaya kapalı olan ICS'leri hedef alınarak siber güvenlik farkındalığı yada yeteri kadar hazırlığı olmayan ülkeler için bir nevi göz dağı niteliği taşımakla kalmamış aynı zaman siber güvenlik tarihinin dönüm noktası niteliğindedir (Çifçi, 2013, s.176).

Aynı zamanda Stuxnet solucanının kodunun karmaşıklığı, büyüklüğü ve sadece özellikli sistemlere buluşması bu olay arkasında en az bir devletinin olduğunu düşündürmüştür. Nitekim dünya kamuoyu asıl saldırganları bulamazsa da ABD ve İsrail'in ortaklaşa ürettiğini düşündüren güçlü kaynaklar vardır(Mueller ve Yadegari, 2012, s.10).

2.2.6. Rusya ve Türkiye Arası Siber Saldırılar (2015)

Ülkemizde 14 ve 24 Aralık 2015 tarihlerinde altı farklı "DNS Sunucusu" hedef alınarak tarihinin en büyük siber saldırına maruz kalmıştır. DDoS saldırı neticesinde internet hizmettin engellenmesi amaçlanmıştır. Bir hafta boyunca yaklaşık 400 bin "com.tr", "edu.tr", "gov.tr" uzantılı sitelere hiç giriş sağlanmamıştır. Bu saldırıyı Anonymous adlı hacker grubu üstlenmesine rağmen bu büyüklükteki gerçekleşen saldırıyı bir devlet desteği olmadan yapılma olasılığı düşük olduğu değerlendirmektedir. Bu saldırı öncesinde ise 24 Kasım 2015 de Rusya

ile yaşanan uçak krizi nedeniyle Rusya'nın olma ihtimalli akıllara gelmiştir(http://www.gazetevatan.com/siber-saldiri-degil-savas--898985-gundem/).

Ayrıca burada değinemediğimiz birçok siber saldırı örneği olduğu gibi siber uzayın büyümesiyle siber saldırılar her geçen gün artmaktadır. Bazı siber saldırı örnekleri mevcuttur. Bunlar; Gürcistan Olayı, İsrail'in Orchard Operasyonu, Black Energy ve KillDisk Truva Atı, Shady RAT, İsrail'in Cast Lead Harekâtı,Titan Rain, Conficker, JSF (Joint Strike Fighter veya F-35) verilerinin çalınması, Ghostnet, Operation Aurora, Night Dragon, Duqu, Flame ve Kızıl Ekim (Red October) Virüsü gibi yaşanmış başka örnekler mevcuttur.

Sonuç olarak yaşanan örneklerden anlaşıldığı üzere konvansiyonel savaşlar başlamadan ya da savaş sırasında siber saldırılarla siber savaşın varlığını gerçek olduğunu gözler önüne serilmektedir. Ayrıca konvansiyonel silahlardan daha az maliyetli ve hızlı oluşu kazanılmak istenilen savaşlar da dengeleri değiştirmiş ve değiştirilecektir(Çeliktaş,2016,s.s.12,13).

2.3. Siber Saldırılar Ve Siber Tehditler Karşı Alınacak Önlemler

Siber uzayın genişlemesi ve internettin yaygınlaşması sonucu kötü amaçlı insanların bu duruma paralel olarak siber saldırı teknikleri gelişmiş, sistem zafiyetlerinden teknolojik açıklardan daha fazla faydalanarak sistemlere, kurum, kuruluş ve devletlere birçok zarar verebilecekleri ortadadır. Siber saldırı ve siber tehditlerin artması nedeniyle bireysel ve ulus olarak yaşadığımız maddi kayıpların yani sıra kamu düzeninin bozulmasıyla artık topyekun olarak kamu kurum ve kuruluşların, sivil toplum örgütleri ve ulusal boyutta siber güvenlik hazırlıkları ve farkındalığının oluşturulması, geliştirilmesi ve uygulanması artık elzemdir(Canbay ve Ünver, 2010, s.99).

Ulusal güvenlik için yapılması gereken adımları şekil-5 de gösterildiği gibi adımlar atılması gerekmektedir.

Şekil-5- Güvenlik Unsurları Şeması

Ulusal güvenlik tedbirleri adımları oluşturulup uygulanırken siber güvenlik ve savunma ve önlemlerinin yanı sıra kurumlar mevcut veya muhtemel riskleri öngörerek kurumca ortaya çıkan sonuca göre kurumun güvenlik ihtiyaçlarına ve maliyetlerine göre riskleri kontrol etmelilerdir. Muhtemel risk süreçlerini, risk kontrollü ve risk analizi ile oluşturdukları risk yönetim mekanizmayla düzenli aralıklarda kontrol sağlanmalıdır. Çünkü iletişim ve bilgi teknolojilerinin gelişen ve sürekli değişen doğası gereği tehditler, zafiyetler, açıklıklar ve güvenlik ihtiyaçları da değişlik göstermektedir(Yılmaz ve Salcan, 2008,s.78). Aynı zaman da siber savunma sistemlerinin doğru ve efektif olarak kullanılması gerekmektedir.

2.3.1.Güvenlik Duvarı

Bilgisayar sistemlerine ve ağ bağlı oldukları ortamdan gelen giden sadece izin verilen bilgilerin geçmesine izin veren donanım veya yazılım parçasıdır. Güvenlik duvarında giden ve gelen paket trafiği izlendiği gibi filtrelemeler yapılabilmektedir(Çeliktaş,2016,s.48).

2.3.2. Anti Virüs

Virüsler ve solucan gibi zararlı yazılımları, klavye dinleme yazılımları, truva atları, arka kapı ve rootkitler gibi zararlı yazılımlarım sisteme girişini tespit ve yok eden programlara verilen genel addır(Çifçi, 2013, s. 200; Keleştemur, 2015, s.320). Kurum ya da bilgisayar

kullanıcılarının sıklıkla anti virüs programının güncelleme paketlerini yüklemesi ve güncelliğini takip etmesi gerekmektedir.

2.3.3.Yığın İleti Engelleme (Anti Spam)

Kullanıcıların e-postalarına reklam amaçlı gönderilen kötü amaçlı yazılımları engelleyen sistemlere denmektedir(Çifçi, 2013, s.201; Keleştemur, 2015, s.326). Kaynağının bilinmediği e-postaların açılmaması, bilgisayarına sızmak isteyen kötü amaçlı yazılımları engellemektedir.

2.3.4. Uç Nokta Güvenliği Sistemi (Endpoint Security)

Tek bir merkezden kurum içerisinde kontrol edilen bilgi iletişim ve ağ teknolojilerinin, yönete birliğini kolaylaştıran, saldırı tespiti, ağ erişim kontrolü, güvenlik duvarı ve veri kaçağı önleme gibi bütünleşik güvenlik sitemleridir(Çifçi, 2013, s.204; Keleştemur, 2015, s.321).

2.3.5. Elektronik İmza, Sayısal İmza (Electronic - Digital Signature)

Birçok bireyin ve birçok kurumun artık daha çok tercih ettiği elektronik imza ile yasal kimlik doğrulama sistemi elektronik ortam da imza yerine geçen, üretilmiş belgelerin imzalanmasına verilen genel ifadedir. Elektronik imza ile mesajın ya da belgenin inkar edilmemesine ve bütünlüğüne katkı sağlamakla asimetrik bir şifreleme yapmaktadır(Salcan ve Yılmaz, 2008, s.90).

2.3.6. Elektromanyetik Güvenlik (TEMPEST Karşı Tedbirleri)

Ağ ve bilgi teknolojilerinden yayılan veri sinyallerinin kötü niyetli kişiler tarafından yakalamasına ve yönlendirilmiş enerji saldırılarına karşı alınan güvenlik tedbirlerine genel olarak TEMPEST ya da elektromanyetik güvenlik denmektedir(Çifçi, 2013, s.s.211, 212).

Siber uzayda yaşanana siber saldırı ve tehditlerin çokluğu kadar karşı siber savunma mekanizmaları da her geçen gün gelişmektedir. Burada bahsetmediğimiz, Bal Küpü (Honeypot),Şifreleme (Kriptografi), Steganografi, Hava Boşluğu Sistemi, Ağ Erişim Kontrol Sistemi, Adli Bilişim Sistemleri (Computer Forensic Systems), İçerik Filtreleme Sistemi (Content Filter), Veri Kaçağı Önleme Sistemi (Data Loss Prevention, DLP), gibi birçok siber saldırıları engelleme ve önleme sistemi mevcuttur.

