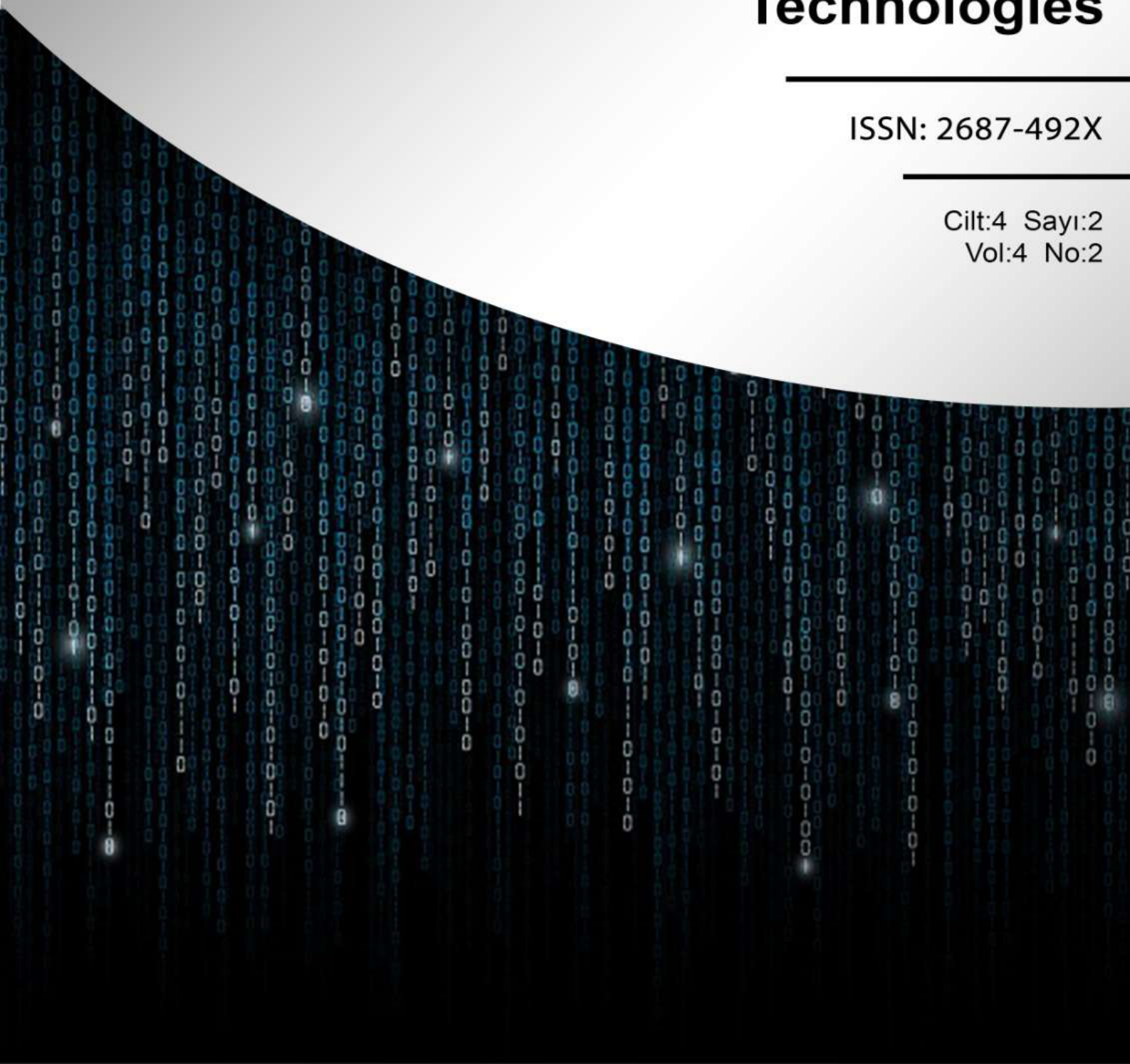
Bilgi ve İletişim Teknolojileri Dergisi

Journal of Information and Communication Technologies

ISSN: 2687-492X

Cilt:4 Sayı:2
Vol:4 No:2



BİLGİ VE İLETİŞİM TEKNOLOJİLERİ DERGİSİ

JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

ULUSLARARASI HAKEMLİ DERGİ / INTERNATIONAL REFEREED JOURNAL

Volume/Cilt: 4, Issue/Sayı: 2, 2022

Contact
Journal of Information and Communication Technologies
e-mail: bilgiveiletisimdergisi@gmail.com

Journal of Information and Communication Technologies; is an **online, open access, free international peer-reviewed** journal published in Turkish or English.

İletişim
Bilgi ve İletişim Teknolojileri Dergisi
e-posta: bilgiveiletisimdergisi@gmail.com

Bilgi ve İletişim Teknolojileri Dergisi; araştırma ve derleme çalışmalarını Türkçe veya İngilizce olarak **çevrimiçi** yayımlanan, **açık erişime sahip, ücretsiz, uluslararası hakemli** bir dergidir.

Index List / Dizin Listesi

Google Scholar, Index Copernicus, Asos Index, CiteFactor, J-Gate, ESJI Index, Directory of Research Journal Indexing, Academic Resource Index, ROAD, Türk Eğitim İndeksi, Rootindexing, Journals Directory, Journal Factor, International Servicesfor Impact Factor and Indexing (ISIFI), The Scientific Literature Database, Akademik Dokümanlar Dizini (Index of Academic Documents [IAD])

BİLİM KURULU / EDITORIAL BOARD

4. CİLDİN HAKEMLERİ / REVIEWERS OF THE 4th VOLUME

Prof. Dr. Gül KALELİ YILMAZ
Prof. Dr. Recep ÇAKIR
Doç. Dr. Agah Tuğrul KORUCU
Doç. Dr. Gökhan DAĞHAN
Doç. Dr. Hatice YILDIZ DURAK
Doç. Dr. Mehmet KARA
Doç. Dr. Hüseyin POLAT
Doç. Dr. Mustafa YAĞCI
Doç. Dr. Nezih ÖNAL
Doç. Dr. Ramazan YILMAZ
Doç. Dr. Şahin GÖKÇEARSLAN
Doç. Dr. Volkan KUKUL
Dr. Öğr. Üyesi Ahmet Berk ÜSTÜN
Dr. Öğr. Üyesi Çağla ÖZEN
Dr. Öğr. Üyesi Erdem ERKAN
Dr. Öğr. Üyesi Evrim GÜLER
Dr. Öğr. Üyesi Eyüp Burak CEYHAN
Dr. Öğr. Üyesi Fatih ERDOĞDU
Dr. Öğr. Üyesi Gökhan DEMİRASLAN
Dr. Öğr. Üyesi Harun ÇİĞDEM
Dr. Öğr. Üyesi Mehmet Fikret GELİBOLU
Dr. Öğr. Üyesi Seyfullah GÖKOĞLU
Dr. Hüseyin ATEŞ

Prof. Dr. Gül KALELİ YILMAZ
Prof. Dr. Recep ÇAKIR
Assoc. Prof. Dr. Agah Tuğrul KORUCU
Assoc. Prof. Dr. Gökhan DAĞHAN
Assoc. Prof. Dr. Hatice YILDIZ DURAK
Assoc. Prof. Dr. Mehmet KARA
Assoc. Prof. Dr. Hüseyin POLAT
Assoc. Prof. Dr. Mustafa YAĞCI
Assoc. Prof. Dr. Nezih ÖNAL
Assoc. Prof. Dr. Ramazan YILMAZ
Assoc. Prof. Dr. Şahin GÖKÇEARSLAN
Assoc. Prof. Dr. Volkan KUKUL
Assist. Prof. Dr. Ahmet Berk ÜSTÜN
Assist. Prof. Dr. Çağla ÖZEN
Assist. Prof. Dr. Erdem ERKAN
Assist. Prof. Dr. Evrim GÜLER
Assist. Prof. Dr. Eyüp Burak CEYHAN
Assist. Prof. Dr. Fatih ERDOĞDU
Assist. Prof. Dr. Gökhan DEMİRASLAN
Assist. Prof. Dr. Harun ÇİĞDEM
Assist. Prof. Dr. Mehmet Fikret GELİBOLU
Assist. Prof. Dr. Seyfullah GÖKOĞLU
Dr. Hüseyin ATEŞ

CONTENT / İÇİNDEKİLER

CONTENT / İÇİNDEKİLER

2022

4(2), 128-142

VarioGram – Zaman Serileri İçin Renkli Bir Zaman-Graf Temsili

İlker Türker[1], Serkan Aksu*[2]

Anahtar Sözcükler

Graf temsili
Ses sınıflandırma
Zaman serilerinin sınıflandırılması
Karmaşık ağlar

Makale Hakkında

Gönderim Tarihi
20 Eylül 2022
Kabul Tarihi
03 Kasım 2022
Yayın Tarihi
28 Aralık 2022
Makale Türü
Araştırma Makalesi

Öz

Bu çalışmada zaman serilerinin ağ tabanlı temsili için bir çerçeve sunulmuştur. Önerilen yöntemde öncelikle, zaman domenindeki sinyaller %50 örtüşmeli sabit genişlikli zaman pencerelerine bölünerek segmentasyon işlemi tamamlanır. Her segment, ana sinyalin mutlak maksimum genlik değerinin ve negatif karşılığının tanımladığı aralık baz alınarak normalize edilir ve normalize sinyaller 2^n seviyesine kuantize edilir. 3 farklı atlama değerinin ifade ettiği 3 kanaldan ilerleyen bu dönüşüm, kanalların katmanlar şeklinde birleştirilmesiyle düşey bir RGB görüntü temsilini oluşturur. Sinyalin her zaman penceresinden elde edilen bu düşey RGB imajlarının yan yana döşenmesinin sonucunda yatay eksenin zamanı ve düşey eksenin sinyal dalgalanmalarını temsil ettiği *VarioGram* olarak adlandırılan bir zaman-graf temsili elde edilmiş olur. Çevresel ses sınıflandırma problemlerinde sıklıkla kullanılan ESC-10 veri setindeki ses sinyallerinin dönüşümü ile elde edilen *VarioGram* temsilleri bir ResNet modeline girdi olarak verildiğinde %82.08'lik bir sınıflandırma başarısı elde edilmiş, mel-spectrogram görüntüleri ile hibritleştirilerek kullanılan *VarioGram* temsilleri ile bu başarı %93.33'e kadar çıkarılmıştır. Dolayısıyla VarioGram temsilleri, tek başına mel-spectrogram ile elde edilebilen en yüksek sınıflandırma başarısını küçük bir farkla iyileştirme yönünde etki yapmıştır.

VarioGram – A Colorful Time-Graph Representation For Time Series

Keywords

Graph representation
Sound classification
Time-series classification
Complex networks

Article Info

Received
September 20, 2022
Accepted
November 03, 2022
Published
December 28, 2022
Article Type
Research Paper

Abstract

In this study, a framework for network-based representation of time series is presented. In the proposed method, initially, a segmentation procedure is completed by dividing the signals in the time domain into fixed-width time windows with 50% overlap. Each segment is normalized based on the range defined by the absolute maximum amplitude value of the main signal and its negative counterpart, and the normalized signals are quantized to 2^n levels. This transformation, proceeding through 3 channels expressed by 3 different jump values, generates a vertical RGB image representation by combining the channels in layers. As a result of tiling these vertical RGB images from each time window horizontally, a time-graph representation called VarioGram is obtained, where the horizontal axis represents time, and the vertical axis represents signal fluctuations. Feeding a ResNet model with VarioGram representations obtained by the transformation of the audio signals in the ESC-10 dataset which is frequently used in environmental sound classification problems, a classification success of 82.08% has been obtained, while this success has been 93.33% with the VarioGram representations hybridized with mel-spectrogram images. The VarioGram representations therefore acted to slightly improve the highest classification success achievable with the mel-spectrogram alone.

Atıf: Türker, İ. & Aksu, S. (2022). VarioGram – Zaman serileri için renkli bir zaman-graf temsili. *Bilgi ve İletişim Teknolojileri Dergisi*, *4*(2), 128-143. https://doi.org/ 10.53694/bited.1177504

Cite: Türker, İ. & Aksu, S. (2022). VarioGram – A colorful time-graph representation for time series. *Journal of Information and Communication Technologies*, *4*(2), 128-143. https://doi.org/ 10.53694/bited.1177504

* **Sorumlu Yazar/Corresponding Author:** aksu@bartin.edu.tr

[1] Assoc. Prof. Dr., Karabuk University, Faculty Of Engineering, Karabuk/Turkey, iturker@karabuk.edu.tr, https://orcid.org/0000-0001-7577-4658

[2] PhD., Bartın University, Vocational School, Bartin/Turkey, aksu@bartin.edu.tr, https://orcid.org/ 0000-0001-6920-7219

Introduction

Scientific interest on time series classification and representation techniques have increased together with the increasing availability of temporal datasets from diverse domains such as medicine, finance, aviation, telecommunication, industry, weather, multimedia etc. (Bao et al., 2017; Canizo et al., 2019; Dafna et al., 2018; Gharehbaghi & Lindén, 2017; Pourbabaee et al., 2018; Soares et al., 2018). These available datasets facilitate several data-driven tasks including classification, clustering, segmentation, anomaly detection and so on (Ares et al., 2016; Canizo et al., 2019; Kanani & Padole, 2020; Ruiz et al., 2021). The main motivation for developing different representation techniques is reducing the complexity mostly caused by the high dimensionality of the data. Additionally, while converting time series data into diverse representations, scientists focus on improving classification accuracy, removing noise and accelerating the overall task (Deng et al., 2016).

Recently, sparse representation has been an attractive topic for time series, for which a test sample is represented as a sparse combination of training samples. The solution of the sparse representation problem further gives sparse representation coefficients and the test sample is assigned to the class minimizing the residual between itself and the reconstruction from the training samples of its class (Chen et al., 2015; Yin et al., 2012).

A mainstream of representation techniques involve in transformation domain methods including discrete Fourier transform (DFT) and discrete wavelet transform (DWT), Karhunen-Loeve (KL) transform or Singular Value Decomposition (SVD), either mapping the time sequences to a new feature space of a lower dimensionality, or providing a multi-resolution representation with time-frequency localization property (Chan & Fu, 1999). Transformation domain methods further evolved into image-based representations like mel-spectrograms especially used for sound signals, as a robust representation to noise content compared to mel-frequency cepstral coefficients (MFCCs), the coefficients capturing the envelope of the short time power spectrum. The spectrogram image is simply generated by applying discrete Fourier transform (DFT) to the fixed-size segments of the original sound, further finalized with a mel-filter provided from MFCCs (Sharan & Moir, 2015). A similar time-frequency image representation known as Cochleagram handles the frequency band in logarithmic fashion similar to human cochlea. By the way, it includes more frequency components in the lower and less frequency components in the higher frequency range (Peng et al., 2021).

An alternative framework for representing time series in a more structured format is powered by network science, which proposes that each complex interconnected system can be represented as a network (Baydilli et al., 2017; Demir & Türker, 2021; Türker et al., 2016; Türker & Sulak, 2018). Time series are converted into graph representations, which evaluate quantized amplitude levels as nodes and neighborhood between consecutive levels as edges between them (Lacasa et al., 2015). A well-known member of this convention is *visibility graph*, constructed by keeping the convexity information of sequential samples by establishing connections between quantized amplitude levels if they are visible from the top of another level in a pre-defined neighborhood (Lacasa et al., 2008). The resulting graph is a mean-adjacency matrix calculated over a whole time series, that can be assessed a stationary representation. Türker and Aksu achieved 2-3% more successful results than mel-spectrogram based methods in ESC-10 dataset classification with the Connectogram method, which they developed based on the graph representation of time series (Türker & Aksu, 2022).

The main motivation of this study is to develop a graph-inspired representation for time series data which can capture the convexity properties of a given signal, also capturing the time-dependent deviations in this graph representation. Instead of capturing edge formations between consecutive signal levels (nodes), we focus on differences between these nodes and encode them to a vertical array calculated from each frame of the segmented signal. These vertical arrays are then concatenated horizontally to form a time-graph representation, which in turn captures both signal envelope in its shape and power of alternance in the color levels. The color info is provided by applying the same procedure for three different subsampling rates, each of which forms a single layer of a resulting RGB image. The details of the conversion procedure together with its classification performance is presented in the coming sections.

Method

Data and preprocessing

In this study, we focus on an Environmental Sound Classification (ESC) task, dealing with recognizing some classes of sounds from the real environment. As a subfield of audio processing, ESC is a complex task involving classification of several sound events as one of the predefined sounds such as helicopter, sea waves, crying baby, crackling fire etc. (Zhang Zhichao and Xu, 2018). The most commonly used datasets in ESC tasks are known as ESC-10, ESC-50 (Piczak, 2015b) and UrbanSound8k (Salamon et al., 2014) datasets. The bigger ESC-50 dataset is a multiclass source consisting of 2000 separate environmental sound excerpts subdivided into 50 classes and 5 major categories. A filtered subset of ESC-50 is known as ESC-10, that is reduced to 400 samples consisting of 5-second records from 10 classes (Zhang Zhichao and Xu, 2018). Having a mono-channel signal form, environmental sound records can be assessed as a one-dimensional time series data which naturally holds both time and frequency components. We pick the ESC-10 dataset to apply the proposed conversion method. The steps of preprocessing are detailed in the next subsection.

Before the proposed method is applied, a unified preprocessing procedure is applied to all samples. We sampled the sound waves at 22050 Hz, filtered out components below 60dB and min-max normalized the signals into [-1, 1] range. An augmentation procedure is run in signal level first, applying time stretch, pitch shift, dynamic range compression, white noise addition to the raw sounds, augmenting the data size 6 times, to 2400 samples. A second augmentation procedure will also be applied through the TensorFlow library in Python environment, including image distortion methods (rotation, horizontal and vertical shift, brightness, shear, zoom) to the image representation of the sounds (Mushtaq et al., 2021).

After the signal-level preprocessing steps are applied, we apply a segmentation procedure subdividing the whole samples into frames with a window size of 1024 samples and hop-length of 512 samples, corresponding to 50% overlap between consecutive frames. Alternatively, it is possible to give a predefined number of frames to the function, that would result in VarioGrams of desired width and height, employing a different overlap percentage. Sound processing tasks are performed via Librosa library in Python environment, while all classifier models are trained using Keras library with TensorFlow backend on Google Colab environment.

Converting Sound Waves Into *VarioGrams*

We handle each frame including 1024 samples separately, performing a graph-based conversion into a vertical array demonstrating the varying patterns between consecutive signal levels.

- We first fix a *bit-depth* to quantize the signal, for which we employ a default value of 6, resulting a node count of $2^6 = 64$ signal levels (*scale* parameter). This means we further map the normalized amplitude range [-1,1] into [0, 63]. By the way, we achieve signal arrays including integers within this interval, that is ready for generating *variance arrays* (a term used for representing the varying rates, not statistical variance).
- A *variance array* is a resulting array with height $2 \times 2^6 = 2^7 = 128$, width 1, and depth 3.
    - *Height:* Since difference between neighboring amplitude levels are encoded, these differences can take values in range $[0 - 63]\ to\ [-63 - 0] \rightarrow [-63,63]$. Therefore, a size of 2^7 is needed regarding this scale.
    - *Width:* This array calculated from a separate sound segment, will be represented as a 1 pixel-width sequence, which are to be tiled horizontally to form the resulting *VarioGram*.
    - *Depth:* The conversion procedure will be held for 3 different subsampling rates to the original signal, resulting in 3 different $2^7 \times 1$ arrays, those are evaluated as RGB channels from a single variance array.
- Each *variance array* is calculated with 3 different subsampling rates given in a *jump* parameter holding default values as: [3,5,7]. The first value 3 means that a subsampling rate of 3 is applied to the original segment, before the neighborhood relations are encoded into the variance array. These subsampling rates are used to calculate R, G and B layers of the colored *variance array*.
- After each subsampling, the differences between neighboring amplitude levels in proceeding order within the range $\pm 2^n$, are further added with a constant 2^n to achieve nonnegative differences, and the corresponding element of the variance array of size $2^{n+1} \times 1 \times 3$ is increased by 1. For example, if the sequence is like […47, 33…], a difference of $33 - 47 = -14$ is calculated first. Then, it is shifted by the *scale* parameter as $-14 + 64 = 50$. If we are encoding for the first element of the jump parameter, i.e. 3, we increase the element of the *variance array* with index [50, 0, 0] by 1.
- After processing each frame, all variance arrays are normalized to 0-1 interval.
- This procedure is run for each jump layer (3, 5 and 7; corresponding the resulting RGB layers) to achieve a variance array of size $2^{n+1} \times 1 \times 3$.
- Also applied for each sound frame, this procedure produces vertical RGB arrays as much as the count of consecutive frames, further tiled horizontally to form time-variance images named as *VarioGram*. The complete procedure is illustrated in Fig. 1.

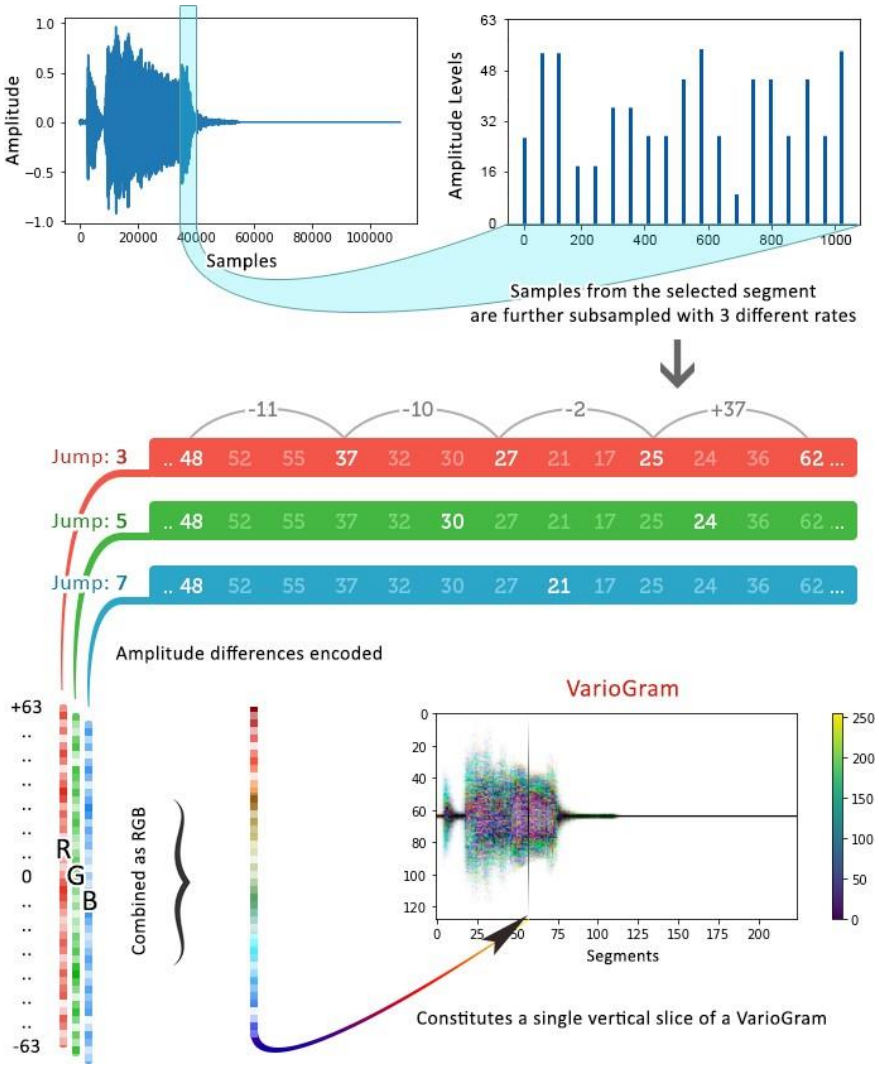


Figure 1. Procedure followed to form a *VarioGram* is illustrated. A sequence is first sampled, quantized and subdivided into frames. Each frame is then subsampled with 3 different rates. For each subsampling rate applied, differences between consecutive amplitude levels are encoded into a vertical array as +1. These vertical arrays are further min-max normalized to 0-1 range, and combined as a RGB-slice representing a single frame. Vertical RGB slices derived from each frame are then tiled horizontally to form a *VarioGram*.

The resulting *VarioGram* images captures both time (horizontal) and convexity (vertical) information of the corresponding time series. Optimal values of the parameters used in conversion procedure are given in Table 1. Having applied the VarioGram converter function to the sound samples in ESC-10 dataset, a set of image representations are generated. Sample VarioGram images together with the original sound plot and mel-spectrogram images are given in Fig. 2 to provide visual comparison to the reader.

As presented in Fig. 2, *VarioGram* representations resemble the shape of the original sound, holding the amplitude information. It also captures signal convexity information as the color range encoded inside the signal shape. By the way, a time-convexity based representation also including amplitude information is generated.

Table 1. *VarioGram* parameters together with their optimal values used in experiments.

Parameter	Value	Definition
bit-depth	6	The original signal sequence is quantized into 2^6 positive integer levels. This value corresponds to vertical slices of size $2^7 \times 1$ since differences between neighboring amplitude levels can vary between -63 and +63 for this setup.
windowSize	2	Differences between each samples neighboring in forward direction are encoded into the vertical variance arrays. This neighboring is applied for 1 and 2-distant samples.
sr	22050	Sampling rate applied to the original sound
jump	[3,5,7]	Undersampling rate for the 3 layers of the variance arrays
winLength	1024	Width of the sound frames
hopLength	512	Distance between the consecutive frames, corresponding to 50% overlap

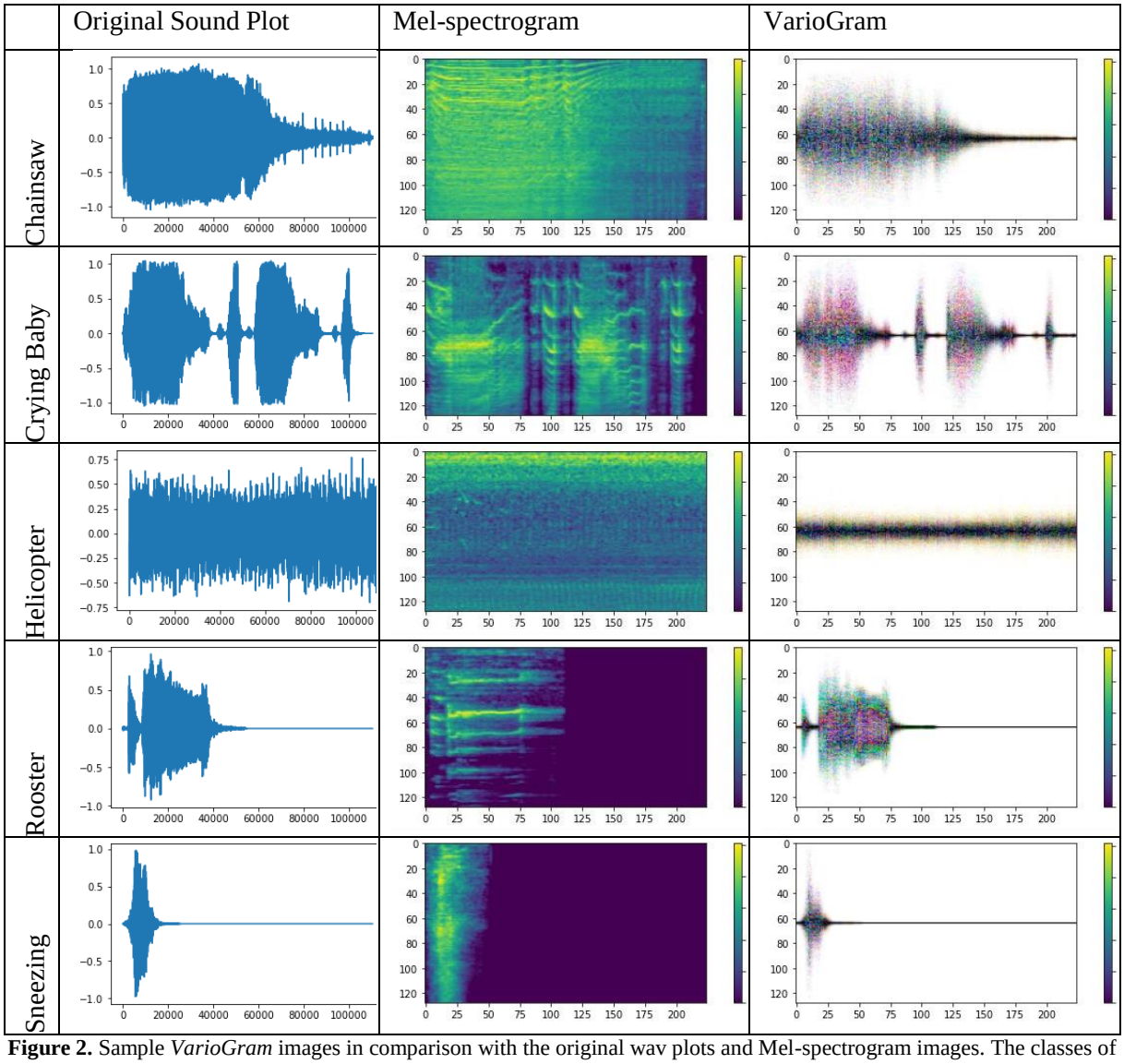


Figure 2. Sample *VarioGram* images in comparison with the original wav plots and Mel-spectrogram images. The classes of the sample sound waves are given in the row headers, while the type of the plot is given in the column headers.

Deep Learning with *VarioGrams*

To assess the representation capability of the *VarioGrams*, we tested these representations through a residual network deep learning architecture (ResNet). This model was first introduced by Microsoft researchers in 2015 and resembles the pyramidal cells of cerebral cortex of human brain. The main property of ResNets is the residual connection shortcutting between consecutive convolutional layers (Ismail Fawaz et al., 2019).

ESC dataset is presented with a fixed 5-fold structure, where sound excerpts from the same original long-duration source are placed in the same fold to preserve the hardness of the problem. Therefore, it is recommended to obey these fold assignments due to avoiding inflation of the classification success (Piczak, 2015a). To strictly satisfy this rule, we also kept the augmented sounds in the same fold.

Due to the nature of the ResNet architecture inheriting the transfer learning parameters, all VarioGram images are resized as 224x224 pixel RGB images to provide optimal match for this model. During the experiments, these VarioGram images are used either in its original RGB form or fused with the mel-spectrogram images of the same source. If they are combined with spectrograms, both *VarioGrams* and mel-spectrograms are converted into grayscale and these grayscale images are used as the single channel of the resulting fusion images. As a result, *VarioGrams* (vario) and mel-spectrograms (mels) derived with same windowing parameters stand for the synchronous channels of the resulting RGB image. We refer these fusion images as [vario+vario+vario] (standalone usage) or [mels+mels+vario] (fusion) notation in the results section.

Findings

To better understand the representation capacity of the *VarioGram* images, we performed classification tasks with 5-fold cross-validation procedure using standalone *VarioGram* images first, followed by standalone mel-spectrogram images and lastly with fusion images as their combination. The classification tasks are performed 10 times for each set, while the best results achieved are presented in Table 2.

Table 2. Classification results for standalone images or combinations of mel-spectrograms (mels) and *VarioGrams* (vario). In combination cases, each representation is first converted to grayscale to form a single channel of the resulting RGB fusion image.

Model	Accuracy
[mels, mels, mels]	92.91 %
[vario, vario, vario]	82.08 %
[mels, mels, vario]	93.33 %

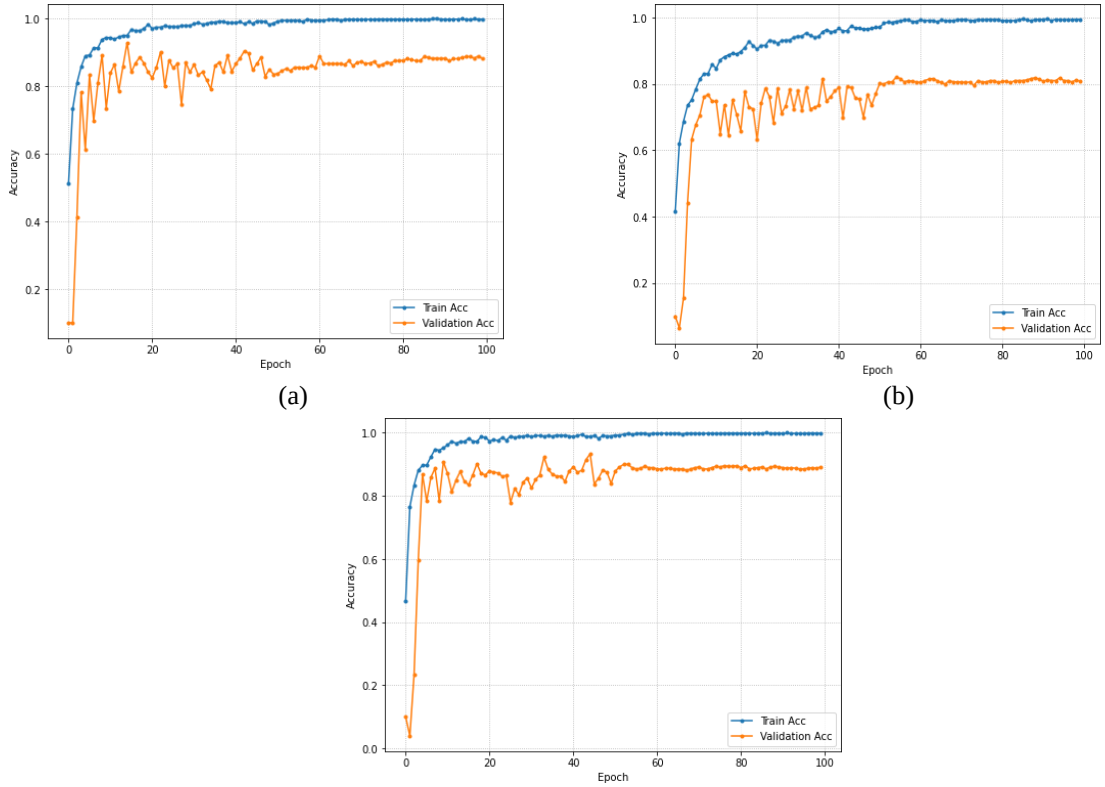


Figure 3. Classification curves for the best case achieved with ResNet50 architecture using the image representations of sounds as (a) [mels, mels, mels], 92.91%, (b) [vario, vario, vario], 82.08%, (c) [mels, mels, vario], 93.33% accuracy.

As presented in Table 2 and Fig. 3, standalone *VarioGram* representations are not as successful as mel-spectrogram representations, yielding approximately 10% lower accuracy scores. However, a combination of mel-spectrogram and *VarioGram* images can outperform the best standalone representation by ~0.4%. This is an indicator that *VarioGrams* have a boosting capability while used in combination with mel-spectrograms, and they cannot be recommended to be used solely for high-accuracy classification tasks. Since the window parameters used for both representors are the same, the resulting images have synchronous properties in horizontal (time) axis, making them complementary representations those are more powerful while used in hybrid fashion. We can also note that the classification performance that VarioGram represents, being not as competitive as the current classification studies, is better than the original study (80%) presented by Piczak in 2015 (Piczak, 2015a).

Conclusion

The proposed time-convexity representation named VarioGram, having roots from network science, offers a time-dependent representation for time series capturing both its envelope and varying intensity in its resulting shape and color. Although not performing as good as a well-known mel-spectrogram images in c classification task, it increases the sole performance of them while combined, and also forms an alternative way that should be consulted for different AI-related tasks. We recommend studying the representation performance of *VarioGrams* in medical time series data such as ECG or EMG, for which temporal convexity characteristics play a vital role in diagnosing the anomalies.

Genişletilmiş Özet

Giriş

Tıp, finans, havacılık, telekomünikasyon, endüstri, hava durumu, multimedya gibi çeşitli alanlardan zamansal veri setlerinin artan kullanılabilirliği ile birlikte zaman serilerinin sınıflandırma ve temsil tekniklerine olan bilimsel ilgi artmıştır (Bao et al., 2017; Canizo et al., 2019; Dafna et al., 2018; Gharehbaghi & Lindén, 2017; Pourbabaee et al., 2018; Soares et al., 2018). Bu kullanılabilir veri setleri, sınıflandırma, kümeleme, segmentasyon, anomalilik algılama vb. dahil olmak üzere çeşitli veri odaklı görevleri kolaylaştırır (Ares et al., 2016; Canizo et al., 2019; Kanani & Padole, 2020; Ruiz et al., 2021). Verileri temsil etmek için farklı teknikleri geliştirmedeki temel motivasyon, çoğunlukla verilerin yüksek boyutluluğundan kaynaklanan karmaşıklığı azaltmaktır. Ek olarak, bilim adamları zaman serisi verilerini çeşitli temsillere dönüştürürken, sınıflandırma doğruluğunu iyileştirmeye, gürültüyü ortadan kaldırmaya ve genel görevi hızlandırmaya odaklanır (Deng et al., 2016).

Zaman serilerini daha yapılandırılmış bir formatta temsil etmek için alternatif bir çerçeve de, karmaşık olarak birbirine bağlı nesnelerden oluşan sistemlerin bir ağ formatında temsil edilebilmesidir (Baydilli et al., 2017; Demir & Türker, 2021; Türker et al., 2016; Türker & Sulak, 2018). Bu yöntem kullanılarak zaman serileri, nicelenmiş genlik seviyelerinin düğümler ve ardışık seviyeler arasındaki komşulukların ise kenarlar olarak değerlendirildiği graflar şeklinde temsil edilebilir (Lacasa et al., 2015). Önceden tanımlanmış bir komşulukta başka bir seviyenin üstünden görülebilen nicelenmiş genlik seviyeleri arasında bağlantılar kurularak sıralı örneklerin dışbükeylik bilgileri ile görünürlük grafları inşa edilir (Lacasa et al., 2015). Bu çalışmalardan birinde Türker ve Aksu, zaman serilerinin graf gösterimi temeline dayalı olarak geliştirdikleri *ConnectoGram* temsili ile ESC-10 veri seti üzerindeki sınıflandırma çalışmalarında 2-3% oranında bir başarı artışı sağlanmışlardır (Türker & Aksu, 2022).

Yöntem

Veri ve ön işleme

Bu çalışmada, gerçek ortamlardan elde edilmiş bazı ses sınıflarını tanımakla ilgilenen bir Çevresel Ses Sınıflandırması (ÇSS) görevine odaklanılmıştır. Ses işlemenin bir alt alanı olarak çevresel seslerin sınıflandırılması işlemi; helikopter, deniz dalgaları, ağlayan bebek, çatırdayan ateş gibi önceden tanımlanmış seslerden oluşan çeşitli ses olaylarının tespit edilmesini içeren karmaşık bir görevdir (Zhang Zhichao and Xu, 2018). Bu alanda en yaygın kullanılan kütüphaneler arasında ESC-10, ESC-50 (Piczak, 2015b) ve UrbanSound8k (Salamon et al., 2014) veri setlerini sayabiliriz. ESC-50 veri seti 5 ana kategoriye ayrılmış 50 sınıftan oluşan 2000 sesten, ESC-10 ise 5 ana kategoride 10 sınıftan oluşan 400 sesten oluşmaktadır (Zhang Zhichao and Xu, 2018). Seslerin özelliklerini belirlemek için önerilen yönteme geçmeden önce tüm örneklere aynı ön-işleme prosedürü uygulanmıştır. Bu aşamada ses dalgaları 22050 Hz'de örneklenmiş, 60 dB'in altındaki bileşenler filtrelenmiştir. Bu işlemelerin ardından sinyallerin minimum ve maksimum değerleri [-1, 1] aralığında normalleştirilmiştir. Derin öğrenme yöntemlerinin daha başarılı sonuçlar vermesi için sinyal seviyesinde veri büyütme teknikleri uygulanmış ve 400 olan ses örneği sayısı 2400'e çıkartılmıştır. Grafa dayalı imajlar oluşturulduktan sonra ise *Python* dilinde yazılmış olan *Tensorflow* kütüphanesi ile ayrıca imaj düzeyinde döndürme, yatay ve dikey kaydırma, parlaklık, kırpma, yakınlaştırma gibi veri büyütme teknikleri uygulanmıştır (Mushtaq et al., 2021).

Ses Sinyallerinin VarioGram'a Dönüştürülmesi

Ardışık sinyallerin örüntüsünü oluşturacak şekilde graf tabanlı bir diziye dönüştürme işlemini gerçekleştirmek için her bir çerçeve 1024 farklı örnek içerecek şekilde ele alınır. Bu amaçla;

- İlk olarak bit tabanlı sayısallaştırma yapmak üzere ölçekleme seviyesi varsayılan olarak 6 bit derinliği seçilir ve $2^6 = 64$ sinyal seviyesi oluşturulur. Böylece [-1,1] aralığı [0,63] aralığına dönüştürülmüş olur.
- Bir *varyans dizisi*, sonuçta yüksekliği $2 \times 2^6 = 2^7 = 128$, genişliği 1, ve derinliği 3 olan bir dizidir.
    - **Yükseklik:** Kodlanan komşu genlik seviyeleri arasındaki fark. Bu fark $[0-63]\ to\ [-63-0] \rightarrow [-63,63]$ aralığına karşılık gelir. Böylece bu ölçeği göz önünde bulundurulduğunda boyut 2^7 olur.
    - **Genişlik:** Ardışık ses segmentlerinden elde edilmiş olan ve *VarioGram*'ı oluşturmak üzere yatay olarak döşenecek dizinin genişliği 1 pikseldir.
    - **Derinlik:** Dönüştürme işlemi her bir ses sinyalinden [3,5,7] olmak üzere 3 farklı atlama seviyesi ile gerçekleştirilir ve böylece RGB imajlarının katmanlarını oluşturacak şekilde 3 farklı $2^7 \times 1$ boyutunda dizi elde edilmiş olur.
- Her bir *varyans dizisi*, varsayılan atlama değerleri [3,5,7] olarak tutan bir atlama parametresi ile elde edilen 3 farklı alt örnekleme oranı ile hesaplanır. Böylece her bir örnekleme için renklendirilmiş *varyans dizisi'*ni oluşturacak ***R***, ***G*** ve ***B*** katmanları elde edilmiş olur.
- Ayrıca her ses karesi için uygulanan bu prosedür, *VarioGram* olarak adlandırılan zaman-varyanslı görüntüleri oluşturmak için yatay olarak döşenen ardışık kare sayısı kadar dikey RGB dizileri üretir.

VarioGram ile Derin Öğrenme

VarioGram'ların temsil kabiliyetini değerlendirmek için, ResNet derin öğrenme modeli kullanılmıştır. Bu model ilk olarak 2015 yılında Microsoft araştırmacıları tarafından tanıtılmış ve insan beyninin serebral korteksinin piramidal hücrelerinin araştırılmasında kullanılmıştır. ResNets'in ana özelliği, ardışık evrişim katmanları arasındaki artık bağlantı kısayollarıdır (Ismail Fawaz et al., 2019).

Çalışmanın veri kısmında ise 5 farklı ortamdan elde edilip 5 farklı klasörün her birine benzer sınıfa ait eşit uzunluktaki seslerin Dağıtıldığı ESC veri seti kullanılmıştır. Bu nedenle, sınıflandırma başarısındaki aşırı öğrenme gibi sorunlardan kaçınmak için eğitim ve test aşamalarında bu 5 klasöre ayrılmış ve bu seslerin karıştırılmadan kullanılması tavsiye edilmiştir (Piczak, 2015a).

Transfer öğrenme parametrelerini kullanan ResNet mimarisinin doğası gereği en iyi sonucu elde etmek üzere tüm *VarioGram* imajları RGB formatında 224x224 piksel olarak yeniden boyutlandırılmıştır. Eğer *VarioGram* imajlar mel-spectrogram imajlarla birleştirilecekse her iki imaj da öncelikle gri tonlamaya dönüştürülür ve bu gri tondaki imajlar birleştirilerek RGB formatının birer katmanı olarak ele alınır. Sonuç olarak, birleştirilmeden sadece *VarioGram*'ların olduğu imajlar [vario+vario+vario] ve mel-spectrogram'lar ile birleştirilen imajlar ise [mels+mels+vario] olarak eğitime alınmış olur.

Bulgular

VarioGram görüntülerinin temsil kapasitesini daha iyi belirlemek için, sınıflandırma işlemi 5-fold çapraz-doğrulama yöntemi ile gerçekleştirilmiştir. İlk olarak *VarioGram* ve mel-spectrogram imajlar ayrı ayrı hiçbir

birleştirme işlemi uygulanmadan eğitim için kullanılmıştır. Ardından *VarioGram* ve mel-spectrogram imajların birleştirilmiş hali ele alınmıştır. Eğitimden daha başarılı sonuçlar elde etmek için her sınıflandırma görevi 10 kez tekrarlanmış ve bu tekrarların ortalaması alınmıştır. Yapılan çalışmalardan elde edilen sonuçlar Tablo 2'de gösterilmiştir.

Sadece *VarioGram* imajların kullanılması durumunda mel-spectrogram imajlar kadar iyi sonuç elde edilememiş ve yaklaşık olarak 10% kadar daha düşük verimli sonuçlar ortaya çıkmıştır. Bununla beraber *VarioGram* ve mel-spektrogram imajların birleştirilmiş hali ile yaklaşık olarak ~0.4% gibi daha iyi bir sonuç elde edilmiştir. Bu durum, mel-spectrogram'larla birlikte kullanıldığında *VarioGram*'ların bir performans artırma kapasitesine sahip olduğunu göstermektedir. Her iki temsil yöntemi için kullanılan pencere parametreleri aynı olduğundan, ortaya çıkan görüntüler yatay (zaman) eksende senkronize özelliklere sahiptir. Bu da, bu iki yöntemin hibrit modda kullanılması halinde zaman serileri ile ilgili daha güçlü tamamlayıcı temsiller elde edilmesini sağlamaktadır. Mevcut sınıflandırma çalışmaları kadar rekabetçi olmamakla birlikte *VarioGram'*ın temsil ettiği sınıflandırma performansının, 2015 yılında Piczak tarafından sunulan orijinal çalışmadan (%80) daha iyi bir sonuç verdiği görülmektedir (Piczak, 2015a).

Sonuç

Bu çalışmada önerdiğimiz ve köklerini ağ biliminden alan *VarioGram*, zaman serileri için genlik seviyeleri arasındaki farkları ve yoğunlukları dikkate alarak bu değişimleri renk tonları ile ifade eden zamana bağlı yeni bir temsil metodu sunmaktadır. Sınıflandırma çalışmalarında her ne kadar bu yöntem bilinen ve sık kullanılan mel-spektrogram imajlarına dayalı yöntemler kadar iyi sonuç vermese de farklı yapay zeka çalışmalarında önerdiğimiz bu yöntemin imajlarla birlikte kullanılması halinde performans artışına katkı sağladığı görülmüştür. Sağlık sorunlarını belirlemek amaıyla geçici değişimlerin hayati önem taşıdığı ECG veya EMG verileri gibi tıbbi zaman serilerinin analizinde *VarioGram* temsil yönteminin kullanılmasını tavsiye etmekteyiz.

Yayın Etiği Bildirimi / Research Ethics

Araştırma ve yayın etiği konusunda bilimsel etik kaideleri göz önünde bulundurulmuştur. / Scientific ethical principles have been taken into consideration in research and publication ethics.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Birinci araştırmacı, makalenin genelinde kavramsallaştırma, metodoloji, formal analiz ve sorumlu yazar olarak görev alırken, ikinci araştırmacı, literatür taraması, metodoloji, yazılım geliştirme, test ve doğrulama konularında katkı sağlamıştır. / While the first researcher worked as the conceptualization, methodology, formal analysis and lead author throughout the article, the second researcher contributed to the literature review, methodology, software development, testing and validation.

Çıkar Çatışması / Conflict of Interest

Bu çalışmada herhangi bir çıkar çatışması bulunmamaktadır. / This study has no conflict of interest.

Fon Bilgileri / Funding

Bu çalışmada herhangi bir fon kullanılmamıştır. / No funds were used in this study.

Etik Kurul Onayı / The Ethical Commitee Approval

Bu araştırma makalesinin etik sorunu olmadığını beyan ederiz. / We hereby declare that this research article does not have an unethical problem.

Kaynakça/References

Ares, J., Lara, J. A., Lizcano, D., & Suarez, S. (2016). A soft computing framework for classifying time series based on fuzzy sets of events. *Information Sciences*, *330*, 125–144. https://doi.org/10.1016/J.INS.2015.10.014

Bao, W., Yue, J., & Rao, Y. (2017). A deep learning framework for financial time series using stacked autoencoders and long-short term memory. *PLoS ONE*, *12*.

Baydilli, Y. Y., Bayir, Ş., & Türker, I. (2017). A Hierarchical View of a National Stock Market as a Complex Network. *Economic Computation & Economic Cybernetics Studies & Research*, *51*(1).

Canizo, M., Triguero, I., Conde, A., & Onieva, E. (2019). Multi-head CNN–RNN for multi-time series anomaly detection: An industrial case study. *Neurocomputing*, *363*, 246–260. https://doi.org/10.1016/J.NEUCOM.2019.07.034

Chan, K.-P., & Fu, A. W.-C. (1999). Efficient time series matching by wavelets. *Proceedings 15th International Conference on Data Engineering (Cat. No.99CB36337)*, 126–133. https://doi.org/10.1109/ICDE.1999.754915

Chen, Z., Zuo, W., Hu, Q., & Lin, L. (2015). Kernel sparse representation for time series classification. *Information Sciences*, *292*, 15–26. https://doi.org/10.1016/J.INS.2014.08.066

Dafna, E., Tarasiuk, A., & Zigel, Y. (2018). Sleep staging using nocturnal sound analysis. *Scientific Reports*, *8*(1), 13474. https://doi.org/10.1038/s41598-018-31748-0

Demir, S., & Türker, İ. (2021). Arithmetic success and gender-based characterization of brain connectivity across EEG bands. *Biomedical Signal Processing and Control*, *64*, 102222. https://doi.org/10.1016/J.BSPC.2020.102222

Deng, W., Wang, G., & Xu, J. (2016). Piecewise two-dimensional normal cloud representation for time-series data mining. *Information Sciences*, *374*, 32–50. https://doi.org/10.1016/J.INS.2016.09.027

Gharehbaghi, A., & Lindén, M. (2017). A deep machine learning method for classifying cyclic time series of biological signals using time-growing neural network. *IEEE Transactions on Neural Networks and Learning Systems*, *29*(9), 4102–4115.