ÜÇÜNCÜ BÖLÜM

3.Türkiye'de Siber Güvenlik Politikalarının Durumu

Güvenlik kavramının soğuk savaş döneminden sonra değişmesi, siber uzayın genişlemesi ve internettin yaygınlaşmasıyla ülkelerin artık daha hızlı ve ucuz maliyetle savaş sahnelerinde var olmak istemesi siber saldırı ve siber tehditlerin sayısındaki artış dünya ülkeleri ve uluslararası örgütlerin bu konuda çalışmalarına hız vermesine neden olmuştur. Bu nedenle Türkiye'de 2009 yılında "Ulusal Sanal Ortam Güvenlik Politikası" ile siber güvenlik alanında ilk resmi nitelikte belge oluşturulmuştur. Bu politikanın önemli maddeleri arasında temel ilkeler, sistem açıklıkları, tehditler gibi güvenlik adımları ile uygulama adımlarını strateji ve eylem planın yerini almıştır(Kırdı, 2015).

Türkiye'de uzun bir süre siber güvenlik kapsamında siber terör, siber suç, saldırı ve tehditleri inceleyip değerlendirdikten sonra 2012 yılında Bakanlar Kurulu'nun "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna ilişkin Kararı" ile Siber Güvenlik Kurulu kurulmuştur. Bu karar ile Siber Güvenlik Kurulunun ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB)'nın görev ve yetkileri belirlenerek siber güvenlik çalışmaları resmen başlamıştır. Siber Güvenlik Kurulunun kurulma kararı siber güvenliğinin önemi artmaktayken Türkiye için siber güvenlik adına önemli ve stratejik bir adım olmuştur (Çeliktaş,2016,s.7).

Siber Güvenlik kurulunda İçişleri bünyesinde oluşturulan Emniyet Genel Müdürlüğü(EGM) Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma Genel Komutanlığı (JGK) Bilişim ve Teknik İstihbarat Başkanlığı, Sahil Güvenlik Komutanlığı İstihbarat Daire Başkanlığı Siber Suçlarla Mücadele Şube Müdürlüğü, BTK, MİT Başkanlığı, Afet ve Acil Durum Yönetimi (AFAD) Başkanlığı, TSK Siber Savunma Komutanlığı, TÜBİTAK, Savunma Teknolojileri Mühendislik, Hava Elektronik Sanayii (HAVELSAN) ve Askeri Elektronik Sanayii (ASELSAN) ve Siber Güvenlik Kurulu (SGK) yer almaktadır. Oluşturulan kurulda öncellikli eylem planın oluşturulması ve Kritik altyapı sektörlerinin belirlenmesi ve UDHB tarafından "Ulusal Siber Güvenlik Strateji Belgesi ve 2013-2014 Eylem Planı" çerçevesinde yürütülmesi, Kamu kurumlarının Kamu Net projesiyle güvenli bir ağla veri iletişimin yapılması ile Siber Güvenlik Kurulunun görevleri, esas ve çalışma usulleri çizilmiştir. Bu kapsamda Türkiye'nin ilk Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı da yayınlanmıştır(Darıcılı, 2019, s.28).

Siber Uzayın büyümesiyle siber saldırı ve tehditlerin şeklinin değişmesiyle Türkiye' de geçmiş Ulusal Siber Güvenlik Strateji planlarını değerlendirerek ve sürekli yenilenerek 2013-2014,

2016-2019 ve güncel olarak 2020-2023 dönemi Ulusal Siber Güvenlik Eylem Planı yayınlanmıştır. Sürekli olarak gözden geçirilen ve gerekli iyileştirilmeler yapılarak 8 ana başlık altında toplanmıştır.

Eylem Planında yer alan önemli 8 ana başlık ise,

- Yerli ve Milli Teknolojilerin Geliştirilmesi ve Desteklenmesi,
- Ulusal Kapasitenin Geliştirilmesi,
- Kritik Altyapıların Korunması ve Mukavemetin Artırılması,
- Uluslararası İş Birliğinin Geliştirilmesi,
- Yeni Nesil Teknolojilerin Güvenliği,
- Yerli Siber Güvenliğin Milli Güvenliğe Entegrasyonu,
- Organik Siber Güvenlik Ağı,
- Siber Suçlarla Mücadele yer almaktadır.

Ülkemizde siber güvenlik olaylarına müdahale için ulusal ve uluslararası koordinasyon amacıyla USOM yani "Ulusal Siber Olaylara Müdahale Merkezi" kurulmuştur. Bu birim, Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde oluşturulmuştur (www.btk.gov.tr).

BTK bünyesinde olan Ulusal Siber Olaylara Müdahale Merkezi (USOM, TRCERT), kendisine ulaşan ihbarları değerlendirerek tehditleri bertaraf etmek için çalışmaktadır. Gerekli gördüğünde Kamu Kurum ve özel kişiler ile ilgili koordinasyon kurar. İhbarların çözüm sürecine kadar takibini yaparak çözüm üretmekte ve gerekli gördüğünde siber güvenlik tatbikatları yaparak kamu kurumlarının ve kuruluşlarının siber saldırılara karşı farkındalığını geliştirmektedir. (www.usom.gov.tr).

Bilgi Teknolojileri ve İletişim Kurumunun sunmuş olduğu "İnternet Bilgi İhbar Merkezi" hizmeti dikkate değerdir. Buna göre 5651 sayılı yasa uyarınca: İntihara yönlendirme, Çocukların cinsel istismarı, Uyuşturucu veya uyarıcı madde kullanımının kolaylaştırılması, Sağlık için tehlikeli madde temini, Müstehcenlik, Fuhuş, Kumar oynanması için yer ve imkân sağlanması, Atatürk aleyhine işlenen suçlar ile ilgili yeterli şüphe oluştuğu takdirde internet uzantılarını yazarak içerikleri, İhbar Web'e giriş yaparak şikâyette veya ihbarda bulunulabilmektedir (www.ihbarweb.org.tr). Ayrıca, 10 Temmuz 2018 tarihli ve 30474 sayılı Resmî Gazete 'de yayımlanan 1no'lu Cumhurbaşkanlığı Kararnamesi ile kurulan Dijital Dönüşüm Ofisine (DDO) "Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek"

görevi verilmiştir. Bu çerçevede, 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ile Bilgi ve İletişim Güvenliği Tedbirleri yayımlanmıştır.

SONUÇ

Siber güvenliğin önemi siber uzayın genişlemesi, internettin yaygınlaşması ile COVID-19 Pandemi sürecinde bir kez daha anlaşılmıştır. Bu süreçte eğitim ve iş hayatı başta olmak üzere birçok alışkanlığımız değişmiştir. Pandemi sürecinde teknolojinin sunduğu birçok imkândan faydalanırken güvenli bir dijital ortamın sağlanması için birey, kurum ve ülke olarak siber güvenlik farkındalık yüksek olmak zorundadır. Bunun içinde Ülke olarak siber güvenlik için küçük yaşlardan itibaren çocuklarımıza farkındalık eğitimi verilmeli, milli teknoloji özendirilmelidir. Siber farkındalık eğitimleri ve dijital medya okuryazarlığı eğitimleri her yaş grubu bireye verilmelidir. Sürekli kamu spotlarıyla farkındalık oluşturulmalıdır. Üniversitelerde lisans ve lisansüstü program sayısının arttırılması gerekmektedir.

Bilgi ve iletişim ve Teknolojik gelişmeler artık durmadan devam edeceği artık aşikârsa yeni çözümler ve stratejilerin üretilmesi için alanında uzman personelle ihtiyaç da her geçen gün artacaktır. Ülkemiz de bu konuda çalışan akademisyenlerimizin olduğu bilinse de sayısı maalesef yetersiz kalınmıştır.

Devlet ve özel sektör de yer alan kuruşlar kullandıkları uygulamaları genellikle kendi iç ağında gerçekleştirmekte yalnız herkesin erişimine açık olan internet üzerinden gelecek saldır ve tehditlere karşı yetersiz kalmaktadır.

Özellikle e-devlet üzerinden yürütülen hizmetler, kritik altyapı hizmetleri, finans ve bankacılık sektörleri siber tehditlere daha açık bulunmaktadır. Buralarda çalışan üst düzey personel başta olmak üzere düzenli siber farkındalık eğitimlerin verilmesi gerekmekte zaman zaman çalışanlara oltalama yaparak çalışanların farkındalığını sürekli etkin tutmaya çalışılmalıdır.