Ismail Fawaz, H., Forestier, G., Weber, J., Idoumghar, L., & Muller, P.-A. (2019). Deep learning for time series classification: a review. *Data Mining and Knowledge Discovery*, *33*(4), 917–963. https://doi.org/10.1007/s10618-019-00619-1

Kanani, P., & Padole, M. (2020). ECG Heartbeat Arrhythmia Classification Using Time-Series Augmented Signals and Deep Learning Approach. *Procedia Computer Science*, *171*, 524–531. https://doi.org/10.1016/J.PROCS.2020.04.056

Lacasa, L., Luque, B., Ballesteros, F., Luque, J., & Nuño, J. C. (2008). From time series to complex networks: The visibility graph. *Proceedings of the National Academy of Sciences*, *105*(13), 4972–4975. https://doi.org/10.1073/PNAS.0709247105

Lacasa, L., Nicosia, V., & Latora, V. (2015). Network structure of multivariate time series. *Scientific Reports*, *5*(1), 15508. https://doi.org/10.1038/srep15508

Mushtaq, Z., Su, S. F., & Tran, Q. V. (2021). Spectral images based environmental sound classification using CNN with meaningful data augmentation. *Applied Acoustics*, *172*, 107581. https://doi.org/10.1016/J.APACOUST.2020.107581

Peng, Z., Dang, J., Unoki, M., & Akagi, M. (2021). Multi-resolution modulation-filtered cochleagram feature for LSTM-based dimensional emotion recognition from speech. *Neural Networks*, *140*, 261–273. https://doi.org/10.1016/J.NEUNET.2021.03.027

Piczak, K. J. (2015a). Environmental sound classification with convolutional neural networks. *2015 IEEE 25th International Workshop on Machine Learning for Signal Processing (MLSP)*, 1–6.

Piczak, K. J. (2015b). ESC: Dataset for Environmental Sound Classification. *Proceedings of the 23rd ACM International Conference on Multimedia*, 1015–1018. https://doi.org/10.1145/2733373.2806390

Pourbabaee, B., Roshtkhari, M. J., & Khorasani, K. (2018). Deep Convolutional Neural Networks and Learning ECG Features for Screening Paroxysmal Atrial Fibrillation Patients. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *48*(12), 2095–2104. https://doi.org/10.1109/TSMC.2017.2705582

Ruiz, A. P., Flynn, M., Large, J., Middlehurst, M., & Bagnall, A. (2021). The great multivariate time series classification bake off: a review and experimental evaluation of recent algorithmic advances. *Data Mining and Knowledge Discovery*, *35*(2), 401–449. https://doi.org/10.1007/s10618-020-00727-3

Salamon, J., Jacoby, C., & Bello, J. P. (2014). A Dataset and Taxonomy for Urban Sound Research. *Proceedings of the 22nd ACM International Conference on Multimedia*, 1041–1044. https://doi.org/10.1145/2647868.2655045

Sharan, R. v, & Moir, T. J. (2015). Cochleagram image feature for improved robustness in sound recognition. *2015 IEEE International Conference on Digital Signal Processing (DSP)*, 441–444. https://doi.org/10.1109/ICDSP.2015.7251910

Soares, E., Costa, P., Costa, B., & Leite, D. (2018). Ensemble of evolving data clouds and fuzzy models for weather time series prediction. *Applied Soft Computing*, *64*, 445–453. https://doi.org/10.1016/J.ASOC.2017.12.032

Türker, İ., & Aksu, S. (2022). Connectogram – A graph-based time dependent representation for sounds. *Applied Acoustics*, *191*, 108660. https://doi.org/10.1016/J.APACOUST.2022.108660

Türker, İ., Şehirli, E., & Demiral, E. (2016). Uncovering the differences in linguistic network dynamics of book and social media texts. *SpringerPlus*, *5*(1), 864. https://doi.org/10.1186/s40064-016-2598-2

Türker, İ., & Sulak, E. E. (2018). A multilayer network analysis of hashtags in twitter via co-occurrence and semantic links. *International Journal of Modern Physics B*, *32*(04), 1850029. https://doi.org/10.1142/S0217979218500297

Yin, J., Liu, Z., Jin, Z., & Yang, W. (2012). Kernel sparse representation based classification. *Neurocomputing*, *77*(1), 120–128. https://doi.org/10.1016/J.NEUCOM.2011.08.018

Zhang Zhichao and Xu, S. and C. S. and Z. S. (2018). Deep Convolutional Neural Network with Mixup for Environmental Sound Classification. In C.-L. and C. X. and Z. J. and T. T. and Z. N. and Z. H. Lai Jian-Huang and Liu (Ed.), *Pattern Recognition and Computer Vision* (pp. 356–367). Springer International Publishing.

2022

4(2), 143-170

Bilgi ve İletişim Teknolojileriyle Özel Hayata Karşı İşlenen Suçların Değerlendirilmesi

Türkay Henkoğlu[*][1]

Anahtar Sözcükler
Özel hayat
Gizlilik
Bilgi ve iletişim teknolojileri
Sosyal medya

Makale Hakkında
Gönderim Tarihi
09 Nisan 2022
Kabul Tarihi
22 Haziran 2022
Yayın Tarihi
28 Aralık 2022

Makale Türü
Araştırma Makalesi

Öz

Elektronik ortamda yer alan bilgilerin işlenme süreçlerinde bilginin gizliliğinin korunmaya ihtiyacı olduğu kadar, bu bilgilerin sahipleri olarak kişilerin gizliliğinin de korunmaya ihtiyacı vardır. Elektronik ortamda bilginin işlenmesiyle ilişkili olarak bireylerin özel hayatının korunması hedef alındığında, özel hayata ve hayatın gizli alanına karşı işlenebilecek suçlara yönelik önlemlerin alınması ve/veya bu konudaki hukuksal sorumlulukların yerine getirilmesi önem taşımaktadır. "Özel hayata ve hayatın gizli alanına karşı suçlar" Türk Ceza Kanunu'nun (TCK) dokuzuncu bölümünde 132 ila 140. maddeleri arasında düzenlenmiştir. Bu çalışmada, elektronik ortamlarda özel hayata ve hayatın gizli alanına karşı işlenebilecek suçlara dikkat çekilmesi ve çoğunlukla bilgi teknolojilerinin yardımıyla gerçekleşen bu suçlara ilişkin Yargıtay kararları üzerinden mevcut durumun ortaya konulması amaçlanmıştır. Çalışmada betimleme yöntemi kullanılmış ve çalışma kapsamında, TCK'da "özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında tanımlanan suçlara yönelik Hukuk Türk bilgi bankası üzerinden erişim sağlanan toplam 129 Yargıtay kararı incelenmiştir. Elde edilen bulgular sonucunda, ilgili suçların bilgi ve iletişim teknolojilerinden yararlanılarak işlenme oranlarının yüksek olduğu görülmektedir. Çalışmada bu suçlara ilişkin uygulama, yorumlama ve karar verme süreçlerindeki yanılgılar Yargıtay kararları üzerinden değerlendirilerek, konuya ilişkin karar vericiler ve bilgi profesyonellerine yönelik farkındalığa katkı sağlayacak hususlara dikkat çekilmiştir.

Assessment of Crimes Committed Against Private Life Through Information and Communication Technologies

Keywords
Private life
Privacy
Information and communication technologies
Social media

Article Info
Received
April 09, 2022
Accepted
June 22, 2022
Published
December 28, 2022

Article Type
Research Paper

Abstract

In the process of information processing in an electronic environment, the privacy of individuals as the owners of the information need to be protected, as well as the privacy of this information. When it is aimed to protect the private life of individuals in relation to information processing in the electronic environment, it is important to take measures against crimes committed against private life and the secret sphere of private life and/or to fulfill legal responsibilities in this regard. Crimes against private life and the secret sphere of private life are regulated in Section 9 of the Turkish Penal Code (TPC) between Articles 132 and 140. This study, it is aimed to draw attention to the crimes committed against private life and the secret sphere of private life in electronic environments, and to reveal the current situation regarding these crimes, which are mostly committed with the help of information technologies, through the decisions of the Court of Cassation. For this purpose, in the study a total of 129 decisions of the Court of Cassation defined under the title of crimes against private life and secret sphere of private life were analyzed through the descriptive survey research method. As a result of the findings, it is seen that the rate of committing these crimes by using information and communication technologies is high. In the study, by evaluations of mistakes in the implementation, interpretation, and decision-making processes regarding these crimes within the framework decisions of the Court of Cassation, attention is drawn to the issues that will contribute to the awareness of decision-makers and information professionals on the subject.

Atıf: Henkoğlu, T. (2022). Bilgi ve iletişim teknolojileriyle özel hayata karşı işlenen suçların değerlendirilmesi. *Bilgi ve İletişim Teknolojileri Dergisi*, *4*(2), 143-170. https://doi.org/10.53694/bited.1100987

Cite: Henkoğlu, T. (2022). Assessment of crimes committed against private life through ınformation and communication technologies. *Journal of Information and Communication Technologies*, *4*(2), 143-170. https://doi.org/10.53694/bited.1100987

[*] **Sorumlu Yazar/Corresponding Author** turkay.henkoglu@adu.edu.tr

[1] Assist, Prof. Dr., Aydın Adnan Menderes University, Department of Management Information Systems, Aydın/Turkey, turkay.henkoglu@adu.edu.tr, https://orcid.org/0000-0002-0567-5408

Introduction

Today, a large part of the information is processed in electronic media, and a large part of "crimes against private life and the confidential sphere of private life" is committed in electronic environment and through information systems. In the process of information processing in an electronic environment, the privacy of individuals as the owners of the information needs to be protected, as well as the privacy of this information. Within the scope of information security, it is possible to say that protecting the privacy of information, it contributes to the protection of individuals' private lives. However, when it is aimed to protect the private life of individuals in relation to information processing in the electronic environment, is necessary to take measures against crimes committed against private life and the secret sphere of private life and/or to fulfill legal responsibilities in this regard. While professional organizations point out the legal regulations on the subject by drawing attention to the increasing threats against private life and the confidential sphere of life in their social media policies, there is no explanatory information about how these crimes are committed and how the legal regulations should be interpreted. In order to respect the private life and the secret sphere of private life in daily life and to reduce the crime rates committed in this regard, it is important to include information on the legal approach to this issue in the daily information that people use practically in their daily lives.

In the study, it is aimed to increase the awareness of decision-makers and information professionals on the subject by revealing the current situation within the framework of the Supreme Court decisions, which facilitate the interpretation of legal regulations and guide in terms of implementation. For this purpose, answers to the following research questions are sought:

- What are the “crimes against private life and the confidential sphere of life” in electronic media?
- Which methods are used to commit crimes against privacy violation, and how many of these crimes are committed by using information and communication technologies?
- What kind of misconceptions or different opinions are encountered in practice regarding crimes committed against private life and the secret sphere of private life by using information and communicationtechnologies?
- What are the decisions and evaluations of the Court of Cassation regarding the crimes against violation of the confidentiality of communication in electronic media, listening of private conversations between individuals by a listening device or recording these conversations, privacy violation, recording personal data, unlawful delivery or acquisition of data, and failing to destroy all copies of the data?

Method

Crimes against private life and the secret sphere of private life are regulated the Section 9 of the Turkish Penal Code (TPC) between Articles 132 and 140. This study, it is aimed to draw attention to the crimes committed against private life and the secret sphere of private life in electronic environments, ad to reveal the current situation regarding these crimes, which are mostly committed with the help of information technologies, through the decisions of the Court of Cassation which are facilitating the interpretation of legal regulations and guiding in terms of their application. For this purpose, in the study a total of 129 decisions of the Court of Cassation defined under the title of crimes against private life and secret sphere of private life were analyzed through descriptive

survey research method. In this way, it is also aimed to increase the awareness of decision makers and information professionals on the subject.

In this context, answers were sought about what are the crimes committed against private life and secret sphere of private life in electronic media, what are the effects of the use of social media and information technologies in violation of privacy of private life and related decision-making processes, how the Court of Cassation made decisions regarding the crimes of violation of privacy of communication in electronic media, listening and recording of conversations between individuals, recording of personal data, and unlawful acquisition or disclosure of data.

As a result of the findings, the extent of the effects of the use of information and communication technologies and social media in the decision-making processes regarding these crimes were revealed. In the study, by revealing the current situation within the framework decisions of the Court of Cassation, which are a guide for interpretation and implementation of legal regulations, attention is drawn to the issues that will contribute to the awareness of decision makers and information professionals on the issues like the crimes of violating the confidentiality of communication, listening and recording of conversations between individuals, violating the privacy of private life, recording personal data, unlawfully giving or obtaining data, and not destroying data.

Discussion and Conclusion

In order not to become a part of the crimes committed against private life and the secret sphere of life or to take adequate measures against these crimes, it is important to have information about the crimes regulated in Section 9 of the Turkish Penal Code (TPC) between Articles 132 and 140. Nowadays, it is possible to say that examining these crimes through information and communication media has become a necessity. It is observed that the rate of these crimes committed with the help of information and communication technologies is very high in the decisions of the Court of Cassation. Also, it is seen that there is an increase in the rate of crimes against private life and the secret sphere of life being committed through social network providers with the widespread use of social media in all institutions and organizations. Legal responsibilities are becoming more important and their reflections on both the person and the relevant institution may be more severe if people who tend to share their private life on social media are public employees. The fact that crimes committed against the privacy of private life are committed mostly through information and communication technologies today leads to make more mistakes in application, interpretation, and criminal decision-making processes. For this reason, it is thought that it would be beneficial for information professionals who process, manage and develop information policies about the informationprocessingd in electronic media to take into account the legal conditions and increasing risks regarding the protection of privacy.

Giriş

İnsanoğlu sosyalleşmenin ve paylaşma gereksiniminin bir yansıması olarak toplum içinde iletişim halinde kalmaya çalışırken, aynı zamanda kendisine ait olan ve sadece sınırlı sayıda kişi tarafından bilinmesini istediği bilgilerin korunmasına yönelik arayışını sürdürmektedir. İletişim ve sanal gruplarla etkileşim gereksinimi kişisel kullanımların ötesinde, kurumsal çözüm ve politika geliştirme arayışlarında da hissedilmektedir (Akbaş & Fenerci, 2016; Gülaslan, 2018, s. 180-200; Yalçınkaya, 2020, s. 25). Bu tür çözümler sunulurken, mahremiyetin korunmasının hukuksal sorumluluklar kapsamında garanti altına alınması ya da garanti edilemiyorsa politikalarda bunun açık bir şekilde belirtilmesi gerekmektedir (American Library Association [ALA], 2018, s. 6-7).

Bilgi ve iletişim teknolojilerindeki gelişmeler, sosyalleşme ve sanal gruplarla etkileşimi kolaylaştırırken, özel hayatın gizliliğine yönelik riskleri arttırmaktadır. Elektronik ortamlarda bilginin işlenme süreçlerindeki tüm aşamalarda, bilgi ve iletişim teknolojileri kullanılarak özel hayatın gizliliğini hedef alan suçların arttığı bilinmektedir. Bu risklerin azaltılabilmesi için hukuksal düzenlemelerin bilgi ve iletişim teknolojilerindeki gelişmelere bağlı olarak güncellenmesi ve var olan düzenlemelere ilişkin farkındalığın arttırılması gerekmektedir. 5237 Sayılı Türk Ceza Kanunu'ndaki (TCK) özel hayata ve özel hayatın gizli alanına karşı işlenen suçlara ilişkin Yargıtay kararlarının bulunduğu 2006-2021 yılları arasındaki süreç dikkate alındığında, bu suçların işlenmesinde kullanılan ve bu suçların işlenmesini kolaylaştıran bilgi ve iletişim teknolojilerine ilişkin durum ortaya konulabilmektedir.

Sosyal medya kullanımının yaygınlaşmasıyla birlikte, "özel hayata ve hayatın gizli alanına karşı suçların" sosyal ağ sağlayıcılar üzerinden işlenmesinin daha kolay hale geldiği görülmektedir. Bu durum, bilginin işlendiği ortamlardaki değişikliğin ve bireylerin bilgi davranışının[2] doğal bir sonucudur. Sosyal medya kullanımı konusunda bireylerin iş yaşantısı ile özel yaşantısı arasındaki sınırın belirlenerek birbirinden ayrılması da çoğu zaman mümkün olamamaktadır (Gülaslan, 2018, s. 175, 248).

Bilginin kullanılabilirliği için, toplanması, saklanması, paylaşılması ve erişilebilir hale getirilmesi önem taşımaktadır. Bu amaca uygun olarak saklanan ve erişilebilir hale getirilen bilgiler tarihsel süreç içinde değerli hale gelirken, hukuka aykırı olarak elde edilen, saklanan ve dağıtılan bilgiler yaşanmakta olan süreç için sorun haline gelebilmektedir. TCK gerekçesinde de (2004) 135. maddeye ilişkin olarak belirtildiği gibi, çağımızda kişilerle ilgili kayıtlar, kurumlar tarafından bilgisayar ortamlarına aktarılmakta ve muhafaza edilmektedir. Bu bilgilerin önceden belirtilmiş amacın dışında kullanılması ya da üçüncü şahıslar tarafından hukuka aykırı olarak yararlanılması nedeniyle, söz konusu bilgilerin sahipleri telafisi mümkün olmayan zararlara uğrayabilmektedirler. Bu nedenle gündelik yaşamda özel hayata ve özel hayatın gizli alanına karşı saygılı olunması ve bu konuda işlenen suç oranlarının azaltılabilmesi için, kişilerin günlük yaşamlarında pratik olarak kullanmış oldukları ve sezgi ya da sağduyuya dayalı günlük bilgileri[3] içinde, günlük yaşamın parçası olarak bu konudaki hukuksal yaklaşıma ilişkin bilgilerin de olması önem taşımaktadır. Böylece kişisel hakların ihlâline neden olmayan, olumlu sonuçlara yol açan kullanımın da desteklenebileceği düşünülmektedir (Junco, 2011, s. 60). Konuya ilişkin kurumsal risklerin arttığı son yıllarda, Türk Kütüphaneciler Derneği (TKD) gibi meslek kuruluşları bünyesinde oluşturulan sosyal

[2] Bilgi davranışı, bireylerin bilgiye nasıl yaklaştığını ve işlediğini ifade eder. Bireyin bilgiyi araması, kullanması, değiştirmesi, paylaşması, depolaması ve hatta görmezden gelmesi bilgi arama davranışı kapsamımda değerlendirilebilir (Davenport, 1997, s. 83).

[3] Gündelik bilgi, insanın düşüncelerine, duyu verilerine, kendine özgü yaşam deneyimine, içinde bulunduğu çevrenin geleneklerine bağlı olarak edindiği, çoğunlukla pratik ihtiyaçlarını gidermeğe yönelik olarak ve yaşama uyum sağlamak için kullandığı bilgi türüdür (Gürkan, 2019, s.1).

medya politikalarında da özel hayatın gizliliğine ilişkin hukuksal düzenlemelere dikkat çekildiği görülmektedir (TKD, 2018, s. 6).

Çalışma kapsamında irdelenen ve gündemde sıklıkla yer alan bilgi ve iletişim teknolojileri ile "özel hayata ve özel hayatın gizli alanına karşı işlenen suçlara" ilişkin Yargıtay kararları, elektronik ortamda üretilen bilgilere yönelik olarak nasıl bir tutumun gösterilmesi gerektiği hakkında fikir vermekte ve yol gösterici olabilmektedir. Hukuk ve ceza mahkemeleri kararlarının son merci tarafından karara bağlanmış hali olan Yargıtay kararları, somut olayın özelliğine bağlı olarak uygulamaya yönelik en kapsamlı değerlendirme örneklerini sunan hukuksal kaynaklardır. Yargıtay içtihat metinlerinde yer alan açıklamalar, özel hayatın gizliliğine ve bu konuya yönelik olarak uygulamada tereddütlerin bulunduğu hususların yorumlanmasına yardımcı olan önemli bir kaynak niteliği taşımaktadır. Bu nedenle çalışma kapsamında TCK'nın dokuzuncu bölümünde "özel hayata ve özel hayatın gizli alanına karşı suçlar" şeklinde düzenlenen suçlara yönelik Yargıtay kararları incelenmiştir. Çalışmada öncelikle "özel hayata ve hayatın gizli alanına karşı suçlar" hakkında genel bilgi sunulmuş ve araştırmada kullanılan hukuk bilgi bankası üzerinden erişilen konuya ilişkin tüm Yargıtay kararları incelenerek bu çerçevede değerlendirilmiştir.

Çalışmanın Amacı ve Soruları

Bu çalışmada, "özel hayata ve hayatın gizli alanına karşı suçlara" ilişkin Yargıtay kararları incelenerek, elektronik ortamlarda özel hayata karşı işlenen suçlarda bilgi ve iletişim teknolojilerinin rolü ortaya konulmuştur. Günümüzde bilginin çok büyük bir bölümü elektronik ortamlarda işlendiği gibi, "özel hayata ve özel hayatın gizli alanına karşı işlenen suçların" da büyük bölümü elektronik ortamda ve bilişim sistemleri aracılığıyla işlenmektedir (Tripathi ve diğerleri, 2016, s. 24). Bu durum, yapılacak hukuksal düzenlemelerde, mevcut düzenlemelere ilişkin karar verme süreçlerinde ve bilgi yönetim süreçlerinde, elektronik ortamlarda ve bilişim sistemleri aracılığıyla işlenen bilginin özel hayata yönelik durumunun dikkate alınmasını gerektirmektedir. Bazı mesleki kuruluşlar (TKD, 2018, s. 6) özel hayata ve hayatın gizli alanına karşı artan tehditlere sosyal medya politikalarında dikkat çekerek konuya ilişkin hukuksal düzenlemeleri işaret ederken, bu suçların nasıl işlendiği ve hukuksal düzenlemelerin nasıl yorumlanması gerektiği konusunda açıklayıcı bilgiler bulunmamaktadır. Bu çerçevede, çalışmada doğrudan Yargıtay kararlarını merkeze alarak Ceza Hukuku çerçevesinde değerlendirme yapılmamış, araştırma evreninde yer alan Yargıtay kararları kapsamında bilgi ve iletişim teknolojileriyle özel hayata karşı işlenen suçların incelenmesi hedef alınmıştır.

Çalışmada, hukuksal düzenlemelerin yorumlanmasını kolaylaştıran ve uygulama açısından yol gösterici olan Yargıtay kararları çerçevesinde mevcut durum ortaya konularak, konuya ilişkin karar vericilerin ve bilgi profesyonellerinin farkındalığının arttırılması amaçlanmıştır. Bu amaç doğrultusunda aşağıdaki araştırma sorularına yanıt aranmaktadır:

- Elektronik ortamlarda özel hayata ve hayatın gizli alanına karşı işlenen suçlar nelerdir?
- Özel hayatın gizliliğinin ihlâline yönelik suçlar hangi yöntemlerle ve ne kadarı bilgi ve iletişim teknolojileri ile birlikte elektronik ortamlar kullanılarak işlenmektedir?
- Özel hayata ve hayatın gizli alanına karşı bilgi ve iletişim teknolojileri kullanılarak işlenen suçlara ilişkin uygulamada ne tür yanılgılar ya da farklı görüşlerle karşılaşılmaktadır?
- Elektronik ortamlarda haberleşmenin gizliliğini ihlâl, kişiler arasındaki konuşmaların dinlenmesi ve kaydedilmesi, özel hayatın gizliliğini ihlâl, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak

verme ya da ele geçirme ve verileri yok etmeme suçlarına yönelik Yargıtay'ın karar ve değerlendirmeleri nasıldır?

Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar

Özel hayat, kişinin göz önünde olmayan, kamuya kapalı ve diğer insanlardan gizlediği hayatıdır. Bir kişinin gizliliğine her ne şekilde olursa olsun girilmesi, özel hayatın gizliliğinin ihlâli olarak değerlendirilmektedir (Hafızoğulları & Özen, 2009). Özel hayat kavramı, kişinin diğer insanlarla paylaşmadığı yaşantısı ve mahremiyeti ile sınırlı olmayıp, herkesin bilmemesi gereken ve/veya istenildiğinde başkalarına açıklanabilen bilgilerin tamamını içermektedir.

Özel hayatın gizliliği ve korunması hakkı, "kişilerin kendi kişiliklerini geliştirmek, manevi değerlerine güvence sağlamak amacıyla diğer insanlar tarafından bilinmesini istemediği hususların oluşturduğu ve buna bağlı olarak da korunması hukuken gerekli olan hayat alanına yönelik temel şahsiyet hakkı" şeklinde tanımlanmaktadır (Yargıtay, 2012b). Bu nedenle, bir görüntü ya da sesin dinlenmesi ve/veya kaydedilmesinin kamuya açık alanda yapılmış olması, buna rıza gösterildiği anlamını taşımamaktadır. Kamuya açık alanlarda kişinin başkalarınca bilinmesini ve/veya görülmesini istemeyeceği tüm faaliyetler özel hayat kavramı kapsamında değerlendirilmektedir. Bir bilginin, özel hayat kavramı kapsamında yer alıp almadığı belirlenirken, içinde bulunulan çevrenin özelliklerinin yanı sıra, kişinin toplum içindeki konumu, mesleği, tanınırlığı, rıza ve öngörüleri ile müdahalenin derecesi de göz önüne alınmalı ve somut olayın özelliğine göre hukuka uygunluk sebeplerinin bulunup bulunmadığı araştırılmalıdır (Yargıtay, 2012a, 2013b).

Özel hayatın gizliliğine yönelik olarak "herkesin özel ve aile yaşamına saygı gösterilmesini isteme hakkı" Anayasa'nın (1982) 20. maddesinde düzenlenmiş ve bu hak Türk Medeni Kanunu'nun 24. ve 25. Maddeleriyle koruma altına alınmıştır. Kişilik haklarına saldırılması durumunda uygulanacak yaptırımlar ise Borçlar Kanunu'nun 49. maddesinde düzenlenmiştir (Yargıtay, 2010).

Bilgi ve iletişim teknolojilerindeki gelişmeler, hukuka aykırı olarak kişilerin özel konuşmalarının dinlenmesine, özel görüntülerinin izlenmesine ve kaydedilmesine olanak sağlamaktadır. Buna yönelik olarak da Anayasa'nın 22. maddesinde haberleşme hürriyeti düzenlenmiş ve korumaya alınmıştır. Anayasa ile garanti altına alınan özel hayata yönelik eylemlerle, kişinin görüntü ve sesinin bilgi ve rızası dışında gizlice kaydedilerek kişilik hakkına zarar verilmesine ilişkin eylemler, TCK'nın 132, 133. ve 134. maddelerinde "haberleşmenin gizliliğinin ihlâli", "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması", "özel hayatın gizliliğinin ihlâl edilmesi" başlıkları altında ayrı ayrı suç olarak düzenlenmiş ve yaptırıma bağlanmıştır. Bu kayıtların medya yoluyla kamuoyuna sunulması ise kişilik haklarına yönelik ikinci bir saldırı niteliği taşımaktadır (Yargıtay, 2007). TCK'nın 135. ve 136. maddelerinde ise "kişisel verilerin kaydedilmesi", "verilerin hukuka aykırı olarak verilmesi ya da ele geçirilmesine" yönelik suçlar tanımlanarak yaptırıma bağlanmıştır.

Avrupa İnsan Hakları Sözleşmesi'nin (1950) 8. maddesinde de kişilerin aile ve özel yaşamına, konutuna ve haberleşmesine saygılı olunmasını isteme hakkının bulunduğu hükmü yer alırken, bu hakkın sınırlandırılmasının "ulusal ve/veya kamu güvenliği, ülkenin ekonomik refahı, suç işlenmesinin önlenmesi, düzenin korunması, sağlığın veya başkalarının hak ve özgürlüklerinin korunması için gerekli olması durumunda mümkün olabileceği" belirtilmiştir.

Haberleşmenin Gizliliğini İhlâl

Haberleşmenin gizliliğini ihlâl suçu TCK'nın 132. maddesinde düzenlenmiştir. 132. maddenin birinci fıkrasında kişiler arasındaki haberleşmenin gizliliğinin ihlâli, ikinci fıkrasında ifşası (açığa çıkarılması) yaptırım altına alınmıştır. İlgili maddenin üçüncü fıkrasında ise kişinin tarafı olduğu haberleşmenin içeriğinin açığa çıkarılması suç olduğu düzenlenmiştir. Haberleşme içeriğinin öğrenilmesi, görülmesi, duyulması, dinlenmesi ya da kayıt edilmesi eylemlerinin tamamlanması halinde suç oluşurken, yarım kalması fiili bu suça yönelik teşebbüsü oluşturmaktadır (Hafızoğulları & Özen, 2009, s. 11). Suçun sadece kastla (bilerek ve isteyerek) işlenebilmesi nedeniyle, dikkatsizlik ve özensizlik sonucunda haberleşmenin gizliliğinin ihlâl edilmesi halinde suç oluşmayacaktır.

132. maddenin birinci fıkrasında, en az iki kişinin, diğer insanların bilmemeleri gerektiğini düşünerek ve gizliliği sağlamaya çalışarak, uygun araç (internet, telefon, mektup, kâğıt vd.) ve sembollerle (söz, yazı, işaret vd.) paylaştıkları bilgi ve düşüncelerinin, özel hayata yönelik olsun veya olmasın, özel bir çaba sarf edilerek, doğrudan veya dolaylı şekilde, başka kişiler tarafından, okunmak veya dinlenmek suretiyle öğrenilmesi eylemi suç olarak tanımlanmıştır. Buna göre haberleşenler dışında herkesin bu suçun faili olabilmesine karşın, haberleşmenin tarafı olan kişiler suçun faili olamamaktadır. Haberleşme kişiler arasında sınırlı olduğu için, suçun mağdurları haberleşen kişilerdir (Hafızoğulları & Özen, 2009, s. 10). Birinci fıkrada aynı zamanda, anlaşılabilir olsun ya da olmasın, yazı, ses, görüntü, özel işaretler gibi başkalarının haberleşme içeriklerinin, kâğıt, manyetik bant, bellek vb. nesne üzerine aktarılarak kaydedilmesi suçun nitelikli şekli olarak tanımlanmıştır. Bu nesneler üzerindeki haberleşmeye ilişkin gizlilik, nesne üzerinde yer alan bilgi ve bu bilginin alıcısı dışında başkaları tarafından öğrenilmesi ile ilgilidir.

132. maddenin ikinci fıkrasında, ilgililerin rızası dışında haberleşme içeriğinin öğrenme yetkisi bulunmayan kişilere yayılması, açığa vurulması ve/veya kamuoyuna duyurulması eylemi suç olarak düzenlenmiştir. Haberleşme içeriği hukuka uygun olarak öğrenilmiş olsa dahi, bu içeriklerin yetkisiz kişilerce öğrenilmesinin sağlanması suçun oluşması için yeterlidir. TCK gerekçesinde de (2004), soruşturma aşamasında haberleşme içeriklerinin televizyonlarda ya da gazetelerde yayınlanmasının, hukuka uygun olarak kayda alınmış olsalar dahi bu suçu oluşacağı belirtilmektedir.

132. maddenin üçüncü fıkrasında ise kişinin kendisiyle yapılan haberleşme içeriğini, ilgililerinin rızası dışında, en az iki kişi tarafından algılanabilme olanağı bulunan aleni ortamda açığa çıkarması eylemi "haberleşmenin gizliliğini ihlâl" suçu çerçevesinde düzenlenmiştir. Bu düzenleme kapsamında suçun oluşması için açığa çıkarmanın alenen yapılmış olması önem taşımaktadır. Bu nedenle TCK gerekçesinde (2004), öğrenilen bilginin ilgili kişinin rızası olmaksızın alenen duyurulması ya da sosyal medya vd. ortamlardan başkalarının erişimine sunulması halinde suçun oluşacağı belirtilmektedir. Açığa çıkarmanın basın ve yayın aracılığıyla yapılması halinde, 132. maddenin dördüncü fıkrası gereğince verilecek cezanın artırılması öngörülmüştür.

Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması

Anayasanın (1982) 22. maddesi gereğince haberleşmenin gizliliği esastır ve hukuksal zorunluluklar olmadıkça, başkaları ile olan konuşmalarının alenileştirilmesine kişiler sadece kendileri karar verirler. "İki veya daha fazla kişinin, belirli sayıda dinleyici çevresi dışına çıkmayacağını düşünerek yüz yüze gerçekleştirdikleri sesli düşünce ve açıklamaları, konuşmanın tarafı olmayan kişilerce, ilgilisinin rızası olmadan, uygun bir aletle (duyulabilir ve/veya algılanabilir hale getirmeye yarayan bir düzenekle) dinlenmesi ya da kaydedilmesi", TCK'nın 133/1. madde ve fıkrasında suç olarak tanımlanmıştır (Yargıtay, 2014d, 2014c). Burada tanımlanan suç seçimlik hareketli

olmasına karşın, dinleme ve kaydetmenin birlikte yapılması halinde tek bir suç işlenmiş olmaktadır ve temel ceza yüksek tutulmaktadır (Hafızoğulları & Özen, 2009, s. 14). TCK gerekçesinde (2004) aleni olma durumuna ilişkin olarak konuşmanın yapıldığı yerin öneminin olmadığı, özel çaba harcanarak duyulabilmesi durumunda aleni olmayan konuşmanın söz konusu olacağı belirtilmektedir. Bu suçu konuşmanın tarafı olmayan kişi işleyebilmektedir. Kast ile dinleme ya da kaydetme işlemi başladığı anda suç tamamlanmış olarak kabul edilmektedir. Ancak konuşmaları dinlemenin ya da kaydetmenin, bunu mümkün kılan bir aletle yapılmış olması önemlidir. Suçun mağdurları ise aralarındaki konuşmanın dinlenmesi ya da kaydedilmesine rıza göstermeyen kişilerdir. Konuşmayı yapanlardan birinin rızasının olmaması suçun oluşması için yeterli iken, taraflardan birinin rızasının olması suçun oluşmasına engel değildir. Konuşma esnasında hakaret, tehdit veya şantaj içeren sözlerle karşı karşıya kalan ve buna bağlı olarak konuşmaları kaydeden mağdurun bu şekilde elde ettiği delil ise hukuka uygun olarak kabul edilmektedir. Bu noktada kaydetme işleminin gerçekleşmekte olan bir haksız saldırıya karşı yapıldığı, kayıtları takip organlarına verme işlemininse tekrarı mümkün olan haksız saldırıya yönelik olarak yapıldığı düşünülmekte ve her iki hareketin de meşru savunma sınırları içinde gerçekleştiği değerlendirilmektedir (Tezcan ve diğerleri, 2013, s. 545).

TCK'nın 133/2. madde ve fıkrasında ise üç ya da daha fazla kişinin, yüz yüze yapılan ve aleni olmayan söze dayalı düşünce paylaşımının, ilgililerinin rızası bulunmamasına karşın, konuşmanın tarafı olan kişilerce bir ses alma cihazıyla kaydedilmesi suç olarak tanımlanmıştır. Söyleşiye katılanlardan birinin, kayda elverişli bir cihaz ile söyleşinin bir parçasını dahi diğer katılanların rızası olmaksızın kaydetmiş olması, suçun oluşması için yeterlidir.

Kişiler arasındaki aleni olmayan konuşmanın kaydedilmesi yoluyla elde edilen bilgilerin hukuka aykırı olarak açığa çıkarılması eylemi TCK'nın 133/3. madde ve fıkrasında suç olarak düzenlenmiştir (Yargıtay, 2014f, 2014c). TCK gerekçesine (2004) dayalı başka bir ifadeyle, TCK'nın 133/1. ve 133/2. maddesinde tanımlanan suçların işlenerek elde edildiği verilerden yarar sağlanması, üçüncü kişilere verilmesi ya da başkalarının bilgi edinmesinin sağlanması suç olarak tanımlanmıştır. Örneğin birçok kurum ve kuruluşun yardım masası vb. isimler altında destek sunan birimlerinde kaydedilen konuşmaların e-posta vb. araçlarla başkalarına verilmesi bu suç kapsamında değerlendirilmektedir. Bu konuşmaların bir web sayfası üzerinden yayınlanması ise basın ve yayın yoluyla yayımlanması suçunu oluşturmaktadır (Avşar & Öngören, 2010, s. 153). Verilerin basın ve yayın yoluyla yayımlanmasına yönelik olarak TCK'nın 133/3. madde ve fıkrasında belirtilen ceza ile TCK gerekçesinde (2004) öngörülen ceza arasında çelişkiler olmakla birlikte, asıl olan TCK'nın 133/3. madde ve fıkrasında aynı cezaya hükmolunacağı belirtilmektedir. TCK'nın 133. maddesi kapsamında işlenen suçların takibi şikâyete bağlıdır.

Özel Hayatın Gizliliğini İhlâl

"Özel hayatın gizliliğini ihlâl" suçları TCK'nın 134. maddesinde düzenlenmiştir. 134. maddenin birinci fıkrasında "özel hayatın gizliliğini ihlâl ve gizliliğin görüntü ve/veya seslerin kayda alınmasıyla ihlâli" suç olarak tanımlanmıştır. İkinci fıkrada kişilerin "özel hayatına yönelik görüntü ya da seslerin hukuka aykırı olarak açığa çıkarılması" suç olarak tanımlanmıştır.

TCK gerekçesinde (2004), hukuka aykırı olarak açığa çıkarılan görüntü ya da seslerin hukuka uygun olarak kayda alınmış olabileceği gibi, birinci fıkrada ifade edilen suçun işlenmesi suretiyle de elde edilmiş olabileceği belirtilmektedir. İkinci fıkrada belirtilen suçun oluşabilmesi için, hukuka aykırı olması ve ses ya da görüntü kayıtlarının açığa çıkarılarak yetkisiz kişiler tarafından öğrenilmesinin sağlanması yeterlidir. Hata ile farklı bir

kişinin özel hayatına yönelik görüntü ve/veya seslerin ihlâl edilmesi halinde, suçun varlığı ortadan kalkmamaktadır.

Özel hayatın gizliliğini ihlâl suçu kastla işlenen, yani failin, bir kişinin özel hayatını ihlâl ettiğini bilerek ve isteyerek davranışına devam ettiği bir suçtur. Gizliliğin görüntü ya da seslerin kayda alınarak ihlâl edilmesi durumunda cezanın alt sınırının ağırlaştırılması öngörülmüştür. Suçun takibi şikâyete bağlıdır.

Kişisel Verilerin Kaydedilmesi

Kişisel verilerin korunmasına yönelik düzenlemelerin amacı, kişisel veriler işlenirken özel hayatın gizliliğini ve kişilerin temel haklarını korumaktır. Bunun için kişisel verileri işleyenlerin yükümlülükleri ile uyulması gereken usul ve esaslar düzenlenmektedir (Kişisel Verilerin Korunması Kanunu [KVKK], 2016). TCK gerekçesinde (2004) ve KVKK'nın (2016) 3. maddesinde tanımlanan, "kimliği belirli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilginin hukuka aykırı olarak kaydedilmesi", TCK'nın 135. maddesinde suç olarak tanımlanmıştır. KVKK'nın gerekçesinde (Kişisel Verileri Koruma Kurumu [KVK Kurumu], 2019) 3. maddeye ilişkin açıklamalarda belirtildiği gibi, ad, soyad ve doğum tarihi gibi kesin teşhisi sağlayan verilerin yanı sıra, kişi ile ilişkilendirilen ve kişiyi belirlenebilir kılan fiziksel, ailevi, psikolojik, ekonomik, sosyal ve kültürel kimliği ifade eden veriler de kişisel veri olarak nitelendirilmektedir. Bilgi ve iletişim teknolojinin gelişimine bağlı olarak, elektronik ortamlarda belirli hizmetleri almak amacıyla edinilen kimlik bilgileri de (e-posta adresi, kullanıcı hesap bilgileri vb.) kişi ile ilişkilendirilmesi halinde bu kapsamda değerlendirilmektedir.

TCK gerekçesinde (2004) belirtildiği gibi, kişisel verilerin bilgisayar ya da kâğıt üzerinde kayda alınması, suçun oluşması açısından önem taşımamaktadır. Suçun meydana gelmesi için kişisel verilerin hukuka aykırı olarak kaydedilmesi gerekirken, ilgili kişinin rızasının bulunması ya da kamu hizmetlerinin gereği olarak kanun hükümlerine istinaden kişisel bilgilerin kayda alınması halinde suç oluşmamaktadır. TCK'nın 135/2. madde ve fıkrasında ise özel nitelikli kişisel veri olarak da nitelendirilen (KVKK, 2016), kişilerin ahlaki eğilimlerine, siyasi, felsefi ya da dini görüşlerine, cinsel yaşamlarına, ırki kökenlerine, sağlık durumlarına ya da sendikal bağlantılarına yönelik bilgilerin kaydedilmesi suç olarak tanımlanmıştır. Hassas verilerin kaydedilmesine yönelik olarak hukuka aykırılık vurgusunun yapılmamış olması, bu bilgilerin kaydedilmesinin her koşulda hukuka aykırı olduğunu göstermektedir. TCK gerekçesinde (2004), bu bilgilerin suçlulukla mücadelede, suçluların ortaya çıkarılmasını sağlamak amacıyla belli ölçüde kaydedilmesine izin verilebileceği ifade edilmektedir.

Kişisel verilerin hukuka aykırı olarak kayıt altına alınması işlemiyle suç tamamlanmaktadır. Ayrıca bir neticesinin olması gerekmemektedir. "Kişisel verilerin hukuka aykırı olarak kaydedilmesi" suçu kastla işlenen suçlardan olup, eylemin kamu görevlisi tarafından görevin sağladığı yetki kötüye kullanılarak ya da bir mesleğin/sanatın sunduğu kolaylıktan yararlanılarak gerçekleşmesi halinde, TCK'nın 137. maddesi gereğince cezada artırım uygulanması gerekmektedir. Kişisel verilerin kaydedilmesine ilişkin suçlar TCK'nın 139. maddesi gereğince resen takip edilmektedir.

Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme

"Verilerin hukuka aykırı olarak verilmesi ya da ele geçirilmesi", TCK'nın 136/1. madde ve fıkrasında suç olarak düzenlenmiştir. Bu madde hükmüne göre kişisel verilerin hukuka uygun olarak kaydedilmiş olup olmadığına bakılmaksızın hukuka aykırı olarak elde edilmesi, başkalarına verilmesi ya da yayılması suç olarak tanımlanmıştır (Türk Ceza Kanunu Gerekçesi, 2004; Yargıtay, 2018f). "TCK'nın 135. maddesinde olduğu gibi, 136. maddesinde

de genel olarak korunan hukuki değer kişilerin özel hayatı iken özelde kişisel verilerdir. Kişisel verilerin korunmasına yönelik suçlarda korunan hukuki değer "sır" değil, veri sahibinin kişilik haklarıdır (Dülger, 2004, s. 579). TCK'nın 135. ve 136. maddelerinde sadece sır niteliğini taşıyan kişisel verilerin korunacağına dair bir hüküm bulunmamaktadır. Bununla beraber TCK'nın 135. maddesinin gerekçesinde gerçek kişiye ilişkin tüm bilgilerin kişisel veri olarak kabul edileceği belirtilmektedir. Bu nedenle her türlü kişisel verinin hukuka aykırı olarak ele geçirilmesi, verilmesi veya yayılması halinde TCK'nın 136. maddesinde tanımlanan suçun oluştuğu söylenebilir (Yargıtay, 2018h).

"Kişisel verilerin hukuka aykırı olarak ele geçirilmesi, başkalarına verilmesi ya da yayılması" suçu, genel kastla işlenen suçlardandır (Yargıtay, 2017f). Bu suçlar TCK'nın 139. maddesi gereğince resen takip edilmektedir.

"Haberleşmenin gizliliğini ihlâl", "kişiler arasındaki konuşmaların kayda alınması ve/veya dinlenmesi", "kişisel verilerin kaydedilmesi", "özel hayatın gizliliğini ihlâl" ve "verileri hukuka aykırı olarak verme ya da ele geçirmeye" yönelik suçların kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılarak ya da bir mesleğin/sanatın sağladığı kolaylıktan yararlanılarak işlenmesi, TCK'nın 137. Maddesi gereğince cezada artırım nedenleri arasında sayılmıştır.

Verileri Yok Etmeme

Kullanılma amaçları yönünden bazı kişisel verilerin saklanma süresi kanunla sınırlandırılabilmektedir. Belirlenen süre sonunda, özel hayata ilişkin gizliliğinin korunması kapsamında bu verilerin yok edilmesi gerekmektedir. Hukuka uygun bir şekilde kaydedilmesine karşın kanunlarda belirlenen süresi geçmiş olan "kişisel verilerin yok edilmemesi", TCK'nın 138. maddesinde bağımsız bir suç olarak tanımlanmıştır. Elektronik ortamda yer alan verilerin yok edilmesi için tüm kopyalarının kalıcı olarak silinmesi ve bir örneğinin kalmaması gerekmektedir (Akdağ, 2013, s. 148). Verilerin, kullanım süresi aşıldıktan sonra yok edilmesi, suçun varlığını ortadan kaldırmamaktadır. Bunun yanı sıra, suçun tamamlanmış sayılması için bir zararın oluşması şartı bulunmamaktadır.

Verileri yok etmeme suçu, silinme koşulları gerçekleşmesine rağmen bu görevi yerine getirmekle yükümlü kişilerin görevlerini ihmal etmeleri ile gerçekleşmektedir (Şen, 2006, s. 611). Bu nedenle suçun faili, süresi geçmiş olan kişisel verileri yasalar çerçevesinde yok etmekle yükümlü kişilerdir (Akdağ, 2013, s. 144). KVKK'nın (2016) 7. maddesinde, kişisel verilerin işlenmesini gerektiren nedenler ortadan kalktığında, veri sorumlusu[4] tarafından resen ya da veri sahibinin isteği nedeniyle yok edileceği belirtilmektedir. Bu kanunun 17. maddesinde ise 7. maddeye aykırı olarak bu verileri silmeyen veya anonimleştirmeyenler için TCK'nın 138. maddesinin uygulanacağı belirtilmektedir. Mağdurun bu konuda rıza göstermesi de kastla işlenen bu suçun oluşumuna engel değildir. Süresi geçen verilerin yok edilmemesine ilişkin suçlar TCK'nın 139. maddesi gereğince resen takip edilmektedir.

Yöntem

Araştırmanın Deseni

Özel hayatın gizliliğinin ihlâline yönelik suçların hangi yöntemlerle ve ne kadarının bilgi ve iletişim teknolojileri kullanılarak işlendiğinin, özel hayata ve hayatın gizli alanına karşı bilgi ve iletişim teknolojileri kullanılarak

[4] Kişisel Verilerin Korunması Kanunu'nun (2016) 3. Maddesinde veri sorumlusu; "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" olarak tanımlanmaktadır.

işlenen suçlara ilişkin uygulamada ne tür yanılgıların ya da farklı görüşlerin bulunduğunun ve Yargıtay'ın bu suçlara ilişkin karar ve değerlendirmelerinin neler olduğunun, HukukTürk bilgi bankası üzerinden erişim sağlanan toplam 129 Yargıtay kararı üzerinden ortaya konulmasını sağlayan bu çalışmada betimleme yöntemi (modeli) kullanılmıştır. Betimleme modeli, geçmişte ya da halen var olan ve araştırma konusunu oluşturan bir durumu herhangi bir müdahalede bulunmaksızın mevcut haliyle betimlemeyi hedefleyen araştırma modelidir (Karasar, 2012, s.77).

Evren ve Örneklem

Araştırmanın evrenini, TCK'da "özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında tanımlanan suçlara yönelik olarak HukukTürk bilgi bankası üzerinden erişim sağlanan toplam 129 Yargıtay kararı oluşturmaktadır. Yargıtay kararları, hukuk ve ceza mahkemeleri kararlarının son merci tarafından karara bağlanmış hali olması ve uygulama için referans sağlayan hukuksal kaynaklar olması açısından önem taşımaktadır. Çalışmada Yargıtay kararları içinde yer alan açıklamalar, dikkate alınması gereken en önemli kaynaklardan biri olarak özel hayata karşı işlenen suçlara yönelik uygulamada yanılgıların ya da farklı görüşlerin olduğu görülen hususların yorumlanmasına yardımcı olmaktadır.

Araştırma evreninde yer alan Yargıtay kararlarının belirlenmesinde HukukTürk bilgi bankasından yararlanılmıştır. HukukTürk bilgi bankası, çalışmanın araştırma amacına uygun olarak kararların madde bazında sınıflandırılmasında kolaylık sağlaması ve madde bazında yapılan aramalarda ilgililiğin yüksek olması nedeniyle tercih edilmiştir. TCK'nın yürürlüğe girdiği 2005 yılından 2022 yılına kadar olan sürece ilişkin olarak, HukukTürk bilgi bankasında bulunan "özel hayata ve hayatın gizli alanına karşı suçlara" yönelik 129 Yargıtay kararı araştırma kapsamında ele alınmıştır. Araştırmada örneklem seçme yöntemine başvurulmamış, araştırma konusu ile ilgili HukukTürk bilgi bankası üzerinde yer alan 129 Yargıtay kararı araştırmaya dahil edilerek tam sayım yöntemi (Lin, 1976, s. 164) kullanılmıştır.

Veri Toplama Süreci

Özel hayata ve hayatın gizli alanına karşı suçların, TCK'nın 132,133,134,135,136. ve 138. maddelerinde düzenlendiği görülmektedir. "Özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında tanımlanan bu suçlar;

- Haberleşmenin gizliliğinin ihlâli,
- Kişiler arasındaki konuşmaların dinlenmesi ve/veya kayda alınması,
- Özel hayatın gizliliğini ihlâl,
- Kişisel verilerin kaydedilmesi,
- Verileri hukuka aykırı olarak verme ya da ele geçirme ve
- Verileri yok etmeme suçlarıdır.

Araştırmada öncelikle bu suçların hangi eylemlerin sonucunda oluşacağı, suçun nasıl ve kimler tarafından işlenebileceği, suçun mağdurunun kim ya da kimler olabileceği, suçun takibinin nasıl yapılacağı ve suça ilişkin yaptırımları içeren hukuksal koşullar hakkında temel bilgi sunulması amaçlanmıştır. Bu nedenle çalışmanın ilk bölümünde TCK madde gerekçeleri ve Yargıtay kararları içindeki açıklamalar ağırlıklı olmak üzere, konuya ilişkin literatürden yararlanılarak bilgi sunulmuştur. Bu kapsamda, yukarıda belirtilen suçlar ayrı alt başlıklar halinde

yapılandırılmıştır. Yargıtay kararları içindeki açıklamalar için, araştırma evrenini oluşturan 129 Yargıtay kararlarına hukuk bilgi bankası üzerinden erişim sağlanmıştır.