Siber tehditlerin sayısı her geçen gün artarken yıkıcı sonuçları ve saldırı türleri de sürekli değişmektedir. Bu durum da tehditlerle mücadele risklerin ve ihtiyaçların doğru analiz edilmesine, kaynakların doğru kullanılmasına kısa ve uzun vadede planlamalarla ülke olarak siber güvenliğimiz daha iyi değerlendirilmiş olacaktır. Nitekim 2020-2023 Ulusal Siber Güvenlik Strateji ve Eylem Planında genel hatlarla belirtildiği gibi Milli Teknoloji, Milli ağ kullanımı için çalışmalar yapmanın önemi her geçen gün artmaktadır. Milli ürünlerle hem dışa bağımlığımızı hem de ekonomik büyük kazançlar sağlanacaktır.

Sonuç olarak, dijital dünyanın getirmiş olduğu avantajlı yanları kullanırken dezavantajlı taraflarını gören ve bu konuda öngörü oluşturabilen devletler, siber güvenlik mücadelesinden bertaraf olmayacaklardır. Siber güvenlik meselesine sadece devlettin meselesi gibi değil topyekûn millet olarak yaklaşmak bireysel olarak üzerimize düşen görev ve sorumlulukları yapmalıyız. Teknolojik açıdan toplumsal farklılıkların hiç olmadığı kadar azaldığı günümüzde bu durumu lehimize çevirerek öncü bir toplum olabilir kendi milli ürünlerimizi üretmek için gayret gösterebiliriz.

KAYNAKÇA

Aydın, M.(2013), 21.Yüzyılda Siber Güvenlik, 1.Baskı, İstanbul: İstanbul Bilgi Üniversitesi Yayınları

Bıçakçı, S. (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", Uluslararası İlişkiler Akademik Dergisi, s.s.101-130.

Bilgi Teknolojileri ve İletişim Kurumu. (2021). USOM ve Kurumsal Siber Olaylara Müdahale Ekibi. E.t:10.09.2021 (https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahaleekibi)

Bilgi Teknolojileri ve İletişim Kurumu. (2020). İnternet Bilgi İhbar Merkezi. E.t:10.09.2020 (https://www.ihbarweb.org.tr/).

Burlu, K. (2013). Bilişimin Karanlık Yüzü (4. Baskı), Nirvana Yayınları, Ankara.

Brown, G.D. ve Metcalf, A. O.(Ed.) (2014), "Easier Said Than Done: Legal Reviews of Cyber Weapons", Journal of National Security Law and Policy, s.s.115- 138

Canbek, G. ve Sağıroğlu, Ş.(2007), "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, s.s.1-12.

Çakmak, H.ve Soyoğlu, İ. K. (2009), "Doğu Avrupa ve Asya'dan Siber Saldırı Örnekleri", Suç, Terör ve Savaş Üçgeninde Siber Dünya, 1. Baskı, Ankara: Barış Platin Kitabevi.

Çeliktaş, B.(2016), Siber Güvenlik Kavramının Gelişimi Ve Türkiye Özelinde Bir Değerlendirme, Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü,Trabzon.

Çifçi, H.(2013), Her Yönüyle Siber Savaş, İstanbul: TÜBİTAK Popüler Bilim Kitapları.

Darıcılı, A.B. (2018). Askerileştirilen ve Silahlandırılan Siber Uzay, Ankara: NOBEL Akademik Yayıncılık.

Güngör, M. (2015), Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma, Uzmanlık Tezi, T.C. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı.

Gürkaynak, M.ve İren, Â. A.(2011), Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler, Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Dergisi, s.s.263-279.

Keleştemur, A.(2015), Siber İstihbarat,1. Baskı, İstanbul: Yazın Basın Yayınevi Matbaacılık Trz.Tic.Ltd.Şti.

Kırdı, G.(2015), Türkiye'de ve Dünya'da Siber Güvenlik Alanında Çalışmalar, Et.12.09.2021, http://sahipkiran.org/2015/01/14/siber-guvenlik/

Kiraz, O.Z.(2021), Siber Güvenlik Bağlamında Yeni Tehdit Algılamalarının Türkiye'nin Güvenlik Politikalarına Etkileri, Batman Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, s.s.60, 64.

Mueller P. ve Yadegari B. (2012), "The Stuxnet Worm", Et.10.09.2021, https://www2.cs.arizona.edu/~collberg/Teaching/466566/2012/Resources/presentations/topic9-final/report.pdf

Sağıroğlu, Ş.(2018). Siber Güvenlik Ve Savunma: Önem, Tanımlar, Unsurlar Ve Önlemler, (der: Sağıroğlu, Ş. ve Alkan, M.), Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Grafiker Yayınları, Ankara.

Singer, P.W. ve Friedman, A.(2015), Siber Güvenlik ve Siber Savaş, (Çev. Ali ATAV), 1.Baskı, Ankara: Buzdağı Yayınevi, 57.

Smith, Craig S. (2001), "6-12; The First World Hacker War", The New York Times, Et.12.09.2021, https://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html.

Tatar, Ünal (2011), Sosyal Mühendislik Saldırıları, TÜBİTAK, BİLGEM, Et: (03.09.2021), https://www.emo.org.tr/ekler/288230da37dbf3c_ek.pdf.

TASAM(Türk Asya Stratejik Araştırmalar Merkezi). (2004). Siber Terörizm Raporu,Et:05.09.2021https://tasam.org/Files/Icerik/File/siber_terorizm_raporu_84be5753-d219-418f-9a68-e6c719b645b1.pdf.

Türkiye Cumhuriyeti İç İşleri Bakanlığı Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı. Et:24.09.2021 https://www.egm.gov.tr/siber/sibersucnedir.

Ünver, M. ve Canbay, C. (2010), Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik, Elektrik Mühendisliği Dergisi, s.s.94-103.

Yılmaz, S. ve Salcan, O.(2008), Siber Uzay'da Güvenlik ve Türkiye, 1, İstanbul: Milenyum Yayınları.

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Planlaması, https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf Et.20.08.2021

http://www.gazetevatan.com/siber-saldiri-degil-savas--898985-gundem/.

ELEKTRONİK BONO VE ÇEK İLE KAMBİYO SENETLERİNDE DEĞİŞEN ÖZELLİKLER

Dr. Öğr. Üyesi Buket Çatakoğlu Aydın [1]

[1] Nevşehir Hacı Bektaş Veli Üniversitesi, İİBF, ORCID: 0000-0002-5035-6908

ÖZET

Kambiyo senetleri içerisinde bono ve çek, ticaret hayatında son derece sık kullanılan iki türü oluşturmaktadır. Anılan senetler kambiyo senetleri olarak adlandırdığımız senet grubuna ilişkin ortak özellikleri bünyesinde barındırmaktadır. Yani soyut nitelikte ve kanunen emre yazılı olarak kabul edilen, ciro yoluyla tedavül eden, senetten dolayı herhangi bir şekilde borç altına girenlerin sorumluluklarının birbirinden bağımsız olduğu ve para alacağı içeren senetlerdir. Çek daha çok bir ödeme aracı niteliğine sahipken, bono ise bir kredi aracı işlevi görmekte ve fakat ileri tarihli (vadeli) çek uygulamasıyla çekler de esasında kredi aracı olarak çoğu zaman ticaret hayatında kullanılmaktadır. Bir taraftan da günümüzde dijitalleşmeye doğru hızla yönelme ve sadece ekonomik boyutta değil, hayatın tüm alanlarında kendisini hissettiren teknolojik gelişmeler yaşanmakta ve bu durum fiziki kağıda bağlı klasik ticari senetlerin yanında elektronik olanlarının da piyasaya çıkmasına neden olmaktadır. İşte elektronik çek ve bono da bu anlamda ülkemizde yasal düzenlemeye kavuşturulması çok yakın zamanda beklenen iki elektronik ticari senet türü olarak karşımıza çıkmaktadır.

Ticaret Bakanlığı bu bağlamda Elektronik Çek ve Bono Kanun Teklifi hazırlayarak bu hususa ilişkin önemli bir adım atmıştır. Böylelikle ticaret hayatında zaten çok önemli yeri olan bu iki kambiyo senedinin hem günümüz teknolojsiyle uyumlu hale getirilmesi, hem kayıt dışılığın ve sahteciliğin önlenmesi ve tüm işlemlerin elektronik ortamda yapılmasına binaen ticaret hayatı için vazgeçilmez olan hızlılık hedeflenmektedir.