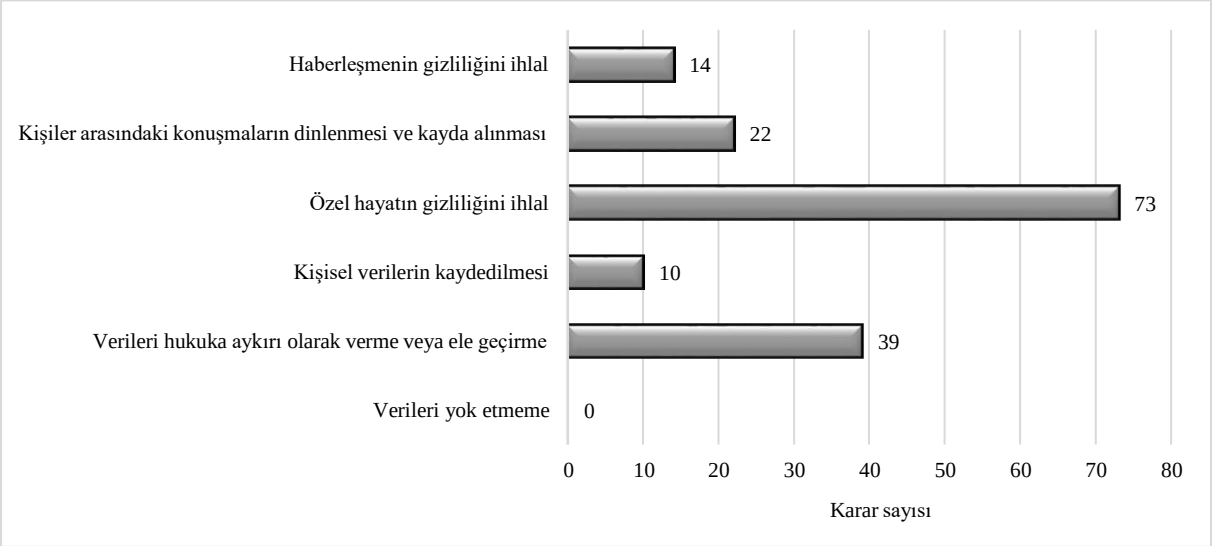
Yargıtay kararlarının araştırma soruları çerçevesinde incelenmesi için, bu çalışmada yararlanılan hukuk bilgi bankası üzerinden erişim sağlanan ve TCK'da "özel hayata ve hayatın gizli alanına karşı suçlar" başlığı altında düzenlenen maddelere ilişkin içeriğe sahip olan 129 Yargıtay kararı tespit edilmiştir. Bu işlem esnasında her madde için ayrı ayrı tespitler yapılmış ve ilgili Yargıtay kararları değerlendirilmek üzere her madde için ayrı ayrı sınıflandırılmıştır. TCK'da ilgili başlık altında yer alan düzenlemelerin madde isimleri, veri toplama ve değerlendirme işlemlerinin daha anlaşılır olması için yapılan sınıflandırmada ve alt başlıkların oluşturulmasında herhangi bir değişiklik yapılmadan kullanılmıştır. Bu aşamada elektronik ortamlarda özel hayata karşı bilgi ve iletişim teknolojileri vasıtasıyla işlenen suçların Yargıtay kararları içindeki ağırlığı ve Yargıtay kararlarında konunun bu yönüne dikkat çeken değerlendirmelerine ilişkin veriler toplanmıştır.

Verilerin Analizi

Araştırma kapsamında toplanan verilerin analizinde yüzde (%) ve frekans (f) gibi betimsel istatistiklerden faydalanılmış, analiz sürecinde "Microsoft® Excel® 2019" programı kullanılmıştır. Değerlendirmeler sonucunda, elektronik ortamlarda "haberleşmenin gizliliğini ihlâl", "kişisel verilerin kaydedilmesi", "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması", "özel hayatın gizliliğini ihlâl", "verileri hukuka aykırı olarak verme veya ele geçirme" ve "verileri yok etmeme" suçlarına ilişkin Yargıtay'ın görüş ve değerlendirmeleri ortaya konulmaya çalışılmıştır. Yargıtay öncesindeki süreçlerde, bu suçların nasıl değerlendirildiği ve bu suçların oluşumuna neden olan eylemlere yönelik hangi yaklaşımlar sonucunda yanılgıların oluştuğu tespit edilmiştir. Bununla beraber, incelenen Yargıtay kararları üzerinden, özel hayatın gizliliğinin ihlâlinde ve buna ilişkin karar süreçlerinde, bilgi ve iletişim teknolojilerinin kullanımının hangi boyutlarda olduğuna yönelik fikir edinilmeye çalışılmıştır.

Bulgular

TCK'nın 9. Bölümünde "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında düzenlenen suç türleri ve her bir suç türünün konusu ile ilgili çalışma kapsamında incelenen kaç adet Yargıtay kararı bulunduğuna ilişkin bilgiler Şekil 1 üzerinde gösterilmektedir.



Şekil 1. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlara İlişkin Yargıtay Karar Sayıları

Çalışma bulguları genel olarak suç türlerine ilişkin alt başlıklarda ortak noktalar üzerinden verilirken, konuya ilişkin öğretici bilgi içeren ya da yanılgıya neden olan yaklaşımlara ilişkin açıklamaların bulunduğu Yargıtay kararları özel olarak belirtilmiştir.

Haberleşmenin Gizliliğini İhlâl

Haberleşmenin gizliliğinin ihlâl edilmesi ile kişiler arasındaki konuşmaların dinlenmesi ve kayda alınmasına yönelik eylemlerin birçok Yargıtay kararında birlikte değerlendirildiği görülmektedir. Bu nedenle her iki eylem için de geçerli olan ve iç içe geçen açıklamaların bulunduğu Yargıtay kararlarının, "Haberleşmenin Gizliliğini İhlâl" ve "Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması" başlıklı bölümlerde birlikte incelenmesi gerektiği düşünülmektedir. Şekil 1 üzerinde yer alan "haberleşmenin gizliliğini ihlâl" ve "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçlarına yönelik toplam 36 Yargıtay kararının 18'inde (%50), detaylı ve standart bir açıklamanın yapıldığı görülmektedir. Yargıtay (2012e, 2014f, 2014g, 2014b) kararlarından açıkça anlaşıldığı gibi, TCK'nın 132. ve 133. maddesi kapsamında düzenlenen "haberleşmenin gizliliğini ihlâl" ve "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçlarına ilişkin olarak, "kişinin, sonradan kanıt elde etme imkânının olmadığı ve yetkili makamlara başvurma olanağının bulunmadığı ani gelişen durumlarda (örneğin; kendisine karşı işlenmekte olan cinsel saldırı, tehdit, hakaret, şantaj, iftira vb. bir suç söz konusu olduğunda)" hukuka aykırılık bulunmamaktadır. Benzer şekilde, "kendisini ya da aile birliğini hedef alan haksız bir saldırıyı önlemek için, kaybolma riski bulunan kanıtların kaybolmasını engelleyerek ve yetkili makamlara ulaştırarak güvence altına almak için, saldırıyı yapan tarafın rızası ve bilgisi dışında, haberleşme içeriklerini ya da özel hayata yönelik ses ve görüntülerini kaydetme, dinleme ya da izleme eylemleriyle kişisel verileri ele geçirme, kaydetme ve yayma eylemleri" hukuka aykırı olarak kabul edilmemektedir. Esasen bu durumda, kişinin hukuka aykırı olduğu bilinciyle hareket ettiğinden de söz edilemeyeceği belirtilmektedir. TCK'nın 132. maddesi kapsamında haberleşmenin gizliliğini ihlâl suçuna yönelik 14 Yargıtay kararının 6'sında (%43) ve TCK'nın 133. maddesi kapsamında "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçuna ilişkin 22 Yargıtay kararının 7'sinde (%32) bu hususa ilişkin açıklamanın yer aldığı görülmektedir. Ancak bir Yargıtay (2014d) kararında belirtildiği gibi, "önceden hazırlıklı ve planlı şekilde, kaybolma riskleri olan mevcut delilin korunmasını sağlamak için değil, yeni bir delil elde etmek amacıyla hareket edilmesi karşısında TCK'nın

133/2. madde ve fıkrasında tanımlanan kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu oluşmaktadır".

TCK'nın 132. maddesinde düzenlenen haberleşmenin gizliliğini ihlâl suçu, bir Yargıtay (2014e) kararında da açıklandığı gibi genel kast ile işlenebilen suçlardandır. Bu nedenle 132. maddenin ilk fıkrasındaki suçun manevi unsurunun oluşabilmesi için, "haberleşmenin gizliliğini ihlâl etme" neticesinin bilinmesi ve istenmesi; 132. maddenin ikinci fıkrasındaki suçun manevi unsurunun oluşabilmesi için, kişiler arasındaki haberleşme içeriklerinin taksirle veya tamamen hukuka uygun olarak elde edilmiş olsa dahi, bilerek ve isteyerek açığa çıkarılmış olması gerekmektedir. Bununla beraber, farklı Yargıtay (2012e, 2012d, 2012c, 2014e) kararlarında vurgulandığı gibi, kişinin kendisiyle gerçekleştirilen haberleşme içeriğini kaydetmesi eylemi 132. maddede suç olarak tanımlanmamış olmasına karşın, koşullara bağlı olarak 134. maddenin birinci fıkrasında tanımlanan "özel hayatın gizliliğini ihlâl" suçunu oluşturabildiği görülmektedir. Kişinin tarafı olduğu haberleşmenin içeriğini diğer tarafın rızasını almaksızın açığa çıkarmasına yönelik bir Yargıtay (2014h) kararında ise eylemin TCK'nın 132/3. maddesinde tanımlanan "haberleşmenin gizliliğini ihlâl" suçunu oluşturduğu dikkate alınmadan, uygulama yeri olmayan TCK'nın 134/1. Maddesine göre hüküm[5] kurulmuş olduğu belirtilmektedir. Buna yönelik Yargıtay kararları üzerinde yapılan detaylı incelemede, Yargıtay süreci öncesinde verilen kararlarda, suçun TCK'nın 132/3. maddesi kapsamında mı yoksa 134/1. maddesi kapsamında mı değerlendirileceğine yönelik tereddütlerin yaşandığı görülmektedir. Haberleşmenin gizliliğini ihlâl suçuna yönelik Yargıtay kararlarının 6'sının (%43) aynı zamanda özel hayatın gizliliğini ihlâl suçu ile ilgili açıklamalar içerdiği görülmektedir. Ayrıca bu 6 kararın Yargıtay tarafından bozulmasına ilişkin sunulan gerekçeler incelendiğinde, 2 kararda suçun nitelendirilmesinde yanılgıya düşülerek hüküm kurulduğunun açık olarak ifade edildiği görülmektedir.

Haberleşmenin gizliliğini ihlâl suçuna ilişkin olarak incelenen Yargıtay kararlarının sadece ikisinin (%14) eski nesil telsiz ve teyp cihazı ile ilgili olduğu, diğer 12 (%86) kararın ise günümüzde yoğun bir şekilde kullanılan bilgi ve iletişim teknolojileri aracılığıyla ve Facebook, Twitter, MSN gibi sosyal medya araçları da kullanılarak işlenen suçlara yönelik olduğu görülmektedir.

Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması

"Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçuna" ilişkin olarak toplam 22 Yargıtay kararı bulunmaktadır. Bu suça yönelik bir Yargıtay (2014g) kararında, TCK'nın 133/2. madde ve fıkrasında "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" başlığı altında tanımlanan suçun oluşabilmesi için, söyleşinin, "aleni olmamasının" gerekli ve yeterli olduğu belirtilmektedir. Başka bir ifadeyle, "belirsiz sayıda kişinin, özel bir çaba harcamadan kolaylıkla duyabileceği şekilde konuşulmaması" yeterli olmakla birlikte, suçun oluşması bakımından konuşma içeriğinin bir önemi bulunmamaktadır. Buna göre, söyleşinin özel yaşam alanı içinde yer alan ve gizlilik taşıyan konular hakkında olabileceği gibi, herkesin bildiği hususlar hakkında da olabileceği belirtilmektedir. Örneğin bir Yargıtay (2018g) kararında belirtildiği gibi, bir kişinin makam odasına gelen ziyaretçilerle yapmış olduğu konuşmalarının gizlice ses alma cihazı ile kayda alınması, TCK'nın 133/1. maddesinde tanımlanmış olan kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçunu oluşturmaktadır.

[5] Hüküm, mahkemenin önüne getirilmiş olan davayı çözen kararıdır. Davayı doğrudan çözmesi nedeniyle, bu karar mahkemenin ara karar ı değil son kararıdır (Çınar, 2009, s. 32).

Söyleşi dışında, iki kişi arasında gerçekleşen bir konuşmada, tarafların kendi aralarında geçen sözleri kayda alması, TCK'nın 133/1. madde ve fıkrası kapsamında değil, koşulları bulunduğu takdirde aynı Kanun'un 134/1. madde ve fıkrasında tanımlanan "özel hayatın gizliliğini ihlâl" suçu kapsamında değerlendirilebilmektedir (Yargıtay, 2014i, 2014f, 2014c, 2018e). Örneğin, sanık ile mağdurun yüz yüze değil, telefon vasıtasıyla görüşmüş olmaları ve sanığın tarafı olduğu haberleşme içeriğini kaydetmesi şeklinde gerçekleşen eylemin, TCK'nın 134/1. madde ve fıkrasındaki "özel hayatın gizliliğini ihlâl" suçu kapsamında değerlendirilebileceği düşünülmektedir (Yargıtay, 2017i). Benzer şekilde diğer Yargıtay (2015g, 2015f) kararlarında, "sanığın, katılan[6] ile yüz yüze yaptığı, içeriği özel, aleni olmayan konuşmaları katılanın bilgisi ve rızası dışında kaydetmesi eyleminde, bir üçüncü kişinin dahil olmaması ve sanığın tarafı olduğu konuşmayı kaydetmesi sebebiyle", TCK'nın 134/1. madde ve fıkrasındaki "özel hayatın gizliliğini ihlâl" suçunu oluşturduğu görüşüne yer verilmiştir.

Haberleşmenin gizliliğini ihlâl suçunda olduğu gibi, "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçuna yönelik olarak yapılan incelemede de Yargıtay süreci öncesinde verilen kararlarda, suçun TCK'nın 133/1. maddesi kapsamında mı yoksa 134/1. maddesi kapsamında mı değerlendirileceğine yönelik tereddütlerin yaşandığı görülmektedir. Bu nedenle "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçuna yönelik Yargıtay kararlarının 10'unun (%45) aynı zamanda "özel hayatın gizliliğini ihlâl" suçu ile ilgili açıklamalar içerdiği görülmektedir. Bu 10 davada kararın Yargıtay tarafından bozulmasına yönelik gerekçeler incelendiğinde, 6 kararda yasal olmayan gerekçelerle ve suçun vasfında yanılgıya düşülerek, TCK'nın 134. maddesi yerine TCK'nın 133. maddesi kapsamında hüküm kurulmuş olduğu ya da sanığın tarafı olduğu haberleşme içeriğini kaydetmesi karşısında eylemin TCK'nın 134. maddesinde düzenlenen "özel hayatın gizliliğini ihlâl" suçu kapsamında değerlendirilebileceği açık olarak ifade edilmektedir.

"Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" suçuna ilişkin olarak incelenen Yargıtay kararlarının 6'sında (%27) sadece ses alma cihazıyla, diğer 16 (%73) kararda ise bilgi ve iletişim teknolojilerinin önemli bir unsuru olarak cep telefonu aracılığıyla konuşmaların dinlendiği ve kayda alındığı görülmektedir. Bununla beraber, 7 kararda (%32) ses kayıtlarının CD ortamına aktarılması amacıyla bilgisayardan faydalanılmış olduğu görülmektedir.

Özel Hayatın Gizliliğinin İhlâl Edilmesi

TCK'nın 9. Bölümünde "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında düzenlenen suçlara yönelik en fazla Yargıtay kararının (N=73), TCK'nın 134. maddesinde düzenlenen "özel hayatın gizliliğini ihlâl" suçu ile ilgili olduğu görülmektedir. "Özel hayatın gizliliğini ihlâl" suçuna ilişkin toplam 73 Yargıtay kararının 66'sının (%90) bilgi ve iletişim teknolojileri aracılığıyla işlenen suçlara yönelik olduğu ve sosyal medya araçlarının da bu suçların işlenmesinde yoğun bir şekilde kullanıldığı görülmektedir. Diğer 6 (%10) Yargıtay kararında ise suçun işlenmesinde kullanılan araca yönelik açık ifade bulunmadığı için kesin bir bulgu elde edilememiştir. Bu çerçevede, günümüzde özel hayatın gizliliğinin ihlâline yönelik suçların hemen hemen tamamının, bilgi ve iletişim teknolojileri ile birlikte elektronik ortamların kullanılarak işlendiğini söylemek mümkündür.

[6] "Kamu davasına katılma (müdahale) isteminin yetkili makam (merci) tarafından kabul edilmesi durumunda, istemde bulunan kişiye, katılan (müdahil) denir" (Çınar, 2019).

Özel hayatın gizliliğini ihlâl suçunun ne şekilde işlendiğine ilişkin olarak Yargıtay kararları incelendiğinde, genel olarak güvenlik kameralarının kullanımı ile görüntü veya seslerin kayda alınması ve açığa çıkarılması konularına yönelik suçların internet ortamının sağladığı kolaylıktan yararlanılarak işlendiği dikkat çekmektedir. TCK'nın 134. maddesi kapsamında incelen tüm Yargıtay kararlarında, suçun işlenme şeklini açıklayan konu başlıklarının dağılımı Tablo 1'de görülmektedir.

Tablo 1. Özel hayatın gizliliğini ihlâl suçuna ilişkin Yargıtay kararlarının (n=73) konusunu oluşturan başlıklar

Suçun konusu	**n**	**%**
Kişilerin özel hayatına yönelik görüntü ve/veya seslerinin hukuka aykırı olarak açığa çıkarılması.	21	28.7
Gizliliğin görüntü ve/veya seslerin kayda alınarak ihlâl edilmesi.	21	28.7
Kişilerin özel hayatına ilişkin gizliliğin ihlâl edilmesi. Başkalarınca görülmesi ve bilinmesi istenmeyen özel yaşantıya müdahalede bulunma.	14	19.1
Kişilerin tarafı olduğu konuşmaların cep telefonu vd. ses alma cihazları kullanılarak gizlice kaydedilmesi.	9	12.3
Olumsuz tutum ve davranışlara yönelik iddiaları ispat etme ve kaybolma riskleri bulunan delillerin korunmasını sağlama amacı ile görüntü veya seslerin kayda alınması.	7	9.5
Güvenlik kamerasının gözetleme amacıyla takılması ve kullanılması.	1	1.3

TCK'nın 134. maddesinde düzenlenen "özel hayatın gizliliğini ihlâl" suçuna ilişkin Yargıtay kararlarının konusunu 6 temel işlenme şekli ile tanımlamak ve sınıflandırmak mümkündür. 134. madde kapsamında işlenen suçların incelenmesi Yargıtay sürecinde bu konu başlıkları kapsamında yapılmasına karşın, doğrudan TCK'nın 134. maddesi ile ilgili olmayan özel hayata ve hayatın gizli alanına karşı diğer suçlara atıfta bulunan kararlar da bulunmaktadır. Örneğin bir Yargıtay (2018e) kararında dinleyicilerin de hazır olduğu bir ortamdaki kişiler arasında aleni olmayan konuşmaların özel hayatın gizliliğini ihlâl edecek bir husus içermediği, benzer bir Yargıtay (2018g) kararında da "suç vasfında yanılgıya düşülerek TCK'nın 134/1. maddesi gereğince mahkûmiyet kararının verilmiş olduğu" belirtilmektedir. Bir Yargıtay (2016) kararında ise suç vasfında yanılgıya düşmenin yanı sıra suçun nitelikli halini oluşturan mesleğinin sağladığı kolaylıktan yararlanma durumunun dikkate alınmamış olduğu belirtilmektedir. Bu örneklerde olduğu gibi özel hayatın gizliliğini ihlâl suçuna yönelik olarak yapılan incelemelerde Yargıtay süreci öncesinde verilen kararlarda, suçun TCK'nın 132, 133, 135. ve 136. maddeleri kapsamında mı yoksa 134/1. maddesi kapsamında mı değerlendirileceğine yönelik tereddütlerin yaşandığı görülmektedir. Bu nedenle özel hayatın gizliliğini ihlâl suçuna ilişkin Yargıtay kararlarının 29'unun (%40) aynı zamanda TCK'nın 132, 133, 135. ve 136. maddeleri ilgili açıklamalar içerdiği görülmektedir.

TCK'nın 134/1. maddesinde düzenlenen "özel hayatın gizliliğini ihlâl" suçuna yönelik toplam 73 Yargıtay kararları incelendiğinde, bunların 19'unun (%26) sosyal medya üzerinden işlenmiş olduğu görülmektedir. Aynı zamanda elektronik ortamlarda özel hayatın gizliliğine yönelik ihlâl suçlarını konu alan Yargıtay kararları içindeki sosyal medya kullanımı hakkında da fikir veren bu oran, özel hayatın gizliliğinin korunması konusunda sosyal medya ortamının önemini ortaya koymaktadır. TCK'nın 134. maddesine ilişkin suçların sosyal medya ve özellikle yurtdışı kaynaklı yer sağlayıcılar üzerinden işlenmiş olması, zamana bağlı kısıtlılıklar nedeniyle bu suçlara yönelik olarak yapılan adli incelemeler için de zorluklar oluşturmaktadır (Drewer ve Ellermann, 2018, s. 141; Shaw ve diğerleri, 2016, s. 315). Bir Yargıtay (2014k) kararında bu hususa dikkat çekilerek, "Google, Yahoo, Facebook,

Skype, Hotmail, Twitter, Youtube gibi internet ortamında yaygın olarak kullanılan yer sağlayıcı firmaların merkezinin Amerika Birleşik Devletleri'nde (ABD) bulunduğu, ABD mevzuatına göre internet ortamında işlenen suçlara ilişkin trafik bilgilerinin yer sağlayıcılar ya da erişim sağlayıcılar tarafından 90 gün süreyle saklandığı ve bu süre içinde resmi otoritelerce başvurulduğunda anılan saklama süresine 90 gün daha ilave edildiği" belirtilmektedir.

TCK'nın 134. maddesine ilişkin bazı Yargıtay (2015c, 2017a, 2018b) kararları incelendiğinde, Yargıtay öncesi süreçlerde verilen kararlarda, gerçekleşen eylemin TCK'nın 226/3 maddesinde düzenlenen "müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları, temsili çocuk görüntülerini veya çocuk gibi görünen kişileri kullanan kişilerle" ilgili olduğu halde, suç vasfının tayininde yanılgıya düşülmüş olduğu ve yazılı şekilde TCK'nın 134/2. maddesiyle mahkumiyete karar verilmiş olduğu görülmektedir. Ancak TCK'nın 44. maddesinde düzenlenen fikri içtima[7] kuralına göre, "tek eylemle birden fazla suçun oluşması" ya da başka bir ifadeyle gerçekleşen eylemin "müstehcenlik" ve "özel hayatın gizliliğini ihlâl" suçlarını oluşturması nedeniyle, TCK'da bu suçlara dair en ağır cezanın tanımlandığı 226/3 maddesinin uygulanması gerekmektedir.

Özel hayatın gizliliğinin ihlâline yönelik suçlarda, ilgilinin rızasına ilişkin hususların da dikkate alınması önem taşımaktadır. Bir Yargıtay (2017c) kararında, görüntü ve seslerin gizlice kaydedilerek sonradan çekim izninin alınmış olmasının, mağdurun izni öncesinde gerçekleşen eyleme rıza gösterdiği sonucunu doğurmadığı belirtilmektedir.

TCK'nın 134. maddesine ilişkin suçların soruşturulması ve kovuşturulması, TCK'nın 139/1. maddesi gereğince şikâyete tabidir. Bu konuya ilişkin örnek Yargıtay (2015d, 2017e, 2017b) kararlarında, "kovuşturmada şikâyet koşulunun gerçekleşmemesi sebebiyle sanık hakkındaki davanın düşmesine karar verilmesi gerektiği" belirtilmektedir.

TCK'nın 134. maddesine ilişkin Yargıtay kararlar incelendiğinde, olumsuz tutum ve davranışlara yönelik iddiaları ispat etme ve kaybolma riskleri bulunan delillerin korunmasını sağlama amacı ile görüntü veya seslerin kayda alınması durumuna dikkat çekilen Yargıtay kararları olduğu görülmektedir. Örneğin bir Yargıtay (2015e) kararında, "sanığın iddiasını ispatlama amacını taşıyan eyleminde hukuka aykırı hareket ettiği bilinciyle hareket etmediğinin anlaşılması nedeniyle, özel hayatın gizliliğini ihlâl suçundan beraatına karar verilmesi" gerektiğine dikkat çekilmiş, benzer bir Yargıtay (2015b) kararında da bu gerekçeyle sanığın beraatına karar verilmesinde isabetsizlik görülmemiştir.

Kişisel Verilerin Kaydedilmesi

TCK'nın 135. maddesinde düzenlenen kişisel verilerin kaydedilmesine yönelik 10 Yargıtay kararının 5'inin (%50), TCK'nın 134. ve 136. maddelerinde tanımlanan suçlarla ilişkili olduğu görülmektedir. Bu nedenle kişisel verilerin kaydedilmesine yönelik eylemlerin, "özel hayatının gizliliğini ihlâl" ve "kişisel verilerin hukuka aykırı olarak verilmesi ya da ele geçirilmesi" suçları ile birlikte değerlendirilmesi gerektiği düşünülmektedir. Bununla beraber incelenen Yargıtay kararlarının 9'unda (%90), söz konusu eylemlerin elektronik ortamlar ve bilgi

[7] Fikri içtima: "İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişinin, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılmasıdır" (TCK, 2004, s. 8974).

teknolojileri kullanılarak gerçekleştirildiği görülmektedir. Bu durum, kişisel verilerin kaydedilmesine yönelik suçlarda elektronik ortamların kullanımına yönelik tercihler ve kullanım kolaylığı hakkında fikir vermektedir.

TCK'nın 135. maddesinde "hukuka aykırı olarak kişisel verilerin kaydedilmesi" suçu düzenlenmiş olmakla birlikte, eylemin TCK'nın 134. maddesinde düzenlenen "özel hayatın gizliliğini ihlâl" suçu kapsamında da değerlendirilmesi önem taşımaktadır. Nitekim bir Yargıtay (2015a) kararında mahremiyete ilişkin görüntülerin kaydedilmesi ve açığa çıkarılması eyleminin "kişisel verilerin kaydedilmesi" suçunu değil, TCK'nın 134/1. maddesinin 2. cümlesi ve 134/2. maddesine uyan "özel hayatın gizliliğini ihlâl" suçlarını oluşturacağı belirtilmektedir. Bununla beraber, bu suçların soruşturulması ve kovuşturulmasının TCK'nın 139. maddesi gereğince şikâyete bağlı olduğunun göz ardı edilmemesi gerekmektedir.

Yargıtay kararları TCK'nın 135. maddesi kapsamında incelendiğinde, eylemin hangi durumlarda TCK'nın 134/1. ve 134/2. maddesi kapsamında değerlendirileceği ve TCK'nın 135. maddesinde tanımlanan suçtan nasıl ayırt edileceği konusunda örneklerin bulunduğu görülmektedir. Bir Yargıtay (2014a) kararında, "özel hayata ilişkin görüntü ya da seslerin kişisel veri olarak nitelendirilmesinde şüphe bulunmamakla birlikte, kişinin özel hayatına ilişkin görüntü veya sesinin kaydedilmesi suretiyle ihlâl edilmesi ya da rızası dışında yayılması, açığa çıkarılması, ilan edilmesi yoluyla içeriği öğrenme yetkisi olmayan kişilerin bilgisine sunulmasının özel hayatın gizliliğini ihlâl suçu kapsamında TCK'nın 134. maddesinde düzenlendiği" ifade edilmektedir. Bu nedenle anılan kararda, "kişinin özel hayatına ilişkin görüntüsü, fotoğrafı ya da sesinin, yasal anlamda TCK'nın 135. maddesi kapsamında kişisel veri olarak değerlendirilemeyeceği" belirtilmektedir. Ayrıca, "kişinin özel yaşam alanı içerisinde yer almayan görüntüsü, fotoğrafı ya da sesinin rızaya aykırı olarak kaydedilmesi veya kullanılmasının kişilik hakkının ihlâli olarak değerlendirilmesi ve bu tür eylemlerin özel hukuk yaptırımlarına konu olabileceği" ifade edilmektedir.

TCK'nın 135, 136. ve 138. maddelerine ilişkin suçların soruşturulması ve kovuşturulması, TCK'nın 139/1. maddesi gereğince şikâyete tabi değildir. Bu konuya ilişkin örnek bir Yargıtay (2013a) kararında, verileri hukuka aykırı olarak verme veya ele geçirme suçunun, soruşturulması ve kovuşturulmasının şikâyete bağlı olmadığı gözetilmeden, kovuşturma aşamasında mağdurların şikayetlerinden vazgeçtiklerinden bahisle davanın düşmesine karar verilmesinin kanuna aykırı olduğu belirtilmektedir.

Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme

Araştırmada elde edilen veriler doğrultusunda, verileri hukuka aykırı olarak verme ya da ele geçirmeye yönelik Yargıtay öncesi süreçlerde verilen kararlarda, bu çalışmada incelenen özel hayata ve hayatın gizli alanına karşı işlenen diğer suçlarla ilgili daha fazla yanılgıya düşüldüğü görülmektedir. Örneğin bir Yargıtay (2018d) kararında, gündelik elbiselerle çekilmiş fotoğrafın ve ad-soyadı bilgilerinin kişisel veri niteliğinde olması nedeniyle bu verilerin hukuka aykırı olarak verilmesine ilişkin eylemde "TCK'nın 136. maddesi kapsamında hüküm kurulması gerekirken, delillerin takdirinde hataya düşülerek TCK'nın 134/2. maddesinde düzenlenen özel hayatın gizliliğini ihlâl suçuna ilişkin hüküm kurulmuş olduğu" belirtilmektedir. Başka bir Yargıtay (2018c) kararında da buna ilâve olarak, daha önce Facebook üzerinden yayımlanmış olmasının kişisel veri olma özelliğini değiştirmeyeceği ve üçüncü kişilere veri sahibinin rızası dışında bu resimleri yayımlama hakkı tanımayacağı vurgulanmaktadır. Benzer şekilde TCK'nın 136. maddesi ile ilgili olarak araştırma kapsamında incelenen 39 Yargıtay kararının 9'unda (%23), Yargıtay süreci öncesinde verilen kararlarda yanılgıya düşülmüş olduğu ifade edilmektedir.

“Verileri hukuka aykırı olarak verme veya ele geçirme” suçuna yönelik olarak incelenen 39 Yargıtay kararının 28’inde (%72), söz konusu eylemlerin elektronik ortamlar ve bilgi teknolojileri kullanılarak gerçekleştirildiği görülmektedir. Banka veya kredi kartlarının kötüye kullanılması suçları doğrudan bu çalışma konusu ile ilgili olmamakla birlikte, kredi kartı kopyalama araçları da bu orana dahil edildiğinde, elektronik ortamların bu suçun işlenmesindeki kullanım oranının %98’e çıktığı görülmektedir. Bu verilere bağlı olarak, “kişisel verilerin hukuka aykırı olarak verilmesi ya da ele geçirilmesine” ilişkin suçların hemen hemen tamamının elektronik ortamlarda gerçekleştiğini söylemek mümkündür.

TCK'nın 136/1. madde ve fıkrasının, "bu madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır" şeklindeki gerekçesi dikkate alındığında, kişisel verilerin verilmesi ya da ele geçirilmesi için kaydedilmiş olması ve bu haliyle başkalarına verilmesi ya da ele geçirilmesi gerekmektedir (Yargıtay, 2018f). Bu çerçevede kişisel verilerin kaydedilmiş olarak bellek vb. nesne üzerine taşınması gibi istenildiğinde tekrar kullanılabilmesine olanak sağlayan faaliyetler, “kişisel verileri ele geçirme” kapsamında değerlendirilebilmektedir. Ancak kişisel verilerin kaydedilmeden önce öğrenilerek, yazılı/basılı ve elektronik ortamlara aktarılmadan başkalarına açıklanması ve bu verilere sadece duyu organlarıyla vâkıf olunması, TCK'nın 134/1. madde ve fıkrasında düzenlenen “özel hayatın gizliliğini ihlâl” suçu kapsamında değerlendirilmektedir (Yargıtay, 2018f).

“Verileri hukuka aykırı olarak verme veya ele geçirme” suçu, seçimlik hareketli bir suç olarak düzenlendiği için, kişisel verilerin hukuka aykırı olarak başkasına verilmesi, ele geçirilmesi ve yayılması şeklindeki seçimlik hareketlerin birinin gerçekleştirilmesiyle suç oluşmaktadır. Bu soyut tehlike suçunun oluşabilmesi için herhangi bir neticenin gerçekleşmesi gerekmemektedir. Seçimlik harekette elden, internet üzerinden ya da diğer elektronik ortamlarda başkalarına (gerçek ya da tüzel kişilere) verilen verilerin hukuka aykırı veya uygun olarak elde edilmiş olmasının bir önemi bulunmamaktadır. Bu noktada verme eyleminin hukuka aykırı olması önem taşımaktadır (Yargıtay, 2017h). Bunun yanı sıra, bir Yargıtay (2018a) kararında kolaylıkla ulaşılması ya da bilinmesi mümkün olan kişisel bilgilerin de “kişisel veri” olarak kabul edildiğine dikkat çekilerek, uygulamada belirsizlik oluşturmaması ve her eylemin suça dönüşmemesi için somut olayın özelliklerinin dikkate alınmasının ve “sanığın eylemiyle hukuka aykırı hareket ettiğini bildiği ya da bilebilecek durumda olduğunun da ayrıca tespit edilmesi gerektiğinin” önemine vurgu yapılmaktadır. Örneğin bir kişinin nüfus cüzdanını ele geçirmedeki kastının kişisel verileri depolama ve yaymak olup olmaması, suçun yasal unsurlarının oluşması açısından önem taşımaktadır.

TCK'nın 134/1. ya da 136. maddelerinin uygulanması açısından dikkat edilen önemli unsurlardan biri de rızanın varlığıdır. Bir Yargıtay (2017g) kararında, “bazı fotoğrafların daha önce mağdurun rızasına uygun olarak sosyal paylaşım sitesinde yayımlanmış olması nedeniyle, özel yaşam alanına ilişkin ve özel hayatının gizliliğini ihlâl edecek nitelikte görüntüler olarak kabul edilemeyeceği” vurgulanmaktadır. Daha sonra bu fotoğrafların rızaya aykırı olarak (söz konusu fotoğrafların mağdur tarafından silinmesinin istenmesine rağmen) yayımlanmaya devam edilmesi durumunda ise TCK'nın 136/1. maddesindeki “kişisel verileri hukuka aykırı olarak yayma” suçunu oluşturacağı belirtilmektedir.

“Verileri hukuka aykırı olarak verme veya ele geçirme” suçunun internet ve sosyal medya üzerinden işlenme durumuna yönelik olarak, daha önce veri sahibi tarafından paylaşılmış olması ve paylaşılan verinin kişisel veri niteliğinin dikkate alınması önem taşımaktadır. Sosyal medya ile ilgili en sık karşılaşılan sorun, sosyal ağ profili

sayfalarında yayınlanan materyaldir (Lenartz, 2012, s. 29). Bu hususa ilişkin bir Yargıtay (2014j) kararında, "Facebook'taki herkes tarafından görülebilen profil resminin hukuk tarafından gizliliği ve korunması temel bir şahsiyet hakkı kabul edilmiş özel yaşam alanına dair bir görüntü olarak kabul edilemeyeceği" vurgulanmaktadır. Bununla beraber, bir kişiye ait herkese açık Facebook profil resminin kopyalanarak başka bir kişi tarafından rıza olmaksızın kendi Facebook hesabında yayımlanmasına yönelik olarak, başkaca bir kişisel bilgiye yer verilmemesi halinde, hukuka aykırı olarak ele geçirme ve yaymadan da söz edilemeyeceği belirtilmektedir. Ancak hukuka aykırı yöntemlerle profil resminin sahte Facebook hesabı üzerinden yayımlanması, TCK'nın 136/1. maddesinde tanımlanan "verileri hukuka aykırı olarak verme veya ele geçirme" suçunu oluşturmaktadır. Ayrıca resimlerin Facebook gibi görsel, işitsel ve elektronik kitle iletişim araçları üzerinden belirsiz sayıda kişinin görgüsüne sunulması, TCK'nın 6/1-g maddesi uyarınca cezada artırım yapılmasını gerekmektedir (Yargıtay, 2017d).

TCK'nın 136. maddesi kapsamında yapılan incelemelerde, kredi kartı ile ilişkili olarak bilgilerin kopyalanması, sahte kredi kartının oluşturulması ve bu kartların kullanılarak yarar sağlanması konusunda, Yargıtay süreci öncesinde tereddütlerin bulunduğu görülmektedir. Bu konuya açıklık getiren bir Yargıtay (2018i) kararında, ele geçirilen kopyalama cihazında kart bilgileri kopyalanarak bir kart oluşturulmasına ilişkin delillerin bulunması halinde ilgili bankanın suçtan zarar gören taraf olduğu dikkate alınarak TCK'nın 245/2. Maddesi kapsamında uygulama yapılması gerektiği belirtilmektedir. Anılan kararda, kart bilgilerinin kopyalanması suretiyle yeni bir kart oluşturulmamasına karşın ele geçirilen ilgili kopyalama cihazı üzerinde bilgi bulunması durumunda, TCK'nın 136. maddesi uyarınca "kişisel verileri hukuka aykırı olarak ele geçirme" suçunu oluşturacağı belirtilmektedir.

Verileri Yok Etmeme

TCK'nın 137. maddesi kapsamında yapılan Yargıtay kararlarına ilişkin incelemede, suçun bir kamu görevlisi tarafından ve görevinin sağladığı yetkinin kötüye kullanılmasıyla veya belli bir sanatın/mesleğin sağladığı kolaylıktan yararlanılarak işlendiği toplam 7 Yargıtay kararının olduğu görülmektedir. Bu kararların, TCK'nın 132, 133, 134. ve 135. maddeleri ile ilişkili olarak verildiği anlaşılmaktadır.

Araştırma kapsamında incelenen Yargıtay kararlarında, TCK'nın 138. maddesinde düzenlenen "verileri yok etmeme" suçuna yönelik bir Yargıtay kararının bulunmadığı görülmektedir. Bu suçun ihmal yoluyla işlenebileceği göz önüne alındığında, verilerin yok edilmesi konusunda yükümlülüğü bulunan bilgi profesyonellerinin ya da diğer veri sorumlularının bu konuda ihmallerinin bulunmadığı yönünde bir çıkarımda bulunulabilir. Ancak diğer taraftan, verilerin yok edilmesi konusuna son yıllarda kişisel verilerin korunmasına yönelik çalışmalarla dikkatlerin yoğunlaştığı da göz ardı edilmemelidir. Başka bir ifadeyle, araştırmada bu konuda Yargıtay kararlarına ulaşılmamış olması, kanaatimizce verilerin süresi içinde yok edildiğini ve bu konuda sorunların bulunmadığını söylemek için yeterli değildir.

Tartışma ve Sonuç

TKD (2010) mesleki etik ilkelerinde de belirtildiği gibi, çalışanların uyması gereken norm ve kurallar çerçevesinde kurum ve kuruluşlarda özel hayatın gizliliğinin korunması için bilgi güvenliğine ilişkin önlemler alınmaktadır. Ancak bilgi güvenliği önlemleri kapsamında bilginin gizliliğinin korunması, veri sahiplerine yönelik özel hayatın korunmasına dolaylı ve sınırlı olarak katkı sağlamaktadır. Bu nedenle son yıllarda mesleki kuruluşlarda sosyal medya politikalarının geliştirilmesine yönelik çalışmalar (TKD, 2018) yürütülürken, "özel hayata ve hayatın gizli alanına karşı suçlarla" ilgili hukuksal düzenlemelere de dikkat çekildiği görülmektedir. "Özel hayata ve hayatın

gizli alanına karşı işlenen suçların" bir parçası haline gelmemek ya da bu suçlara karşı yeterli önlemleri alabilmek için, TCK'nın 9. Bölümünde 132 ila 140. maddeleri arasında düzenlenen suçlara yönelik bilgi sahibi olmak önem taşımaktadır. Ancak hukuksal düzenlemelerde, kişisel verilerin kaydedilmesi gibi örneklere ilişkin olarak her eylemin suç oluşturmaması ve uygulamada belirsizlik yaratılmaması amacıyla, düzenlemelerin amacından fazla genişletilmemesine özen gösterildiği görülmektedir. Bu nedenle eylemlerin suç olarak nitelendirilmesi ya da uygun suç tanımı ile eşleştirilmesi, somut olayın özelliklerinin titizlikle değerlendirilmesini gerektirmektedir. Literatürde kullanılan özel hayatın gizliliğine yönelik fiziki koşullarda gözetleme, karıştırma vb. örneklerin aksine, günümüzde bu suçların bilgi ve iletişim ortamları üzerinden incelenmesinin zorunlu hale geldiği görülmektedir. Özel hayatın gizliliğine yönelik suçların günümüzde daha çok bilgi ve iletişim teknolojileri aracılığıyla işlenmesi, uygulama, yorumlama ve suça yönelik karar verme süreçlerinde daha fazla yanılgıya düşülmesine neden olabilmektedir. Bu nedenle, örneklere bağlı olarak Yargıtay'ın görüş ve değerlendirmeleri hem hukuksal işlemlerin takibi hem de benzer durumlarla karşılaşma olasılığı bulunan bilgi profesyonelleri için önem taşımaktadır.

Çalışmada incelenen Yargıtay kararlarının dağılımı dikkate alındığında, özel hayatın gizliliğinin ihlâl edilmesi ve haberleşmenin gizliliğini ihlâl suçlarının bilgi ve iletişim teknolojilerinden yararlanılarak işlenme oranlarının çok yüksek olduğu görülmektedir. Sosyal medya kullanımının tüm kurum ve kuruluşlarda yaygınlaşmasıyla birlikte, "özel hayata ve hayatın gizli alanına karşı suçların" sosyal ağ sağlayıcılar üzerinden işlenme oranında da artış olduğu görülmektedir (Bahar, 2018, s.25; FBI, 2021). Junco'nun (2011, s. 60) da belirttiği gibi, sosyal medya üzerinden yapılan paylaşımlardaki içeriğin kişisel haklara yönelik ihlâller içermesi ve internet üzerinde hızla yayılması, yüz yüze yapılan iletişime göre daha kolay ve olağan bir durumdur. Buna karşın, bireylerin sosyal medya üzerindeki ifade özgürlüğü ile çevrimiçi saldırılar karşısındaki hakları arasındaki dengenin sağlanması ya da sınırların belirgin olarak çizilebilmesi çoğu zaman kurumlar için zorlayıcı olabilmektedir (Lenartz, 2012, s. 32). Sosyal medya üzerinden özel hayata ilişkin paylaşım eğilimleri olan kişilerin kamu çalışanı olması halinde, hukuksal sorumluluklar daha önemli hale gelmekte ve hem kişiye hem de ilgili kuruma yansımaları daha ağır olabilmektedir. Bu nedenle, elektronik ortamlarda işlenen bilgi ve bu bilgileri işleyen, yöneten ve bilgi politikaları geliştiren bilgi profesyonellerinin, özel hayatın gizliliğinin korunmasına yönelik hukuksal koşulları ve artan riskleri dikkate almalarının yararlı olacağı düşünülmektedir.

Yargıtay kararlarına dayalı bulgular mutlak doğrular olarak kabul edilmemekle birlikte, farklı zamanlarda verilen kararlarda belirgin hale gelen görüşlere dayalı çıkarımda bulunulabilmektedir. Bu çalışmada erişim sağlanan Yargıtay kararları üzerinden yapılan incelemeye bağlı olarak, elektronik ortamlarda özel hayatın ve hayatın gizli alanının korunması amacıyla zaman ve mekân sınırı olmaksızın herkes tarafından göz önüne alınmasının faydalı olacağı düşünülen başlıca hususlar şunlardır;

- Kişinin daha sonra kanıt elde etme imkânının olmadığı ve yetkili makamlara başvurma olanağının bulunmadığı ani gelişen durumlarda yapmış olduğu kayıtlar için, haberleşmenin gizliliğine yönelik hukuka aykırılık bulunmamaktadır.
- Haksız saldırıyı önlemek ve kaybolma ihtimali bulunan delillerin yetkili makamlara ulaştırılarak güvence altına almak amacıyla, haberleşme içeriklerini izleme, dinleme ya da kaydetme eylemleri ile kişisel verileri ele geçirme, kaydetme ve/veya yayma eylemlerinde hukuka aykırılık bulunmamaktadır.
- Bilerek ve isteyerek haberleşmenin gizliliği ihlâl edilmemeli ve kişiler arasındaki haberleşme içerikleri açığa çıkarılmamalıdır.

- Özel bir çaba harcamadan rahatlıkla duyulamayan ve algılanamayan kişiler arasındaki konuşmalar, özel bir çaba ile dinlenmemeli ve kayda alınmamalıdır.
- Söyleşi dışında iki kişi arasında gerçekleşen bir konuşmada, konuşan taraflardan birinin konuşma içeriğini diğerinin izni olmadan kaydetmesi özel hayatın gizliliğinin ihlâline neden olmaktadır.
- Görüntü ve seslerin gizlice kaydedilerek sonradan çekim izninin alınmış olması, mağdurun izni öncesinde gerçekleşen eyleme rıza gösterdiği anlamını taşımamaktadır.
- Kişinin özel hayatına ilişkin görüntü ya da sesinin kayda alınarak ihlâl edilmesi ya da rızası dışında yayılması, açığa çıkarılması, ilan edilmesi yoluyla içeriğe erişim yetkisi olmayan kişilerle paylaşılması, özel hayatın gizliliğinin ihlâline neden olmaktadır.
- Kişisel verilerin hukuka aykırı olarak ele geçirilmesi, kaydedilmesi, verilmesi ya da ve süresi geçmiş olan verileri yok etmeme suçlarının takibi şikâyete bağlı değildir. Bu nedenle mağdurların şikâyetlerinden vazgeçmesi takibi sona erdirmeyecektir.
- Kişisel verilerin kaydedilmesi, bir yerden başka bir yere transfer edilmesi vd. işlemlere ilişkin hukuka aykırılığı ortadan kaldıran hususlar KVKK'da detaylı olarak düzenlenmiştir.
- Gündelik yaşama ait ve kişisel veri niteliği taşıyan verilerin hukuka aykırı olarak verilmesine ilişkin eylemler "özel hayatın gizliliği" değil, "verileri hukuka aykırı olarak verme veya ele geçirme" suçu kapsamında değerlendirilmektedir.
- Daha önce sosyal medyada yayınlanan bir kişisel veri, veri sahibinin rızası dışında üçüncü kişilere yayımlanmamalıdır.
- Sosyal medyada herkes tarafından görülebilen içerik, özel yaşam alanına dair bir içerik olarak kabul edilmemektedir.

Yayın Etiği Bildirimi / Research Ethics

Yazar araştırmanın etik dışı bir sorunu olmadığını, araştırma ve yayın etiği konusunu gözlemlediğini beyan etmektedir. / The author declares that the research has no unethical problem, and observe the research and publication ethics.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Çalışmanın her aşamasına yazar katkı sunmuştur. / The author provide the contribution rates to each stage of the study.

Çıkar Çatışması / Conflict of Interest

Çalışmada herhangi bir çıkar çatışması bulunmamaktadır. / The study has no conflict of interest.

Fon Bilgileri / Funding

Bu çalışmada herhangi bir fon kullanılmamıştır. / There is no funding for this study.

Etik Kurul Onayı / The Ethical Commitee Approval

Etik kurul kararı: Bu araştırmada, tüm araştırmacılara açık, uluslararası veri tabanında yer alan veriler kullanıldığından etik kurul kararı gerektirmemektedir. / The Ethical Committee Approval: This research does not require an ethics committee decision, since data in an international database open to all researchers are used.

Kaynakça / References

American Library Association [ALA]. (2018). Social media guidelines for public and academic libraries. http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/smg2018.pdf

Akbaş, M. ve Fenerci, T. (2016). Üniversite kütüphanelerinde sosyal medya politikaları [Social media policies in university libraries]. *Bilgi Dünyası / Information World, 17*(2), 201-231. https://www.bd.org.tr/index.php/bd/article/download/63/57

Akdağ, H. (2013). *Türk Ceza Kanunu kapsamında kişisel verilerin korunması.* Adalet Yayınevi.

Avrupa Konseyi. (1950). Avrupa İnsan Hakları Sözleşmesi. http://www.echr.coe.int/Documents/Convention_TUR.pdf

Avşar, Z. ve Öngören, G. (2010). *Bilişim hukuku.* Türkiye Bankalar Birliği.

Bahar, A. (2018). Bilişim suçları, iletişim ve sosyal medya [Cyber crimes, communication and social media]. *İstanbul Aydın Üniversitesi Dergisi, 10*(3), 1-36. https://iaud.aydin.edu.tr/wp-content/uploads/2018/07/iaud_v10i3001.pdf

Çınar, A. (2009). Hükmün konusu ve eylemi (fiili) değerlendirmede mahkemenin yetkisi. *Türkiye Barolar Birliği Dergisi* (84), 31-62. http://tbbdergisi.barobirlik.org.tr/m2009-84-542

Çınar, A. R. (2019). Ceza yargılamasında kamu davasına katılma [Participation in the trial in criminal procedure]. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 21*(Özel S.), 2801-2836. https://hukuk.deu.edu.tr/wp-content/uploads/2019/09/ALI-RIZA-CINAR.pdf

Davenport, T. H. (1997). *Information ecology: Mastering the information and knowledge environment.* Oxford University Press.

Drewer, D. ve Ellermann, J. (2018). The Online Environment as a Challenge for Privacy and the Suppression of Crime. M. B. J. Biasiotti M., Cannataci J., Turchi F. (Ed.), *Handling and Exchanging Electronic Evidence Across Europe* (Cilt. 39, s. 141-148) içinde. Springer. https://doi.org/10.1007/978-3-319-74872-6_8

Dülger, M. V. (2004). *Bilişim suçları ve internet iletişim hukuku.* Seçkin Yayınevi.