Anahtar Kelimeler: Elektronik çek, elektronik bono, kambiyo senedi

1. GİRİŞ

Türk Ticaret Kanunu'nun kıymetli evrakı düzenleyen üçüncü kitabının dördüncü kısmı "kambiyo senetleri"ne ayrılmıştır (m.670-823). Poliçe, bono ve çekten oluşan ve ticari senetler olarak adlandırılan bu senet grubu ticari hayatta yaygın olarak kullanılmaktadır. Anılan senetler aynen ödeme kaydıyla yabancı para üzerinden düzenlenebilmekte ve kullanım alanı sınır ötesi işlemleri de kapsamaktadır. Ancak uygulamada poliçenin bono ve çeke oranla daha

az kullanıldığı görülmektedir[1]. Kambiyo senetleri kıymetli evrak niteliğini en belirgin şekilde gösteren senetlerdir ve öncelikle kıymetli evraka ilişkin genel hükümlere tabidirler (TTK.645-653)[2]. Kıymetli evrak kavramında öne çıkan en önemli özellik ise bilindiği üzere "hak ve senet bağlılığı"dır. Hak ve senet arasındaki sıkı bağlılık olmaksızın bir senedi kıymetli evrak olarak nitelendirmek mümkün değildir. Burada bahsedilen "senet" kavramı, genellikle üzerine yazı yazmaya elverişli bir cisim ve çoğunlukla da uygun büyüklükte bir kağıt parçası ile bunun üzerinde yazıyla belirtilmiş bir irade beyanını ifade eder. Ancak günümüz teknolojisinin ilerlemesiyle klasik anlamdaki bu "senet" kavramının yeni versiyonları ortaya çıkmıştır[3]. Mikrofilm, manyetik bant, disket, çip vb. gibi bir irade beyanının elektronik ortamda ifade edilmesini sağlayan ve "taşıyıcı" olarak nitelendirebileceğimiz teknik birtakım araçların ve hatta mail metni gibi sanal ortamların da senet kavramına girebileceği, kıymetli evrakı tanımlayan TTK.645 hükmünün amaçsal yorumundan çıkarılabilir[4]. Fakat tüm bu durumlarda, irade beyanında bulunan kişinin nasıl saptanacağı ve nasıl imza atacağı gibi bir sorun ortaya çıkmaktadır[5].

Bir belgenin senet niteliğini kazanması için irade beyanını yazıyla açıklayan kimsenin imzasının bulunması da gerekir. İmza elle atılan klasik anlamda bir (ıslak) imza olabileceği gibi, senedi düzenleyen kişiden kaynaklandığı sabit olan bir işaret de olabilir. Bu anlayış, bugünkü teknolojik gelişim düzeyi ile de uyumludur. Yasal düzenlemeler de bu teknolojik gelişimin gerisinde kalamamış ve 5070 sayılı Elektronik İmza Kanunu (EİK) m.5/1'de, "*Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur*" hükmü yer almıştır. Buna paralel olarak Türk Borçlar Kanunu (TBK) m.15/1'de, "*güvenli elektronik imza da, el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğurur*" düzenlemesi getirilmiştir[6]. Ne var ki güvenli elektronik imzanın geçerli olmadığı istisnai haller vardır ve kambiyo senetleri de bu istisnalar arasındadır. Elektronik İmza Kanunu m.5/2'de, "*kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile banka teminat mektupları dışındaki teminat sözleşmeleri, güvenli elektronik imza ile gerçekleştirilemez*" denilerek bu istisnalara işaret edilmektedir. Bu hüküm uyarınca borçlar hukuku anlamında bir borç senedi elektronik imza ile düzenlenebilmekte, ancak kambiyo senetlerinden "*poliçe, bono, çek* ile *makbuz senedi,*

[1] Çamoğlu, Ersin, Kıymetli Evrak Hukukunun Temel İlkeleri, 1. Baskı, İstanbul, 2020, s.33-34; Bahtiyar, Mehmet, Kıymetli Evrak Hukuku, 18. Baskı, İstanbul, 2020, s.46.
[2] Pulaşlı, Hasan, Kıymetli Evrak Hukukunun Esasları, 8. Baskı, Ankara, 2020, s.118; Öztan, Fırat, Kıymetli Evrak Hukuku, 24. Baskı, Ankara, 2020, s.68.
[3] Öztan, s.11.
[4] Öztan, s.11-12; Pulaşlı, s.3; Bahtiyar, s.1.
[5] Öztan, s.12; Bahtiyar, s.1.
[6] Ülgen, Hüseyin/ Helvacı, Mehmet/ Kaya, Arslan/ Nomer Ertan, N. Füsun, Kıymetli Evrak Hukuku, 13. Baskı, İstanbul, 2021, s.18.

varant ve kambiyo senetlerine benzeyen senetlerin güvenli elektronik imza ile düzenlenemeyeceği" (TTK.1526/1) ve bu senetlerde imzanın ıslak imza olarak elle atılması öngörülmektedir (TTK.671/1-h, 776/1-g, 780/1-f). Yine "*bu senetlere ilişkin kabul, aval ve ciro gibi senet üzerinde gerçekleştirilen işlemlerin de güvenli elektronik imza ile yapılamayacağı*" açıkça belirtilmektedir (TTK.1526/1). Buna karşın "*konişmentonun, taşıma senedinin ve sigorta poliçesinin imzasının elle, faksimile baskı, zımba, ıstampa, sembol şeklinde mekanik veya elektronik herhangi bir araçla atılmasına*" izin verilmektedir (TTK.1526/2).

Kambiyo senetleriyle ilgili yasal durum yukarıda özetlediğimiz gibi olmakla beraber, Ticaret Bakanlığı'nın hazırladığı ve önce 2020'de ardından 2021'de yürürlüğü planlanmasına[7] rağmen henüz yasalaşmamış "Elektronik Çek ve Bono Kanunu Teklifi"[8], kambiyo senetlerinin en yaygın kullanılan bu iki türünün elektronik ortamda düzenlenmesi ve tedavülüne imkân sağlamaktadır. Böylece çek ve bononun güvenli elektronik imza ve hatta elektronik kimlik doğrulama yöntemiyle oluşturulan kimlik kaydı ile düzenlenmesi mümkün olacak, bu durum kambiyo senedi ve tipik kıymetli evrak niteliğine bağlı özelliklerinde değişimleri de beraberinde getirecektir. Çalışmamızın amacı değişime uğrayan bu özellikleri inceleyip olumlu veya olumsuz anlamdaki etkilerini ortaya koymaktır.

2. ELEKTRONİK BONO VE ÇEK İLE KAMBİYO SENETLERİNDE DEĞİŞEN ÖZELLİKLER

2.1. Elektronik İmza

Ticaret Bakanlığı'nın yukarıda sözünü ettiğimiz kanun teklifi 2015-2018 arası dönemde sadece elektronik çekle ilgili düzenleme içeriyordu. 2019 yılı başlarında elektronik bonoya ilişkin hükümler de bu teklif kapsamına dahil oldu[9]. Kanaatimizce çekin yanı sıra bononun da elektronik ortamda düzenlenmesi ve tedavülünün mümkün kılınması isabetli olmuştur. Zira esasında ticaret hayatında uygulaması en çok olan kambiyo senedi türü bonodur[10]. Ayrıca bu düzenleme sadece çek ile sınırlandırılsa idi, bu durum piyasada bononun kayıt dışı kullanımına ve tedavülüne yönelik bir artışı beraberinde getirecekti. Kanun koyucu

[7] "Çek ve Bonoda Elektronik Dönem Başlıyor", https://www.esin.av.tr/tr/2019/05/03/cek-ve-bonoda-elektronik-donem-basliyor, Erişim Tarihi: 01.12.2021; "2021'de çek-bonoya elektronik sistem getirilmesi planlanıyor", https:// www.bloomberght.com/2021-de-cek-bonoya-elektronik-sistem-getirilmesi-planlaniyor-2269211, Erişim Tarihi: 01.12.2021.

[8] Elektronik Çek ve Bono Kanunu Teklifi ile getirilen düzenlemeler hakkında detaylı bilgi için bkz. Tevetoğlu, Mete, "Elektronik Çek ve Bono Kanunu Teklifi İle Yapılması Planlanan Düzenlemelere Dair Düşünceler", Bilişim Hukuku Dergisi, S.1, 2021, s.31 vd.

[9] Çotuksöken, S. Emre, "Dijitalleşme, Elektronik Çek ve Blockchain İlişkisi", Finans Hukuku Gündemi Dergisi, S.4, (Temmuz) 2020, s.5, dn.3, https://www.kanunum.com/dergiler/finans-hukuku-gundemi-dergisi/sayi-4-temmuz-2020#.YatdktBBzIV, Erişim Tarihi: 30.11.2021; Tevetoğlu, s.36.