FBI (2021). Internet crime report. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

Gülaslan, T. (2018). Kamu yönetiminde sosyal medya kullanımı ve yönetimi: Temel ilkeler ve öneriler [Usage and administration of social media in public administration: Basic principles and recommendations]. [Hacettepe Üniversitesi]. Ankara. http://www.openaccess.hacettepe.edu.tr:8080/xmlui/bitstream/handle/11655/5022/Kamu%20Y%c3%b6netiminde%20Sosyal%20Medya%20Kullan%c4%b1m%c4%b1%20ve%20Y%c3%b6netimi_Temel%20%c4%b0lkeler%20ve%20%c3%96neriler.pdf?sequence=1&isAllowed=y

Gürkan, Ü. (2019). *Hukuk sosyolojisine giriş* (10 bs.). Siyasal Kitabevi.

Hafızoğulları, Z. ve Özen, M. (2009). Özel hayata ve hayatın gizli alanına karşı suçlar. *Ankara Barosu Dergisi*, 67(4), 9-22. https://dergipark.org.tr/en/download/article-file/397650

Junco, R. (2011). The need for student social media policies. *EDUCAUSE Review, 46*(1), 60-61. https://er.educause.edu/-/media/files/article-downloads/erm1118.pdf

KVK Kurumu. (2019). Madde ve gerekçesi ile kişisel verilerin korunması kanunu (bilgi notu) ve kişisel verilerin korunmasına ilişkin terimler sözlüğü. KVKK Yayınları.

KVKK. (2016). Kişisel Verilerin Korunması Kanunu. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

Lenartz, A. J. (2012). All my rowdy "friends": The use of social media in higher education [Northern Arizona University]. San Francisco. https://www.proquest.com/docview/1019989172/fulltextPDF/76CC47A714C14120PQ/1?accountid=11248

Lin, N. (1976). *Foundations of Social Research.* McGraw-Hill.

Shaw, U., Das, D. ve Medhi, S. P. (2016). Social network forensics: Survey and challenges. *International Journal of Computer Science and Information Security, 14*(11), 310-316. https://www.academia.edu/30916542/Social_Network_Forensics_Survey_and_Challenges

Şen, E. (2006). *Yeni Türk Ceza Kanunu Yorumu,* Cilt 1. Vedat Kitapçılık.

T.C. Anayasası. (1982). Türkiye Cumhuriyeti Anayasası. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf

TCK. (2004). Türk Ceza Kanunu. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf

Tezcan, D., Erdem, M. R. ve Önok, R. M. (2013). *Teorik ve pratik ceza özel hukuku.* Seçkin Yayıncılık.

Tripathi, E., Tripathi, A. ve Yadav, M. K. S. (2016). Role of information technology in cyber crime and ethical issues in cyber ethics. *International Journal of Business and Research,* 10, 21-25. http://www.ijber.in/list_volume10.html

Türk Ceza Kanunu Gerekçesi. (2004). Türk Ceza Kanunu Genel Gerekçesi. https://legalbank.net/belge/madde-1-ila-345-turk-ceza-kanunu-genel-gerekce/2677278

Türk Kütüphaneciler Derneği [TKD]. (2010). Türk Kütüphaneciler Derneği Mesleki Etik İlkeleri. http://kutuphaneci.org.tr/wp-content/uploads/2019/11/Mesleki-Etik-%C4%B0lkeleri.jpg

Türk Kütüphaneciler Derneği [TKD]. (2018). Kütüphaneler için sosyal medya politikası. http://kutuphaneci.org.tr/wp-content/uploads/2018/03/K%C3%BCt%C3%BCphaneler-%C4%B0%C3%A7in-Sosyal-Medya-Politikas%C4%B1-TKD-Sosyal-Medya-Politikalar%C4%B1-%C3%87al%C4%B1%C5%9Fma-Grubu.pdf

Yalçınkaya, B. (2020). Geleceğin arşivlerinin inşası: Sosyal medyanın arşivlenmesi hakkında bir değerlendirme [Building archives of the future: An evaluation of archiving social media]. *Bilgi Yönetimi / Information Management, 3*(1), 25-38. https://dergipark.org.tr/tr/download/article-file/1112219

Yargıtay. (2007). Yargıtay kararı (Esas No: 2006 / 13723, Karar No: 2007 / 13089). https://www.hukukturk.com/Goster?v=GE95G5nVYZ6

Yargıtay. (2010). Yargıtay kararı (Esas No: 2009 / 8119, Karar No: 2010 / 7573). https://www.hukukturk.com/Goster?v=GE95G6nuHmC

Yargıtay. (2012a). Yargıtay kararı (Esas No: 2011 / 7345, Karar No: 2012 / 8936). https://www.hukukturk.com/Goster?v=GE95G8XoKe0

Yargıtay. (2012b). Yargıtay kararı (Esas No: 2011 / 20872, Karar No: 2012 / 9834). https://www.hukukturk.com/Goster?v=GE95G8dUJFI

Yargıtay. (2012c). Yargıtay kararı (Esas No: 2012 / 13117, Karar No: 2012 / 14791). https://www.hukukturk.com/Goster?v=GE95G77Ima8

Yargıtay. (2012d). Yargıtay kararı (Esas No: 2012 / 13228, Karar No: 2012 / 14787). https://www.hukukturk.com/Goster?v=GE95G9OmzmC

Yargıtay. (2012e). Yargıtay kararı (Esas No: 2012 / 20608, Karar No: 2012 / 18217). https://www.hukukturk.com/Goster?v=GE95G5UCHku

Yargıtay. (2013a). Yargıtay kararı (Esas No: 2012 / 22005, Karar No: 2013 / 24489). https://www.hukukturk.com/Goster?v=GE95G5Z0uno

Yargıtay. (2013b). Yargıtay kararı (Esas No: 2012 / 32005, Karar No: 2013 / 15770). https://www.hukukturk.com/Goster?v=GE95G6AQfJo

Yargıtay. (2014a). Yargıtay kararı (Esas No: 2013 / 9669, Karar No: 2014 / 3760). https://www.hukukturk.com/Goster?v=GE95G7TIhIO

Yargıtay. (2014b). Yargıtay kararı (Esas No: 2013 / 13614, Karar No: 2014 / 5809). https://www.hukukturk.com/Goster?v=GE95G7Rp80e

Yargıtay. (2014c). Yargıtay kararı (Esas No: 2013 / 15779, Karar No: 2014 / 7263). https://www.hukukturk.com/Goster?v=GE95G7VEJZQ

Yargıtay. (2014d). Yargıtay kararı (Esas No: 2013 / 20481, Karar No: 2014 / 10220). https://www.hukukturk.com/Goster?v=GE95G74VXyC

Yargıtay. (2014e). Yargıtay kararı (Esas No: 2013 / 21755, Karar No: 2014 / 13367). https://www.hukukturk.com/Goster?v=GE95G7jzSKm

Yargıtay. (2014f). Yargıtay kararı (Esas No: 2013 / 22599, Karar No: 2014 / 12706). https://www.hukukturk.com/Goster?v=GE95G7grru4

Yargıtay. (2014g). Yargıtay kararı (Esas No: 2013 / 26087, Karar No: 2014 / 10205). https://www.hukukturk.com/Goster?v=GE95G7oX2Po

Yargıtay. (2014h). Yargıtay kararı (Esas No: 2014 / 1714, Karar No: 2014 / 18859). https://www.hukukturk.com/Goster?v=GE95G77YjYG

Yargıtay. (2014i). Yargıtay kararı (Esas No: 2014 / 2511, Karar No: 2014 / 17251). https://www.hukukturk.com/Goster?v=GE95G7FVVC4

Yargıtay. (2014j). Yargıtay kararı (Esas No: 2014 / 4081, Karar No: 2014 / 19490). https://www.hukukturk.com/Goster?v=GE95G7bFSwC

Yargıtay. (2014k). Yargıtay kararı (Esas No: 2014 / 7409, Karar No: 2014 / 24197). https://www.hukukturk.com/Goster?v=GE95G7MJsJc

Yargıtay. (2015a). Yargıtay kararı (Esas No: 2014 / 11530, Karar No: 2015 / 584). https://www.hukukturk.com/Goster?v=GE95G7sJsBM

Yargıtay. (2015b). Yargıtay kararı (Esas No: 2014 / 13474, Karar No: 2015 / 3). https://www.hukukturk.com/Goster?v=GE95G85qZLk

Yargıtay. (2015c). Yargıtay kararı (Esas No: 2014 / 19535, Karar No: 2015 / 4333). https://www.hukukturk.com/Goster?v=GE95G8IKv4a

Yargıtay. (2015d). Yargıtay kararı (Esas No: 2014 / 22101, Karar No: 2015 / 2153). https://www.hukukturk.com/Goster?v=GE95G8JTJaq

Yargıtay. (2015e). Yargıtay kararı (Esas No: 2015 / 81, Karar No: 2015 / 7817). https://www.hukukturk.com/Goster?v=GE95G7uYBma

Yargıtay. (2015f). Yargıtay kararı (Esas No: 2015 / 14885, Karar No: 2017 / 3121). https://www.hukukturk.com/Goster?v=GE95G75uzWS

Yargıtay. (2015g). Yargıtay kararı (Esas No: 2015 / 17241, Karar No: 2017 / 4259). https://www.hukukturk.com/Goster?v=GE95G6Eb9Ye

Yargıtay. (2016). Yargıtay kararı (Esas No: 2015 / 5128, Karar No: 2016 / 10207). https://www.hukukturk.com/Goster?v=GE95G9Oi360

Yargıtay. (2017a). Yargıtay kararı (Esas No: 2014 / 9227, Karar No: 2017 / 4650). https://www.hukukturk.com/Goster?v=GE95G7xDBC4

Yargıtay. (2017b). Yargıtay kararı (Esas No: 2015 / 10834, Karar No: 2017 / 192). https://www.hukukturk.com/Goster?v=GE95G9aI1nE

Yargıtay. (2017c). Yargıtay kararı (Esas No: 2015 / 11084, Karar No: 2017 / 636). https://www.hukukturk.com/Goster?v=GE95G9bQQJU

Yargıtay. (2017d). Yargıtay kararı (Esas No: 2015 / 11112, Karar No: 2017 / 637). https://www.hukukturk.com/Goster?v=GE95G6kJpLM

Yargıtay. (2017e). Yargıtay kararı (Esas No: 2015 / 12554, Karar No: 2017 / 413). https://www.hukukturk.com/Goster?v=GE95G9dhDM0

Yargıtay. (2017f). Yargıtay kararı (Esas No: 2015 / 13248, Karar No: 2017 / 3108). https://www.hukukturk.com/Goster?v=GE95G5wNFb6

Yargıtay. (2017g). Yargıtay kararı (Esas No: 2017 / 150, Karar No: 2017 / 6231). https://www.hukukturk.com/Goster?v=GE95G5YOyFk

Yargıtay. (2017h). Yargıtay kararı (Esas No: 2017 / 829, Karar No: 2017 / 363). https://www.hukukturk.com/Goster?v=GE95G7lmY9w

Yargıtay. (2017i). Yargıtay kararı (Esas No: 2017 / 4667, Karar No: 2018 / 3187). https://www.hukukturk.com/Goster?v=GE95G6Db0VM

Yargıtay. (2018a). Yargıtay kararı (Esas No: 2015 / 1659, Karar No: 2018 / 2748). https://www.hukukturk.com/Goster?v=GE95G8OicW8

Yargıtay. (2018b). Yargıtay kararı (Esas No: 2016 / 13170, Karar No: 2018 / 439). https://www.hukukturk.com/Goster?v=GE95G9SZHe4

Yargıtay. (2018c). Yargıtay kararı (Esas No: 2017 / 2960, Karar No: 2018 / 1541). https://www.hukukturk.com/Goster?v=GE95G7qbSK0

Yargıtay. (2018d). Yargıtay kararı (Esas No: 2017 / 7385, Karar No: 2018 / 3977). https://www.hukukturk.com/Goster?v=GE95G6JGz6e

Yargıtay. (2018e). Yargıtay kararı (Esas No: 2017 / 10732, Karar No: 2018 / 9468). https://www.hukukturk.com/Goster?v=GE95G8jD2TA

Yargıtay. (2018f). Yargıtay kararı (Esas No: 2017 / 12083, Karar No: 2018 / 2539). https://www.hukukturk.com/Goster?v=GE95G5zyGGG

Yargıtay. (2018g). Yargıtay kararı (Esas No: 2018 / 2226, Karar No: 2018 / 8746). https://www.hukukturk.com/Goster?v=GE95G8kNuQi

Yargıtay. (2018h). Yargıtay kararı (Esas No: 2018 / 3318, Karar No: 2018 / 9281). https://www.hukukturk.com/Goster?v=GE95G8TH1kG

Yargıtay. (2018i). Yargıtay kararı (Esas No: 2018 / 6171, Karar No: 2018 / 10436). https://www.hukukturk.com/Goster?v=GE95G9KfXXc

2022

4(2), 171-196

Siber Tehdit Taksonomilere Siber Aktivizm Çerçevesinde Bir Değerlendirme

Deniz Gönç*[1]

Anahtar Sözcükler

Yeni medya
Dijital kamuoyu
DDoS saldırısı
Siber tehdit taksonomisi
Dijital aktivizm

Makale Hakkında

Gönderim Tarihi
2 Mayıs 2022
Kabul Tarihi
10 Ekim 2022
Yayın Tarihi
28 Aralık 2022
Makale Türü
Araştırma Makalesi

Öz

Çevrimiçi olarak sunulan milyarlarca yeni medya platformu insanlara kendilerini temsil etme ve benzer düşünen insanlarla tanışma olanak sağlar, böylelikle siber uzayda da insan temelli, canlı ve dinamik bir kamuoyu oluşur. Siber uzayda da demokrasiyi mümkün kılmak için, tüm toplumsal gruplar -tüm çatışmaları ile hür ve adil olarak temsil edilmelidir. Devletler ve egemen kullanıcıların siber alana da sirayet eden güç mücadeleleri demokratik bir siber kamuoyunun varlığını gölgelemektedir. Yeni medya ve siber aktivizm çerçevesinde ele alınan bu çalışmada, siber aktivizmin marjinal ve saldırgan bir türü olan hacktivizm motivasyonu siber alanda varlığını ve gücünü kanıtlama mücadelesi olarak ele alınmıştır. DDOS (Dağıtık Hizmet Reddi Saldırıları) saldırıları, siber uzayda iktidar ve kamu yönetimi mücadelesinin temsilcisi olan korsanlar tarafından en çok tercih edilen saldırı türlerinden biridir. Çalışmanın amacı, siber aktivizmi diğer siber suçlardan ayırt edecek kriterlerin belirlenmesine yardımcı olmaktır. Literatürde DDOS taksonomilerinde kullanılan kriterler sunulmuştur. Siber aktivizmi diğer siber suçlardan ayırt edebilmek için Türkiye'de kamuoyunu etkileyen siber saldırılar incelenmiştir ve hackerların mesajlarını içeren bir tablo ile bulgular sunulmuştur. Sonuçta hacktivism motivasyonları görünür kılınarak, belirleyici ölçütlerin DDOS taksonomilerine dahil edilmesi önerilmiştir.

An Evaluation of Cyber Threat Taxonomies in the Framework of Cyber Activism

Keywords

New media
Digital public sphere
DDOS attacks
Cyber threat taxonomies
Digital Activism

Article Info

Received
May 2, 2022
Accepted
October 10, 2022
Published
December 28, 2022
Article Type
Research Paper

Abstract

Billions of new media platforms available online allow people to represent themselves and meet like-minded people, creating a human-based, vibrant and dynamic public opinion in cyberspace. o enable democracy in cyberspace, to, all social groups - with all their conflicts - must be free egalitarian representing. The power struggles of states and sovereign users, which also spread to the cyber space, overshadow the existence of a democratic cyber public opinion. In this study, which is handled within the framework of new media and cyber activism, hacktivism motivation, which is a marginal and aggressive type of cyber activism, is discussed as a struggle to prove its existence and power in the cyber field. DDOS (Distributed Denial of Service) attacks are one of the most preferred attack types by hackers, who are the representatives of the struggle for power and public administration in cyberspace. The study aims to help determine the criteria to distinguish cyber activism from other cybercrimes. The criteria used in DDOS taxonomies are presented in the literature. To distinguish cyber activism from other cybercrimes, cyber attacks affecting the public in Turkey were examined and a table containing the messages of hackers and findings was presented. As the result, it has been proposed to include the determining criteria in DDOS taxonomies by making hacktivism motivations visible.

***Atıf*:** Gönç, D. (2022). Siber tehdit taksonomilere siber aktivizm çerçevesinde bir değerlendirme, *Bilgi ve İletişim Teknolojileri Dergisi*, *4*(2), 171-196. https://doi.org/10.53694/bited.1112219

***Cite*:** Gönç, D. (2022). An evaluation of cyber threat taxonomies in the framework of cyber activism, *Journal of Information and Communication Technologies*, *4*(2), 171-196. https://doi.org/10.53694/bited.1112219

*__Sorumlu Yazar/Corresponding Author__: Deniz Gönç
[1] Yeditepe University, Media Studies, Turkey denizgonc@gmail.com, https://orcid.org/0000-0002-8338-6476

Giriş

Communication technologies that paved the way for globalization have enabled the information society revolution. Today internet has reached a unique structure that includes other networks and digital media like Machine-to-machine (M2M) and Internet of Things (IoT) technologies that covered other networks and digital media and reached a network structure whose boundaries have been unknown (Crowley & Heyer, 2010). In this way, big liquid data is feeding at any moment and provides creative opportunities and solutions in the fields of health, finance, security, logistics, commerce, and even education (Faritha, Revathi, Suganya, & Gladiss, 2020; Sun, Yan, Lu, Bie, & Thomas, 2012). New ways of reaching, creating and analysing information have created a heterogeneous and interactive mass communication model based on its digital-based and multi-format structure. The internet, as the new multi-media, unlike television, which has trapped people on screens, opens its forums and puts the agora on the mobile phone, where virtual communities meet (Genel, 2015). The powerful feedback system of new media allows users to share and discuss their opinions on political issues. This "participant-friendly" model also allows users to increase their online sharing about the world agenda. The new media also creates an environment in which users can share their feedback and opinions. Wide-based widespread use of the internet has brought security problems. It gives a dominant and decisive position to institutions and individuals who are committed to providing this security. Considering the new media as cyberspace, including also the public sphere, to see the struggle for sovereignty is natural (Müller & Kramer, 2014). The conquest of nation-states in cyberspace is continuing. Cyberspace is not a hobby, but a public struggle for existence with an international diplomatic dimension.

In terms of cybersecurity as a defense of cyberspace, there should be ethical principles between the democratic use of the public sphere and motivations of informatics crimes, as well as technical criteria. In this study, a literature review was conducted in terms of the determining criteria of taxonomies used in cyber security studies. The criteria found seem to ignore the democratic necessity of cyber activist actions, namely the nuance between cyber activism and cybercrime. The news of DDoS (distributed denial of service attacks) actions in Turkey was examined and subjected to content analysis. The purpose of the analysis, which examines the messages of cyber attackers, is to make visible the unique characteristics of DDoS attacks in terms of their motivation. As a result of the analysis, new parameters that are not included in the cyber crimea and threat taxonomies are proposed.

New Media

New media is an asynchronous form of media that gives the audience enable, to interact with all online things, that are computational and rely on computers for redistribution. The nature of new media, including traditional media, is purely digital and fluid, growing exponentially geometrically. The production process requires computer and internet technologies from the beginning to the end. Manovich (2002) describes the new media's four characteristics as (i)Digitalism is the conversion of all data into numerical codes. (ii) Automation is the ability of digital software to perform some operations on its own; (iii) Modularity defines the working of parts independently; (iv)Transcoding is the convertibility of content into different formats.

The five basic features of new media are communication, cooperation, community, providing creative thinking and convergence (Friedman & Friedman, 2008). Social media according to four main areas: modernity of communication; productive audiences; dialogic and network structure; and its searchable and tagged nature (Averweg, 2018). Because of their low cost and asynchronous nature, internet forums provide partial communication to unlimited recipients, occupy a global area, accelerate communication and are hypertext (Demircan, 2006). Digital games have hypnotic, imaginary, skinned, interactive, simulated, and cybernetic media culture (Giddens & Kennedy, 2006). Wearable environments are defined by movement, transparency, nanotechnology, brain-machine interfaces, augmented memory, portable technology parameters and participatory culture (Pedersen, 2013). Since new media has an intertextual and modular structure, these conditions can be generalized to all media within the scope of new media. Despite the lack of equal access to resources, cyberspace often provides freedom of expression and access to information. It offers users the opportunity to share their feelings and thoughts, and organize and act jointly.

The new media discussions gave theoretical hope that the internet, which facilitates access to information, can erode the inequality gap that is deepening day by day in the economic and social fields. The integrative effect of the new media and the phenomena of widespread use of social media in environments of conflict and unrest creates a digital public opinion. Especially for using social networks suitable for social movements and the dissemination of activist practices in the presence of political conflicts (Castells, 2008; Zizek, 2013).

Against these positive features, new media distribute the unvoiced information that is manipulated and make internet content unreliable systematically and purposively (Davenport & Prusak, 2001, s. 27). Exactly the political economy of the new media should always be taken into account. Although access to information is not theoretically restricted, transfer and sharing are limited. Internet access can be provided limitedly to the poor, disabled, women, elderly, and children against economic, geographical, gender and age-based inequalities and in internet access.

Digital Public Sphere

The public space is a unifying space where valour and virtue are displayed, where people come together, listen to each other and take action. The public sphere, which is the basis of the political community, is the space in which the individual constructs himself. It is the place where public problems become visible and perceptible, citizens access political information as legislators, and politics become legitimate (Arendt et al., 1997; Habermas, 2002; Onat, 2013; Sennett, 2010). According to Habermas, the public sphere is the living space where people reason and form ideas around a common subject. According to Fresier (1990), the public sphere is the ensemble of informally mobilized non-governmental discursive ideas that stabilize the state. The existence of public islets and public spaces composed of people and groups with similar aims accelerates the expansion of the discursive space. According to Ackerman's liberal dialogue model, the public sphere and the state sphere are identical, and the place of the citizen is in the private sphere. Sennet states that today the public sphere has become formalized, and the focus of the citizen, which has gained a submissive character, shifts to private matters and he states that the public sphere has collapsed. Güven and Satır (2018) cite change.org as an example, as a public space where claims for different sensitivities are expressed from a wide variety of locations. The digital public sphere is a cyberspace of discourse and action that encompasses and unites the public sphere, private and political spheres, and even individuals and institutions.

For understanding the digital public sphere and its functioning, it is required to know about the fact that the friendly appearance of cyber ideology and the network organization behind the internet mask the economic superpowers (Başaran, 2000; Schafer, 2015). As in the real world, the existence of the exploitation and oppression of the limited group that divides the power requires us to see the new media as a field of activism and struggle (Gazeteciler Cemiyeti, 2019). While individuals live parallel existences in the real world in cyberspace, it provides a very rapid social formation and consumption of the virtual public. Cyberspace is polluting like the real world.

In the digital public sphere as in the real world, we should see the existence of the exploitation and oppression of the limited group that divides the power, and the new media as a field of activism and struggle (Sausa, Pinto& Silva, 2015). While individuals experience parallel existence with the real world in cyberspace, it provides very rapid social formation and consumption of the virtual public. Unfortunately, new media, which enables the public space to be produced and consumed more, will not fill the information gaps of the media (Golman & Loewenstein, 2015; Trappel, 2019). Limited and unequal access to the Internet ensures the reproduction of economic inequalities (Giddens, 2012, p.445). According to Noris (2001) due to the digital gap between developed and undeveloped countries, the internet causes the gap between the knowledge levels of its people to continue.

Digital Democracy and New Social Movements

Democracy is based on a problematic pillar and civic participation, also a historical concept that is subject to the contingencies of the social interaction that shape it and challenge it (Sousa, Pinto & Silva, 2013). The reality and existence of democracy is a matter of deep debate, but cyber-public opinion provides the basic conditions of cyber democracy (Yengin, 2017). Thus, the eight criteria of democracy defined by Dahl (2001, p. 40); Freedom of expression, implementation of election results, electoral justice, equal voting rights, right to be elected, freedom to use alternative news sources, freedom of association and participation are theoretically possible in this cyber world. In terms of its contribution to democracy with its web 3.0 semantic feature, new media created opportunities for access to alternative information sources, founding organizations, participation, and freedom of expression. The globalization of actions can eliminate the knowledge monopoly of experts (Beck, 1997; Maigret, 2014, p., 346). In terms of the permeability and limitlessness of public, private and political spaces, we can talk about the existence of democracy in the digital public sphere in a theoretical framework. The interactive structure of the internet enhances the culture of participation and provides the opportunity to create cyber-public opinion. Thanks to the simultaneity, source verification possibilities and data sharing features of new media technologies, people can establish political, cultural, religious or commercial organizations regardless of location (Castells, 2008; Enjolras, Bernard, & Johnsen, 2017). In this respect, new media can be considered a public space due to the effect of bringing social groups together and creating identity (Timisi, 2003).

The characteristics of new social movements seen in the public sphere are also manifested in the digital public sphere. The class and economy-oriented labour struggle has been replaced by new social movements, which focus on political and social conflicts. Social media, which is a new field of existence for freedom of expression and personality performances, has an integrative effect on all users thanks to its fast, unfiltered, inclusive and partially democratic operation.

The integrating effect of the new media in individual and social unrest and conflict creates a virtual public opinion, and sometimes even replaces the real public opinion under pressure. In the presence of political conflicts, especially the use of social networks can turn into social actions, thus enabling social movements and

disseminating activist practices (Castells, 2008; Zizek, 2013). For example, social media allows people to coordinate their actions in the form of mass mobilization or protest both online and in the real world. Arab Spring, Occupy Wall Street, Travel, etc. We have seen a wide variety of uses of new media platforms in social network-based social movements (Bayhan, 2014; Zizek, 2013). The cyber public sphere represents the real system of physical life where violence and bullying have become the reality of new media in the cyber world, as well as the the democratic opportunities offered by the new media for democracy and civil rights. (Langos, 2012; Ang & Goh, 2010).