[10] Çamoğlu, s.34; Tevetoğlu, s.36-37, dn.10.

bu düşünceden hareketle çek gibi bononun da teknolojik gereksinimlere cevap verecek tarzda yeniden dizayn edilmesine olanak sağlamıştır. Böylece her iki senet türüne ilişkin mevzuat teknolojiyle uyumlu hale getirilmiş olacaktır. Fakat söz konusu kanun teklifinin amacı bununla sınırlı değildir. Teklif yasalaştığında bono ve çekin elektronik ortamda düzenlenmesi, devredilmesi ve ödenmesi mümkün olacak, böylece her iki senede ilişkin sahtecilik ve kayıt dışılık gibi olumsuzluklar büyük oranda engellenebilecek, bu da ülke piyasalarındaki ödeme ve kredi fonksiyonlarının güvenli biçimde işlemesini temin edecektir[11].

Genel perspektifini kısaca çizmeye çalıştığımız elektronik bono ve çek düzenlemesi ile esasında bono ve çekin kambiyo senedi ve kıymetli evrak niteliğinin değiştirilmesi söz konusu değildir. Fakat bazı unsur ve özelliklerinin teknolojik yeniliklerle uyumlaştırılması gereklidir. Bunlardan biri de imza unsurudur. Bilindiği gibi kambiyo senetleri sıkı biçimde şekle bağlı senetlerdir. Bu senetlerde hangi unsurların bulunması gerektiği Türk Ticaret Kanunu'nda belirtilmiş olup, bunlardan birinin eksikliği senedin kambiyo senedi niteliğini kazanmasına engel olur[12]. Bu unsurlardan biri de imzadır ve imzanın el yazısı ile atılması senedin geçerlilik şartıdır (TTK.756/1). Poliçeye ilişkin bu düzenleme bono ve çeke de atfen uygulanacaktır (TTK.778/1-i; 818/1-r). Ayrıca yukarıda bahsettiğimiz üzere TTK.1526/1 uyarınca poliçe, bono, çek, makbuz senedi, varant ve kambiyo senetlerine benzeyen senetlerin hem düzenlenmesinde hem de senetlere ilişkin kabul, aval, ciro gibi işlemlerin yapılmasında güvenli elektronik imzaya izin verilmemiştir. Elektronik Çek ve Bono Kanunu Teklifinde ise güvenli elektronik imza veya elektronik kimlik doğrulama yöntemleri öngörülerek bono ve çekteki bu el yazısı ile imzaya ilişkin şekil şartının değiştirildiğini açıkça görmekteyiz.

Bu kapsamda mevcut yasal düzenlemelerde birtakım değişiklikler gerekecektir. TTK ile 5941 sayılı Çek Kanunu'nda öngörülen unsurlar arasında ıslak imzanın istisna tutulması, TTK.1526/1'de güvenli elektronik imza ile düzenlenemeyecek senetler arasından bono ve çekin çıkarılması, el yazısıyla imzaya dair bono ve çeke atfen uygulanacak TTK.756 hükmünün revize edilmesi gerekecektir[13]. Burada dikkat çekmek istediğimiz son bir nokta ise, güvenli elektronik imza dışında elektronik kimlik doğrulama yöntemlerinin de elektronik bono ve çek bakımından uygulanabilecek olmasıdır. Ancak bu uzaktan kimlik doğrulama uygulamalarında birtakım hileli işlemler, teknik altyapının yurt dışı kaynaklı şirketlerce

[11] Tevetoğlu, s.37.
[12] Pulaşlı, s.118-119; Öztan, s.68; Ülgen/ Helvacı/ Kaya/ Nomer Ertan, 105; Bozer, Ali/ Göle, Celal, Kıymetli Evrak Hukuku, 9. Baskı, Ankara, 2020, s.65.
[13] Demirci, Serdar, "Türk Hukukunda Elektronik Çeke Doğru, Dünü ve Bugünüyle Çek", Ankara Barosu Dergisi, C.78, S.3, 2020, s.38.

sağlanmasına bağlı olarak, finansal veri ve işlem güvenliği bakımından sorunlar yaşanması kuvvetle muhtemeldir[14]. Dolayısıyla bu riskler ve sorunlara ilişkin gerekli teknik ve yasal altyapı oluşturuluncaya kadar, elektronik bono ve çek için ilk etapta sadece güvenli elektronik imza ile düzenlenme, devir ve diğer işlemlerin gerçekleştirilmesi gerekir, kanaatindeyiz[15].

2.2. Elektronik İbraz Başlangıç Tarihi

Elektronik Çek ve Bono Kanunu Teklifi ile elektronik çeke özgü olarak karşımıza çıkan yeni bir özellik elektronik ibraz başlangıç tarihidir. Ancak burada öncelikle elektronik çek kavramını ele almakta fayda vardır: "Elektronik çek, kağıt çeklerle birlikte yapılandırılan, çok iyi geliştirilmiş yasal alt yapısı ve iş süreçleriyle benzer bütün elektronik işlemlerin verimliliğini, hızını ve güvenliğini birleştiren yeni bir ödeme aracı" olarak tanımlanmaktadır[16]. Bir diğer ifadeyle elektronik çek, kağıtsız ve sayısal bir imza[17] ile taahhütte bulunulan güvenli bir banka ödeme aracıdır ve ödemenin banka hesabından elektronik fon transferi yoluyla bir kerelik yapıldığı bir sistem üzerine kuruludur[18]. Yani esasında elektronik çek, kağıt çekteki ıslak imza yerine anahtar kriptolu imza ve elektronik ortamda oluşturulan belgelerle yürütülen güvenli elektronik işlem temeline dayalıdır[19]. Elektronik Çek ve Bono Kanunu Teklifinde de bu işlemler için hem bankalar bünyesinde hem de banka sistemlerinin birbiriyle entegrasyonunu sağlamak üzere Elektronik Çek ve Bono Sistemi (ÇEBİS) kurulması öngörülmüştür[20].

Söz konusu sistem, elektronik bono ve çeklerin düzenlenmesi, cirosu, avali, elektronik ibrazı, iptali, haczi ve diğer tüm işlemlerin yapılabileceği, gerek tüm bankalar gerekse sistem işleticisi konumundaki Bankalar Birliği bünyesinde kurulmuş olan tüm sistemlerin bütününü ifade etmektedir[21]. İşte bu sistemde gerçekleştirilecek ve elektronik çeke özgü kavram olan elektronik ibraz, çekin ödenmek üzere ÇEBİS veya takas sistemi[22]

[14] karş. Tevetoğlu, s.61-62 ve dn.71; Demirci, s.39.
[15] bkz. ve karş. Tevetoğlu, s.61-62.
[16] Karabıyık, Ayşegül, "Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek)-1", Muhasebe ve Finansman Dergisi, S.38, 2008, s.81.
[17] Sayısal imza (digital signature); "imzalayana onay garantisi sağlayan, dökümanların veri bütünlüğünü oluşturan ve işlemlerin inkar edilmesine karşılık bir kanıt olan şifrelemeyle ilgili süreçtir. Sayısal imza elle atılan imzanın sayısallaştırılmış hali değildir. Sayısal imzalar açık anahtarlı kriptografi kullanır ve sertifikalarla birlikte çalışır. Sertifikayla birlikte sayısal imzalar imzalanan belgeleri resmen onaylayabilir ve alınan mesajın değiştirilmediğini garanti eder", Karabıyık, Ayşegül, "Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek)-2", Muhasebe ve Finansman Dergisi, S.39, 2008, s.157.
[18] Karabıyık, "E-Çek-1", s.82.
[19] Karabıyık,"E-Çek-2", s.156 vd.
[20] "Çek ve Bonoda Elektronik Dönem Başlıyor", https://www.esin.av.tr/tr/2019/05/03/cek-ve-bonoda-elektronik-donem-basliyor, Erişim Tarihi: 01.12.2021.
[21] Çotuksöken, s.2; Tevetoğlu, s.52.
[22] Çek takas sistemi, elektronik çeke geçiş sürecindeki önemli basamaklardan birini oluşturan ve Takasbank (İstanbul Takas ve Saklama Bankası Anonim Şirketi) nezdinde yürütülmekte olan sistemi ifade etmektedir. Sistemin işleyişi 02.07.2018'de yürürlüğe giren Çek Takas Faaliyetleri Hakkında Yönetmelik hükümleri

(takas odaları aracılığıyla) elektronik ortamda muhatap bankaya ibrazı demektir (TTK.798)[23]. Elektronik ibraz başlangıç tarihi ise, "elektronik çek düzenlenirken belirlenen ve hamilin çeki bankaya ibraz edebileceği en erken tarihi" ifade eder. Bunun anlamı aslında hamilin, çekte düzenleyen tarafından belirlenen bu başlangıç tarihinden önce ödenmek için çeki bankaya ibraz edememesidir. Dolayısıyla bu durumda elektronik çek bakımından karşımıza çıkan yeni bir "ileri tarihli veya vadeli çek" türü söz konusu olmaktadır[24].

2.3. Onay (Senet Zilyetliğinin Devri)

Onay, elektronik bono ve çekin lehdar veya ciro edilen tarafından elektronik ortamda zilyetliğinin devralınması işlemidir[25]. Örneğin elektronik çekte lehdar, hesabının bulunduğu herhangi bir banka sistemi aracılığıyla, elektronik ibraz başlangıç tarihine kadar onay verebilecektir. Onay zilyetliğin devri niteliğinde sayılacak ve bu işlemle birlikte çek geriye yönelik olarak düzenlenmiş kabul edilecektir. Lehdarın onayı olmaksızın çekin düzenlenmiş sayılması veya devri söz konusu olmayacaktır[26]. Bu durum fiziki çek ve bonoda hak ve senet arasındaki sıkı bağlılık unsurunun beraberinde getirdiği "senet zilyetliğinin devri" veya "senedin teslimi" olarak adlandırdığımız zorunlu devir koşulunu farklı bir konsepte dönüştürmüştür. Zira burada kağıt bono ve çeklerden farklı olarak, onay işlemi ile ciro alan veya devralan iradesini aktif olarak ortaya koymaktadır[27]. Ayrıca kanun teklifinde düzenleyenin henüz onaylanmamış bir bono veya çeki belli bir süre içinde değiştirmesi veya geri almasına cevaz verilmiştir. Bu aşamada temel ilişkiden kaynaklı problemler oluşması ihtimal dahilindedir. O nedenle düzenleyenin onay verilmeyen senedin içeriğini değiştirmesi veya geri alması için öngörülecek sürenin kısa tutulması ve tarafların karşılıklı anlaşmasıyla geri çekme veya iptalin söz konusu olması, daha uygun bir çözüm yolu gibi durmaktadır[28].

2.4. Tek Tip İbraz Süresi ve Tek Tip Vade

Elektronik bono ve çek bakımından başka bir değişen özellik de ibraz süresi ve vadeye ilişkin olarak karşımıza çıkmaktadır. Kanun teklifinde elektronik çek için 10 günden

çerçevesinde yürütülmektedir. Anılan yönetmeliğe göre takas işlemi, "5411 sayılı Bankacılık Kanunu'na tabi bankalar ve T.C. Merkez Bankası'ndan oluşan katılımcılara ve çekin düzenlendiği hesabın bulunduğu bankalardan oluşan muhatap katılımcılara ait çeklere ilişkin bilgilerin elektronik ortamda takas odasına iletilmesi, provizyon alınmasına aracılık edilmesi ve netleştirme işlemi" olarak tanımlanmıştır. Takas odaları ise, banka veya diğer finansal kuruluşlarda bulunan çek ve benzeri ödeme araçlarından doğan borç ve alacakları, nakit para kullanmaksızın muhasebe işlemleriyle karşılıklı biçimde tasfiye eden birimlerdir (Demirci, s.27-28).

[23] Demirci, s.38.
[24] Tevetoğlu, s.54.
[25] Tevetoğlu, s.54-55.
[26] Çotuksöken, s.3.
[27] Tevetoğlu, s.55.
[28] Çotuksöken, s.3.

oluşan tek bir ibraz süresi[29] ve elektronik bono için de belirli vade şeklinde oluşturulması gereken tek tip bir vade öngörülmektedir. Kanun teklifi genel gerekçesinde bunun nedeni olarak çek ve bono kullanımının basitleştirilmesi gösterilmektedir. Kanaatimizce de ibraz süresi ve vade unsurları bakımından sadeleştirmeye gidilmesi, teknolojik gereksinimlere uyumlu bir yasal düzenleme yapılması amacıyla da örtüşmektedir[30].

2.5. Tam Ciro ve Temlik Cirosu Zorunluluğu

Elektronik bono ve çekte ciro işlemi, lehine ciro edilen kişi ve ciro türü belirtilmek suretiyle ciro edenin hesabının bulunduğu banka sistemi üzerinden gerçekleştirilecektir. Ciro türünün belirtilmediği durumda da "temlik cirosu" olacağı öngörülmektedir[31]. Kanun teklifindeki bu düzenleme elektronik çek ve bonoda sadece tam cironun mümkün olduğunu, beyaz ciro veya çek bakımından da hamiline yazılı çek düzenleme imkânı bulunmadığını göstermektedir[32]. Ancak elektronik bono ve çekin cirosu bakımından getirilen bu düzenlemenin, tüm işlem basamaklarının elektronik ortamda takibini sağlama ve işlem güvenliği bakımından bilgilerin kayıt altına alınması gerekliliği ile fiziki bono ve çeklerin kolay tedavülünde önemli iki unsur olarak öne çıkan beyaz ciro ve hamiline çek uygulaması arasında daha dengeli bir çözüme kavuşturulması gerektiğini düşünmekteyiz[33]. Zira beyaz ciro veya hamiline yazılı senet uygulaması fiziki bono ve çeklerde sadece tedavülü hızlandırmakla kalmayıp, senet dolayısıyla söz konusu olabilecek başvuru hakkı bakımından sorumluluk zincirine dahil olmamayı ve böylece tercih edilebilirliği artırmaktadır. Bu durumun elektronik bono ve çeklerde zaten gündeme gelebilecek finansal veri ihlalleri sorununu da derinleştirme riski bir tarafa, elektronik bono ve çek bakımından cirantaların sorumsuzluk kaydı koyup koyamayacakları hususu net olarak ortaya konulmadıkça, tedavül hacminin genişlemesi sağlanamayacaktır.

2.6. Seri Numarası ve Karekod

Çek bakımından zaten aranılan bir unsur olan seri numarası ve karekod[34], kanun teklifiyle birlikte elektronik bonolar için de zorunlu hale gelmektedir. Böylece elektronik bonoların çeklerde olduğu gibi banka sistemi aracılığıyla düzenleneceği, ödemenin seri

[29] İbraz süresi, elektronik ibraz başlangıç tarihini izleyen 10 gündür.
[30] Tevetoğlu, s.55.
[31] Çotuksöken, s.4.
[32] Baytemür, Deniz, Elektronik Kambiyo Senetleri, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2020, s.123-124.
[33] Elektronik senetlerde beyaz cironun mümkün olmaması halinde, bunların fiziki senetlere göre daha dezavantajlı bir durumda olacağına ilişkin görüş için bkz. Baytemür, s.141.
[34] 6728 sayılı Yatırım Ortamının İyileştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılmasına İlişkin Kanun (RG: 09.08.2016, S.29796) m.70 hükmü ile TTK.780'de düzenlenen çekin şekli unsurları arasına "banka tarafından verilen seri numarası" ve "karekod" unsurları da eklenmiştir (f.1-g, h). Karekod unsuruna ilişkin olarak Çeklerde Karekod Uygulamasına ilişkin Tebliğ (RG: 31.12.2016, S.29935, 3. Mükerrer) de yayımlanmıştır.

numarası belirtilmek suretiyle bankaya yapılacak ibrazla talep edileceği anlaşılmaktadır[35]. Aynı şekilde yine çeklerde olduğu gibi tedavül güvenliği amacıyla bonoların da karekodlu olarak düzenlenme zorunluluğu getirilmektedir. Karekod sayesinde alacaklı düzenleyenin ödeme geçmişini kontrol ederek bonoyu kabul edip etmeyeceği kararını sağlıklı biçimde verebilmiş olacaktır. Kanun teklifinde, belirli bir tarih öncesindeki bonolar bakımından karekod olmamasının geçerliliği etkilemeyeceği isabetli olarak belirtilmiştir. Ancak teklifin yasalaşmasıyla birlikte tıpkı çeklerde olduğu gibi karekod olmaksızın bono düzenlemenin artık mümkün olamayacağı anlaşılmaktadır[36]. Seri numarası ve karekod gibi unsurların elektronik bono için de öngörülmesi, bononun uygulaması en çok olan kambiyo senedi vasfı nedeniyle yerinde bir düzenleme olmuş, bir kredi aracı olarak ticari işlemlerde daha güvenilir bir şekilde kullanımına zemin hazırlamıştır.

2.7. Düzenleme ve Ödeme Yeri

Elektronik bonolar bakımından, TTK.776'da düzenlenen ve bononun unsurları arasında sayılan "düzenleme yeri" ve "ödeme yeri"nin (f.1-d, f) de artık unsurlar arasında bulunmayacağını söylemek yanlış olmayacaktır. Zira elektronik bononun banka sistemi üzerinden elektronik ortamda düzenlenerek yetkili hamilin banka hesabına ödenmesi söz konusudur. Bu durum elektronik hale dönüşen bonolarda artık fiziksel mekân bildiren kayıtların kullanılması gereğini ortadan kaldıracaktır[37].

3. SONUÇ

Teknolojik gelişmelerle birlikte ticaret hayatı da bundan nasibini almış, finansal piyasalarda teknolojinin getirdiği pek çok yenilikçi ve rekabetçi araçlar, ürünler, modeller ortaya çıkmaya başlamıştır. Elektronik ve sanal para, kripto varlıklar, dijital ödeme sistemleri ve araçları, blok zincir teknolojisi gibi baş döndürücü gelişmeler karşısında, ticaret hayatında kambiyo senetleri adı verilen ve esasında uygulaması son derece yoğun olan klasik ödeme ve kredi araçları olarak karşımıza çıkan senetlerin de teknolojiyle buluşmasını zorunlu kılmıştır. Bu amaçla Ticaret Bakanlığı öncülüğünde 2015 yılından beri yürütülen çalışmalara dayanan Elektronik Çek ve Bono Kanunu Teklifi hazırlanarak kısa sürede yasalaşması için adımlar atılmaya devam edilmektedir. Biz de çalışmamızda bu kanun teklifiyle elektronik bono ve çekte, anılan senetlerin kıymetli evrak ve kambiyo senedi niteliğine bağlı unsur ve özellikler açısından öngörülen değişiklikleri, olumlu ve olumsuz yönleriyle ortaya koymayı amaçladık.

[35] Tevetoğlu, s.67-68
[36] Tevetoğlu, s.44-45 ve dn.33.
[37] Baytemür, s.174.

Genel perspektif olarak baktığımızda, elektronik bono ve çek düzenlenmesi yoluyla sahteciliğin önüne geçilmesi, imza taklidi vb. gibi dolandırıcılıklar yapılarak bono ve çekin çalınması, kaybedilmesi gibi olumsuzluklar giderilecek; kredi ve ödeme pazarı için hayati önemi bulunan bu iki senedin teknolojiyle uyumu sağlanmış olacak ve düzenlenme aşamasından ödemeye kadar tüm tedavül basamaklarının elektronik ortamda izlenebilmesi nedeniyle de kayıt dışılığın önüne geçilmiş olacaktır.

Ayrıca kanun teklifiyle kurulması öngörülen Elektronik Çek ve Bono Sistemi aracılığıyla çek düzenleyenlerin tüm çekleri sayı ve tutar olarak lehdar ve cirantalar tarafından görülebilecek ve düzenleyenin bir çeki karşılıksız çıktığında, bu sisteme entegre olan tüm bankaların bu kimsenin henüz düzenlemediği diğer tüm çek kayıtlarını iptal edebilmelerinin de önü açılmış ve çek alacaklılarının korunması sağlanmıştır. Böylece fiziki çeklerde karşılıksızlıkla ilgili doğabilecek sorunların elektronik çekte minimize edildiğini görmekteyiz[38]. Tüm bu olumlu yönleri destekleyici kambiyo senedi özellikleri olarak güvenli elektronik imza, onay, tek tip ibraz süresi ve tek tip vade ve çekte zaten söz konusu olup elektronik bono için getirilen seri numarası ve karekod unsurlarını zikredebiliriz. Ancak senet zilyetliğinin devrini ifade eden onay aşaması bakımından, düzenleyenin onay verilmeyen senedin içeriğini değiştirmesi veya geri alması için öngörülecek sürenin kısa tutulması ve tarafların karşılıklı anlaşmasıyla geri çekme veya iptalin söz konusu olması şeklinde bir yaklaşımın daha uygun olacağını belirttik. Bir de elektronik bono ve çekte sadece tam cironun mümkün olup beyaz ciroya ve çek bakımından hamiline düzenlemeye izin verilmemesi hususunun yeniden gözden geçirilmesi gerektiğini düşünüyoruz.

KAYNAKÇA

Bahtiyar, Mehmet, *Kıymetli Evrak Hukuku*, 18. Baskı, İstanbul, 2020.

Baytemür, Deniz, *Elektronik Kambiyo Senetleri*, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2020.

Bozer, Ali/ Göle, Celal, *Kıymetli Evrak Hukuku*, 9. Baskı, Ankara, 2020.

Çamoğlu, Ersin, *Kıymetli Evrak Hukukunun Temel İlkeleri*, 1. Baskı, İstanbul, 2020.

Çotuksöken, S. Emre, "Dijitalleşme, Elektronik Çek ve Blockchain İlişkisi", Finans Hukuku Gündemi Dergisi, S. 4, (Temmuz) 2020, https:// www.kanunum.com / dergiler / finans-hukuku-gundemi-dergisi/sayi-4-temmuz-2020#.YatdktBBzIV, (Erişim Tarihi: 30.11.2021).

[38] Tevetoğlu, s.43-44.

Demirci, Serdar, "Türk Hukukunda Elektronik Çeke Doğru, Dünü ve Bugünüyle Çek", Ankara Barosu Dergisi, C.78, S.3, 2020, s.1-47.

Karabıyık, Ayşegül, "Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek)-1", Muhasebe ve Finansman Dergisi, S.38, 2008, s.80-94.

Karabıyık, Ayşegül, "Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek)-2", Muhasebe ve Finansman Dergisi, S.39, 2008, s.155-166.

Öztan, Fırat, *Kıymetli Evrak Hukuku*, 24. Baskı, Ankara, 2020.

Pulaşlı, Hasan, *Kıymetli Evrak Hukukunun Esasları*, 8. Baskı, Ankara, 2020.

Tevetoğlu, Mete, "Elektronik Çek ve Bono Kanunu Teklifi İle Yapılması Planlanan Düzenlemelere Dair Düşünceler", Bilişim Hukuku Dergisi, S.1, 2021, s.31-75.

Ülgen, Hüseyin/ Helvacı, Mehmet/ Kaya, Arslan/ Nomer Ertan, N. Füsun, *Kıymetli Evrak Hukuku*, 13. Baskı, İstanbul, 2021.

İnternet Kaynakları

1) "Çek ve Bonoda Elektronik Dönem Başlıyor", https://www.esin.av.tr/tr/2019/05/03/cek-ve-bonoda-elektronik-donem-basliyor, (Erişim Tarihi: 01.12.2021).

2) "2021'de çek-bonoya elektronik sistem getirilmesi planlanıyor", https:// www.bloomberght.com/2021-de-cek-bonoya-elektronik-sistem-getirilmesi-planlaniyor-2269211, (Erişim Tarihi: 01.12.2021).

CİNSEL SALDIRIDA ADLİ HEMŞİRENİN ROLLERİ

Tuğçe Biter

Üsküdar Üniversitesi , 0000-0001-09165-7291

ÖZET

Cinsel saldırı, cinsel davranışlarla bir kimsenin vücut dokunulmazlığının ihlâl edilmesi durumudur. Risk altındakiler çoğunlukla kadınlar ve çocuklardır. Uluslararası Adli Hemşireler Birliği (IAFN) cinsel saldırı muayene hemşiresini (SANE- Sexual assault nurse examiner) adli hemşireliğin rolleri arasında tanımlamıştır. Sağlık personelinin yeterli eğitim ve tecrübesi olmadığından dolayı tam bir adli vaka muayenesi yapılamıyor olması SANE eğitim programına olan ihtiyacı doğuran nedenler arasındadır. Adli hemşireler, cinsel saldırı kurbanlarının daha ayrıntılı ve hassas biçimde muayene edilmelerini sağlarlar. Cinsel saldırı kurbanlarının ihtiyaç duyduğu; fiziksel değerlendirme, adli muayene, kanıtların toplanması, cinsel yolla bulaşan hastalıklara yönelik testler ve tedavi, destekleme amaçlı öneriler, adli rapor yazımı ve mahkemede tanıklığı içeren acil bakımı sağlamak için gerekli bilgilere sahip olmalıdır. Acil servisler hastane içerisinde adli vakaların en sık görüldüğü yerlerdir. Acil hemşireleri adli vakayı ilk gören, ilk konuşan ve laboratuvar örnekleri ile ilk ilgilenen sağlık çalışanları oldukları için adli vakalar ve olası adli deliller konusunda dikkatli ve hassas davranmalıdırlar. Hemşirenin önceliği hastanın bakım ve tedavisidir, bu görevlerini yerine getirirken kanıta zarar vermemeye özen göstermeli, kanıtların toplanması, saklanması ve kayıt edilmesini bilmelidir. Yurtdışında olduğu gibi ülkemizde de cinsel saldırı muayene hemşireliği alanında yapılacak eğitimler ve bu kişilerin acil servislerde görev almalarının sağlanması, cinsel saldırıya uğrayan bireylerin tanı, tedavi ve bakım süreçleri ve adli işlemlerdeki işleyişi kolaylaştıracaktır.

Anahtar Kelimeler. Adli Hemşirelik – Cinsel Saldırı – Adli Vaka

LEGAL DOCTRINE ON RYLANDS V. FLETCHER: ONE MORE TIME ON FEASIBILITY OF A GENERAL CLAUSE OF STRICT LIABILITY IN THE UK

Maria Lubomira Kubica

Universidad Loyola Andalucia - Spain

Abstract:

The paper reveals the birth and evolution of the British precedent *Rylands v. Fletcher* that, once adopted on the other side of the Ocean (in United States), gave rise to a general clause of liability for abnormally dangerous activities recognized by the §20 of the American Restatements of the Law Third, Liability for Physical and Emotional Harm. The main goal of the paper was to analyze the development of the legal doctrine and of the case law posterior to the precedent together with the intent of the British judicature to leapfrog from the traditional rule contained in *Rylands v. Fletcher* to a general clause similar to that introduced in the United States and recently also on the European level. As it is well known, within the scope of tort law two different initiatives compete with the aim of harmonizing the European laws: European Group on Tort Law with its Principles of European Tort Law (hereinafter PETL) in which article 5:101 sets forth a general clause for strict liability for abnormally dangerous activities and Study Group on European Civil Code with its Common Frame of Reference (CFR) which promotes rather ad hoc model of listing out determined cases of strict liability. Very narrow application scope of the art. 5:101 PETL, restricted only to abnormally dangerous activities, stays in opposition to very broad spectrum of strict liability cases governed by the CFR. The former is a perfect example of a general clause that offers a minimum and basic standard, possibly acceptable also in those countries in which, like in the United Kingdom, this regime of liability is completely marginalized.

Keywords: Abnormally dangerous activities, general clause, Rylands v. Fletcher, strict liability.

DISTINCTIVE FEATURES OF LEGAL RELATIONS IN THE AREA OF SUBSOIL USE, RENEWAL AND PROTECTION IN UKRAINE

NADIIA MAKSIMENTSEVA

Oles Honchar Dnipropetrovsk National University, Ukraine

Abstract:

The issue of public administration in subsoil use, renewal and protection is of high importance for Ukraine since it is strongly linked to energy security of the state as well as it shall facilitate the people of Ukraine to efficiently implement its propitiatory rights towards natural resources and redistribution of national wealth. As it is stipulated in the Article 11 of the Subsoil Code of Ukraine (the Code) the authorities that administer the industry are limited to central executive bodies and local governments. In particular, it is stipulated in the Code that the Ukraine's Cabinet of Ministers carries out public administration in geological exploration, production and protection of subsoil. Other state bodies of public administration include central public authority responsible for state environmental protection policies; central public authority in charge of implementation of state geological exploration and efficient subsoil use policies; central authority in charge of state health and safety control policies. There are also public authorities in the Autonomous Republic of Crimea; local executive bodies and other state authorities and local self-government authorities in compliance with laws of Ukraine. This article is devoted to the analysis of the legal relations in the area of public administration of subsoil use, renewal and protection in Ukraine. The main approaches to study the essence of legal relations in the named area as well as its tasks, functions and methods are analyzed. It is concluded in this article that legal relationship in the field of public administration of subsoil use, renewal and protection is characterized by specifics of its task (development of natural resources).

Keywords: Legal relations, public administration, Subsoil Code of Ukraine, subsoil use, renewal and protection.

A METHOD TO ENHANCE THE ACCURACY OF DIGITAL FORENSIC IN THE ABSENCE OF SUFFICIENT EVIDENCE IN SAUDI ARABIA

Fahad Alanazi

De Montfort University

Andrew Jones

University of Hertfordshire - UK

Abstract:

Digital forensics seeks to achieve the successful investigation of digital crimes through obtaining acceptable evidence from digital devices that can be presented in a court of law. Thus, the digital forensics investigation is normally performed through a number of phases in order to achieve the required level of accuracy in the investigation processes. Since 1984 there have been a number of models and frameworks developed to support the digital investigation processes. In this paper, we review a number of the investigation processes that have been produced throughout the years and introduce a proposed digital forensic model which is based on the scope of the Saudi Arabia investigation process. The proposed model has been integrated with existing models for the investigation processes and produced a new phase to deal with a situation where there is initially insufficient evidence.

Keywords: Digital forensics, Process, Metadata, Traceback, Saudi Arabia.

ENFORCEMENT OF DECISIONS OF OMBUDSMEN AND THE SOUTH AFRICAN PUBLIC PROTECTOR: MUZZLING THE WATCHDOGS

Roxan Venter

University of Johannesburg – South Africa

Abstract:

Ombudsmen often face the challenge of a lack of authority to have their decisions and recommendations enforced. This lack of authority may be seen as one of the major obstacles in the way of the effectiveness of the institutions of Ombudsman and also the South African Public Protector. The paper will address the current legal position in South Africa with regard to the status of the decisions and recommendations of the South African Public Protector and the enforcement thereof. In addition, the paper will compare the South African position with the experiences of other jurisdictions, including Scandinavian countries like Sweden, Denmark and Norway, but also New Zealand and Northern Ireland, with regard to the enforcement of the decisions of Ombudsmen. Finally, the paper will make recommendations with regard to the enhancement of the power and authority of Ombudsmen in order to effectively enforce their decisions. It is submitted that the creation of the office of Ombudsman, and the Public Protector in the South African system, is an essential tool to ensure the protection of society against governmental abuse of power and it is therefore imperative to ensure that these watchdogs of democracy are not muzzled by a lack of powers of enforcement.

Keywords: Enforcement of decisions of Ombudsmen, Governmental control, Ombudsman, South African Public Protector.

THE ROLE OF THE ACCUSED'S ATTORNEY IN THE CRIMINAL JUSTICE SYSTEM OF IRAN, MASHHAD 2014

MAHDI KARIMI

Payame- E- Noor University – Iran

Abstract:

One of the most basic standards of fair trial is the right to defense, hire an attorney and its presence in the hearing stages. On the one hand, based on the reason and justice, as the legal issues, particularly criminal affairs, become complicated, the accused must benefit from an attorney in the court in order to defend itself which requires legal knowledge. On the other hand, as the judicial system has jurists such as investigation judges at its disposal, the accused must enjoy the same right to defend itself and reject allegations so that the balance is maintained between the litigating parties based on the principle of "equality of arms". The right to adequate time and facilities for defense is cited among the principles and rights relevant to the proceedings in international regulations such as the International Covenant on Civil and Political Rights. The innovations made in the Code of Criminal Procedure in 2013 guaranteed the presence of the accused's attorney in the proceedings. The present study aims at assessing the result of the aforementioned guarantee in practice and made attempts to investigate the effect of the presence of accused's attorney on reducing the punishment by asking the question and addressing the statistical population of this study including 48 judges of lower courts and courts of appeal. It seems that in despite of guarantees provided in the new Code of Criminal Procedure, Iran's penal system, does not tolerate the presence of an attorney in practice.

Keywords: Defense attorney, equality of arms, fair trial, reducing the penalty, right to defense.

DEPENDENCY THEORY ON EXAMINING THE RELATIONSHIP BETWEEN THE UNITED STATES AND THE MIDDLE EAST: IN THE CASE OF IRAN, SAUDI ARABIA, AND TURKEY

Abdelhafez Abdel Hafez

Faculty of Law and Political Sciences, Szeged, Hungary

Abstract:

Dependency theory was developed since 1950s, with economic concerns. It divided the world into two parts, the states of the peripheral (third world countries) and the states of the core (the developed capitalist countries). Another perspective developed to the theory with the implementation of the idea of semi-peripheral states in the new world order. With these divisions (core, peripheral, semi-peripheral) this study aims to develop a concept from the perspective of dependency theory, to understand the nature of the relationship of the U.S. with the Middle East Regions through its relation with Iran, Saudi Arabia, and Turkey. The tested countries (Saudi Arabia, Iran and Turkey) are seeking a foothold and influential role in the region. The paper argued that the U.S. directs its policies toward the region, in the way to guarantee no country of the region will be in semi-peripheral level (that could create competitions or danger on the U.S. interest). Therefore, U.S. policies in the region have varied from declaring war to diplomatic channels and sometimes ignoring. The paper is based on the dependency theory, and other international relations theories used to study the Middle East in the international context.

Keywords: Dependency, hegemony, imperialism, Middle East.