Digital Activism

Social movements making progress towards their goals often rely on some form of activism to promote change. Social activism is part of the broader field of social movements that take action to create social change. Digital activism is digitally mediated social activism (Bennett & Segerberg, 2013; Selander & Jarvenpaa, 2016). Activism in the traditional sense requires donations of money and time, and the struggle is not easy to spread. On the other hand, digital resources provide a strong social impact. Success factors in digital activism are digital skills, internet access, digital technologies and large social networks. Electronic civil disobedience is the most militant form of political resistance in the digital humanities and has become popular in recent years (Losh, 2012 p. 166). The use of digital information and communication technology encourages people's participation in activist efforts. Examples of civil disobedience that can be shown on these issues can be further diversified, such as hacking, worms and viruses, virtual sit-ins, fake websites, e-mail shelling, and online signature campaigns. The interactive structure of the internet enhances the culture of participation and provides the opportunity to create cyber-public opinions. The main topics of cyberactivism -parallelly to new social movements can be classified as women's movement, anti-war and peace movement, the environmental movement, farmers' movement, nuclear energy, the movement against low-wage workers, labor movement, and AIDS movement (Kalafatoğlu, 2010). There are many popular digital activism practices on the internet, such as selected internet content consumption, data creation and publishing, original content design and sharing, open-source software development, support, and organization for non-governmental organizations.

George and Leidner (2018, 2019) listed digital activism actions as clicking, meta-voicing, assertion, political consumerism, digital petitions, botivism, e-financing, data activism, disclosure, and hacktivism. Then they analysed the functions, mechanisms, and effects of digital activism actions according to the digital activism hierarchy.

1. Digital Spectator Activities are related concepts with the spectator tier of social media. Clicktivism is being an advocate, individually and remotely. Metavoicing is sharing social media posts and duplicating and recreating. The assertion is creating original digital materials and participation in e-government e-participation.

2. Digital Transitional Activities are exemplified by political consumerism, digital petitions, botivism, and e-funding. Political consumerism is to support a business financially that agrees with their views while boycotting (buycotting) firms that promote dissenting views. Digital petitions mandate a guaranteed response if a minimum number of signatures is met. Botivism refers to the virtual activist who plays the automated digital action like trolls. E-financing is using technology to generate income for a cause in the process of providing funds for business activities, making purchases, or investing.

3. Digital Gladiatorial Activities are not to do the participants do seek to influence change; they to make the change. Data activism uses the activities in open government data, data rescue, civic data hacking and data philanthropy to gain greater individual power over data held by others. Exposure is sharing of knowledge without permission as a leak. According to Coleman (2011, p.138) Hacking is an aggressive attack type of cyber activism through computer codes that exposes information, destroy data, or disrupt operations of individuals by hackers who target governments, and organizations.

Coleman (2011) matches the mechanisms and functions of cyber activism actions as identification: affirming and legitimizing; construction: creating, donating, designing, protecting; aggression: destroying, disrupting, appropriating, attacking, coercing; deception: deceiving, concealing; visibilitation: commending, denouncing, exposing; amplification: reinforcing, repeating, communicating, educating. Hacktivism techniques are listed by O'Malley (2013) as distributed-denial-of-service (ddos) virtual sit-in, website defacement, site redirects, cyber sabotage and information theft. Hacktivism is a type of online activism and is not necessarily cybercrime (Sabillon, Cano, Cavaller, & Ruiz, 2016a).

Hacktivism

The story of hackers includes the history of the devotion of youth, computer programs, authority and genius scientists, hippies, yuppies, liberals, anarchists, and classical socialists in the 60s, 70s, 80s, and 90s (Walleij, 2003). According to the analysis of Eriş (2009) this is a story that turns into a subculture from a mixture of ideologies. Hacker culture based on sharing, helpful, forgiving, reactive, and solidarity generally (Keleş, 2013) Hacker ethic works well intentioned cyber-attack actions are carried out with principles such as ethics, challenge and a field of struggle independent of the state's power apparatus, justice, creating original content and facilitating access to information, or the representation of public power in the cyberspace in political actions against the state and/or power. Ethic hackers defined as white hat, facilitate access to information by developing free software by sharing their knowledge and expertise. Contrastly black hackers self-set unauthorized access to computer systems and disrupt internet transactions attacks.

Hacker ethics was based on to explorer cyber world before '80s. However, in the changing information world, the authoritarian attitude of the state and the fact that many acts of hackers are considered crimes due to commercialization have also led to the transformation of hacker ethics. Since the beginning of the 2000s, Anonymous Turkey, RedHacker, Türk Hack Team, Ayyıldız Tim, Beyaz Hacker, Akıncılar, Turkish Security, Cold Hackers, Mesopotomia Hackers, Pkk Hack Team, belonging to different political frameworks, have been carrying out cyber attacks. These groups generally carry out internationally linked actions (Bıçakçı, Ergun, Çelikpala, p., 41). Hacktivists are categorized into three categories based on their ethic positions as civilian hackers, patriotic hackers, in a different term cyber militia and cyber terrorists (Dahan, 2013; Denning, 2000; Johnson & Robinson, 2014; Sauter, 2013). Civilian hackers organizing loosely groups that perform actions such as creating and updating digital systems for the good of society and legally (Hunsinger & Schrock, 2016; Schrock, 2016). Patriotic hackers has nationalist motivations and the state and/or power informally support their activities generally (Dahan, 2013; Green, 2016). Cyber terrorist is who act hacking and spreading viruses and malware, destroying websites, and performing denial of service (DOS) or botnet attacks among other activities for malicious trespass (Goode, 2015).

The crime-oriented approach working for understanding hacking activities associates the hacker phenomenon with the crime. On the other hand, the emancipatory approach determine within the framework of hacker ethics distinguishes hacking from the crime phenomena. It provides a way to broaden and deepen our understanding of the use and policies of tools and to question the uncritical instrumentality that many digital humanities projects assert (Losh, 2012, p.163).

Cyber Threats and DDoS attacks

Cyber-attack is intentional actions taking by people or information systems anywhere in cyberspace in order to destroy the confidentiality, integrity, or accessibility of information and industrial control systems in cyberspace or data processed by these systems (Turkey National Security Cyber Strategy Report). Kang et al. (2009) are listed digital threats of present-days as authorization violation, logic or time bombs, browsing, bypassing controls, data modifications, denial of service, eavesdropping, illegitimate use information leakage, intercept/ alter, interference database query analysis, masquerade, physical intrusion, replay, repudiation, resource exhaustion, sabotage, scavenging, spying, service spoofing, sniffers, substitution, terrorism, theft, traffic analysis, trap door/ back door, Trojan Horse, tunnelling, unauthorized access, violations of permission, unauthorized access, piggybacking, virus and worm.

The most common types of cyber attacks are denial of service (DoS) and distributed denial of service (DDoS) attacks and Man in the Middle attacks (Menlick, 2018). The DDoS attack relies on setting up a “zombie network” to cause the victim to overload web resources, rendering online resources inoperable. The attack targets a server or process on the victim system, making it unable to process legitimate requests for service. Unlike DDoS attacks, the cybercrime we have seen so far consists of the traditional crimes being committed with cyber tools. Theft, blackmail, harassment, trespassing, child abuse, encroaching the copyrights, as well as committing crimes such as murder are physical activities that can be carried into the cyber world. However, DDoS attacks do not correspond to any legal or illegal activity in the physical world. For this reason, it is a new type of performance, and the act may be defined as a crime specific to cyberspace only. International laws are not clear about DDoS attacks not also Council of Europe Convention on Cybercrime or Budapest Convention does not have a universal structure and evaluation of cyber crimes depend on local laws (Nikolskaia & Minbaleev, 2000). DDoS attacks considered the most effective attacks are actions that stand out by criteria such as procedural creativity, difficulty, and damage and impact. DDoS attacks, which became widespread with Mafiaboy, became the hacktivist tool of Annonymous' and SOCa in the 2000's. Cyber warfare is the nation-states use cyberspace to achieve their goals by using conventional military force.

According to Kelsey (2008) armies use cyber weapons for disabling civilian infrastructure serving as power plants, telecommunications, and transport infrastructure. Cyber warfare is the nation-states use cyberspace to achieve their goals by using conventional military force. In the context of national defense, reciprocal attacks that are macro in nature and between two or more countries have the potential to turn into wars between a number of sovereign states in the virtual arena (Indrajit et al., 2021). Cyber warfare is practised between states, whereas cyber terrorism is practised by non-state actors. Digital militarism different from cyber war is the use of digital technologies for war purposes and motivation differs from nationalist militarism attacks, commercial competition, or all cyber activism. The attacks have physical effects in the real world, and they are cyber attacks even, so their domain is

the real world. The purpose of cyberterrorism is to coerce or intimidate a government or its people to pursue political or social ends through illegal attacks and threats of attack on computers, networks, and stored information. Cyber terrorism's tactics are politically intended hacking operations (such as leaking and spying), unlawful attacks of intimidation, and controlling attack that ruins computerized systems for critical infrastructures tools. Terrorism in the real -world usually achieves its primary goal of demoralizing civilians by destroying property and injuring or killing civilians this distinguishes terrorism from warfare, which is not supposed to target civilians (Brenner, 2010, s., 387).

Cyber diplomacy is an important tool in furthering a nation's foreign policy as it enables direct interaction and engagement with the foreign public as a strategy for managing change through digital tools and virtual collaboration (Bjola & Holmes, 2015 p.89). It is the use of the Internet and ICT (information and communication technologies) to help implement diplomatic objectives or refers to harnessing the internet and modern communication technology to connect with an external audience in order to create an enabling environment for a country's foreign policy. Riordan (2016) made refers to cyber diplomacy as the use of diplomatic tools, and the diplomatic mindset, to resolve issues arising in cyberspace. Cyber diplomacy has five characteristics: Transparency, centralization and decentralization, disintegration and merger, possible accuracy and virtualization (Abdulsaliq, 2017; Ekşi & Taş, 2020). Serious attacks on critical infrastructures can be acts of cyberterrorism depending on their effects but for diagnosing as cyberterrorism, an attack must result in violence against persons or property (Denning, 2000). Specifying whether an attack is a terrorist or a war attack is a matter of diplomacy and law. Civil hackers may work for states informally as cyber militias, or information soldiers (Gürdal, 2021). If these hackers aim to provide the interests of the opposing state, cyber spies are declared traitors (Walden, 2005). It is a political choice whether to disclose information about the attacks carried out at the state level or not through diplomatic channels (Riordan, 2016; Shorter, 2014).

Cyber threat taxonomies

Cybercrime and threat taxonomies provide crime prevention by analyzing its origin and development. Bosh (2010) divided cyber crimes according to aims. Computer-assisted offences are the former include fraud and intellectual property offences that pre-date the Internet and are merely enabled by the socio-structural features of the internet. On the other hand, computer-oriented offences, are computer-oriented or computer-assisted offences such as viruses that target the computer hardware and software.

In the literature, many criteria are used in the evaluation of cyber threats, attacks, and crimes. Cyber threat and DDoS taxonomies which are of special importance were examined the existence of taxonomies suitable for the concepts of digital democracy and cyber activism in this study. Criminal taxonomies often focus on the purposive and technical dimensions of cybercrime (Indrajit et al., 2021). The purpose of classification is to reduce complexity and unnecessary hierarchy by organizing subtypes into well-defined categories along broad criteria. The main requirement for this is to ensure mutual exclusivity, which is possible with a clear definition of process and classification characteristics. The basic principle is that the first, direct and immediate point of impact must be specified for each cyber threat (Chandra & Snowe, 2020).

The main criteria of taxonomies are various according to analyzing data. Cyber threat taxonomy uses criteria such as attacker, victim, relationship, purpose, tool, tactic, result, impact, target, attack, and power of influence. Donald and Bryson's (2014) cybercrime taxonomy's nine attributes are victim, attacker, objective, tool & tactic, impact,

result, relationship, target, and offence. Narwal, Mohapatra, and Usmani (2019) describe cyber threat taxonomy which categorizes the threat into eight aspects.

Meyers, Powers, and Faissol (2009) presented a classification of different types of cyber enemies and their corresponding methods, motivations, maliciousness and skill levels, within the scope, prevalence and economic impact of cybercrime. Each of the enemy types is listed by respective skill level in table 1 (maliciousness, motivation, and method (adopted from Meyers, Power, & Faissol, 2009).

Table 1. A Taxonomy of Cyber Adversaries

Adversary Class	**Motivation**	**Method**
Script kiddies, novices	boredom, thrill seeking	download and run already-written hacking scripts known as ‟toolkits‟
hacktivist, political activists	promotion of a political cause	engage in denial of service attacks or defacement of rival cause site
cyberpunks, crashers,	prestige, personal gain, thrill seeking	write own scripts, engage in malicious acts, brag about exploits
user malcontens insiders,	disgruntlement, personal gain, revenge	uses insider privileges to attack current or former employers
coders, writers	power, respect prestige,revenge	write scripts and automated tools used by newbies, serve as mentor
white hat hackers, old guard	intellectual gain, ethics, respect	non-malicious hacking to help others and test new programming
black hat hackers, professionals	personal gain, greed, revenge	sophisticated attacks by criminals/thieves; may be ”guns for hire‟ or involved in organized crime
cyber terrorists	enemy nations, ideology, politics	espionage state-sponsored, well-funded cyber attacks against enemy nations

The criteria here are the target, the attack class, the degree of access gain, the source of the attack, the severity of the threat, the effects on the security targets, the result, and the motivation of the threat.

Sabillon, Cavaller, Cano, and Serre Ruiz (2016) extended to include elite, script kiddies, cyber-terrorists, disgruntled employees, virus writers, hacktivists, lamer, crackers, ethical hackers, GPS hackers, industrial spy hackers, government agent hackers, military hacker and cyber warriors. Kjaerland (2005) stated that cyber effects are tested in four categories as disrupt, distort, destruct, and disclosure. Simmons et al. defined a tree which classifies the cyber effect according to five core categories like attack vector, operational impact, defense, informational impact, target, and expanded than Kjaerland's (2006) taxonomy. Regarding the classification of cyber impact, Derbyshire et al. (2018) stated impact is the main motivation of a cyber attack and is the result of the action. Intended effects are usually denial of service, physical damage, leaks, premature code execution (Derbyshire et al., 2018). Cyber threat prediction and prevention applications are widely used to ensure the security of information systems. AVOIDIT cyber attack taxonomy figure includes attack vector, operational impact, defense, impact and the target parameters in figure1 is from Simmons, Ellis, Shiva, Dasgupta and Wu (2014). AVOIDIT is different from other taxonomies in the literature, categorizing cyber threats into attack vector, operational impact, defense, informational impact, and target categories, by aiming to educate the defender on possible cyber attacks.

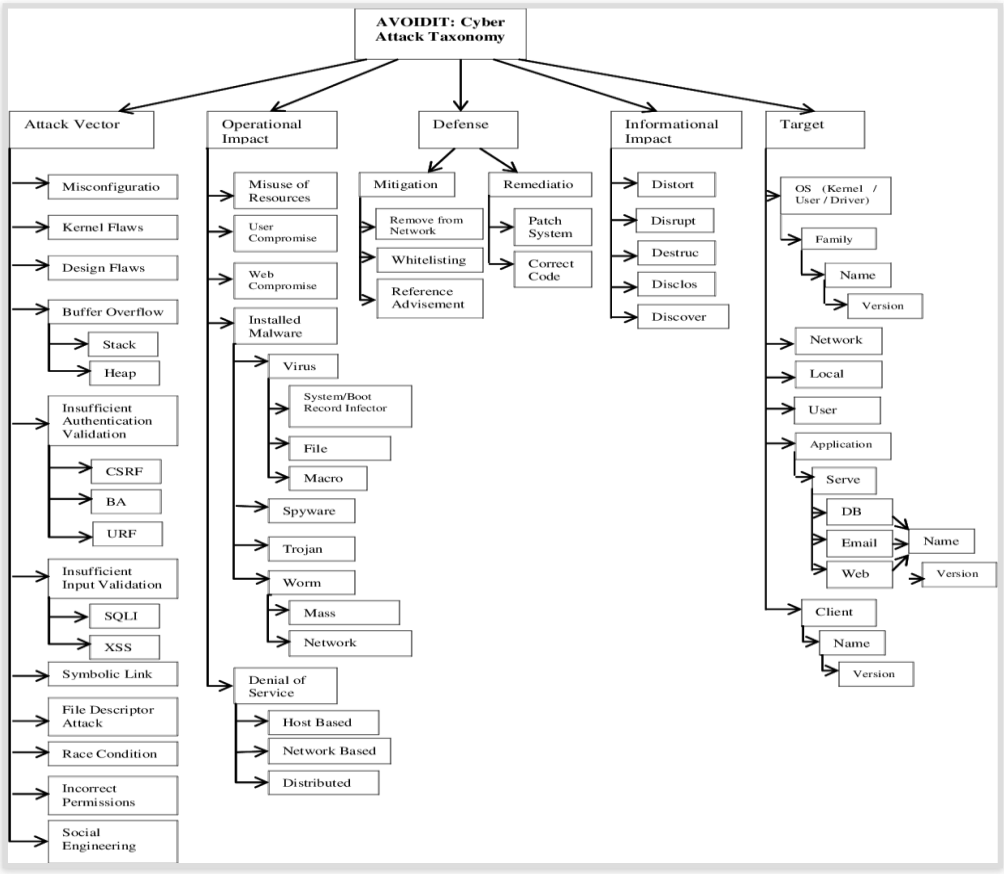


Figure 1. AVOIDIT

AVOIDIT could be extended to include new categories within each classification and it will provide a defender with the appropriate information to make an educated decision in defending against cyber attacks (Simmons, Ellis, Shiva, Dasgupta, & Wu, 2014).

CADAT is a process to make easier to the classification of cyber attacks with using of cause, action, defense, analysis, and target parameters (Banga, Gupta, & Bathla, 2019). Ebios risk management system determines the business and technical scope of the studied object the most appropriate source of risk/target pairs for the remainder of the study; identifies the stakeholders of the ecosystem of the studied object and creates operational scenarios that define technical attack methods that can be used by the risk source to assess threat levels and realize the identified strategic scenarios.

Lough (2001) developed IT (information technologies) security oriented a tree-like cyber-attack taxonomy for wired and wireless networks that used validation, exposure, randomness, deallocation, improper, and conditions parameters coded with VERDICT word. Cyberthreat and cybercrime taxonomies include the tool and the object dimensions (Urbas & Choo, 2008; Alkaabi et al, 2010) Cyber attacker's aims are linked to their motivation as challenge, status, revenge, politics, ideological, thrill, political or financial gain, and sexual impulses. (Choo, Smith, & McCusker, 2007; Howard & Longstaff, 1998; Moitra, 2004).

According to Chandra and Snowe (2020), the real question is "the actor who committed the crime". The taxonomy includes (i) accounting, which seeks to manage by measurement; (ii) technology, which provides efficiency through innovations; (iii) regulation, which seeks to provide transparency and accountability; (iv) enforcement,

which needs conceptual clarity; and, (v) public policy, which seeks capacity building and skill development in the society.

Cybercrime is divided into two pure technology crimes perpetrated by computers and networked systems, and advanced cybercrimes perpetrated by individuals, institutions, and governments at Chandra and Snowe's victim-centred taxonomy, which kept apart traditional- offline crimes from cybercrime. Pure technology crimes include computer systems, related technology and network system. Situations where a victim is a natural person, commercial institution, property, and governments suffering financial damage are considered as 'advanced cybercrime'. If the victim is the computer technology ecosystem, and networked systems, the cyber attack is considered in the category of pure technology cybercrime. The decisive point of reporting the denunciation of cyber crimes is the first direct and immediate effect of the event. Cyber advanced crime includes natural persons, property other than, and the governments. Situations where the victim is a natural person, commercial institution, property, and government suffering financial damage are considered 'advanced cybercrime'. If the victim is the computer technology ecosystem, and networked systems, the cyber attack is considered in the category of pure technology cybercrime. The decisive point of reporting the denunciation of cyber crimes is the first direct and immediate effect of the event.

Chandra and Snowe (2020) explained the classification of crimes against the government as: including acts that disrupt, hinder, assault or collapse its governing body or institutions, mechanisms or bureaucracy, and/or processes or systems, through which citizens and groups exercise their rights, meet their obligations, articulate their interests, and mediate their differences. Crime against Governments is a category of direct victims, including acts that target a nation, state or sovereign commonwealth. Crimes against governments affect their ability to effectively function and discharge their fiduciary, administrative, or statutory duties. If our taxonomies overlook and neglect to consider the structures of governments, the constraints of one type of government may fail to recognize the nature of the different forms of governments.

Moitra's (2004) modelling focused on victims. In the study, which also has a behavioral perspective, the motivations of cybercriminals to harm their victims were classified.

Magklaras and Furnell (2001) use semantics clues to classify the nature of IT insider threats. Online verbal behaviours may evaluate signs of aggression and domination score for an evaluated potential threat (EPT) (Schultz, 2002).

Meyers, Powers and Faissol (2009) presented a classification of different types of cyber enemies and their corresponding methods, motivations, maliciousness, and skill levels within the framework of the scope, prevalence and economic impact of cybercrime. Each of the adversary types has listed based on the corresponding skill level, maliciousness, motivation, and method.

DDoS taxonomies

While designing the Internet, the prime concern was to provide for functionality, not security. DDoS attacks mainly take advantage of the architecture of the internet, and this is what makes them powerful. As a result, many security issues have been raised, which are exploited by attackers. Cyber attackers have financial, political, and social motivations and they create diverse destructive tactics. DDoS attacks appear to be politically motivated (Yu,

2014). In these, the victim is thought to have wronged someone on the side of the attacker (Nazario, 2008; Simmons, Shiva, Bedi, & Dasgupta, 2014). Only a little subset of denial-of-service attacks is financially motivated.

Harry (2018) classified disruptive effects as data and physical attacks, internal and external denial of service, and message manipulation. Singh and Bhandari (2020) suggest a new-flow based DDoS Attack taxonomy which have four main category.

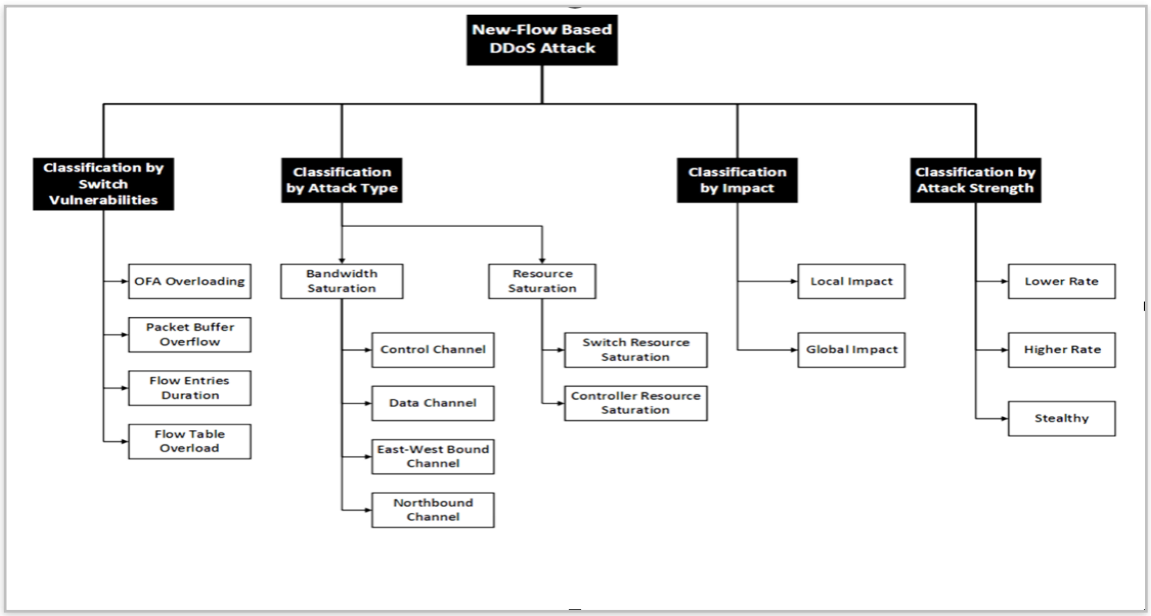


Figure 2. *New Flow based DDoS attack*

New flow-based DDoS attacks in figure 2, shows the taxonomy classified by switch vulnerabilities, attack type, impact and attack strength. DDoS defenses approaches are analyzing by Kaur et al. (2021) in literature at three popular categories. Fifty eight percent of the studies focused on Controller Resource Saturation, twenty eight percent bandwidth saturation of communication channel and thirteen percent are focused on flow table overloading and buffer saturation wiev (Kaur et al., 2021). Abhista et al. (2020) stated, to evaluate the reasons for selecting a victim, we make use of socio- cultural, economic and political (SPEC) dimensions. For the choice of target infrastructure, we utilize the dimensions of value, inertia, visibility and accessibility (VIVA).

Mirkovic and Reihner's (2004) taxonomy of distributed denial of services attack highlight features of attack strategies. The taxonomy of DDoS attacks has categorized into eight as:

1. Degree of Automation,
2. Exploited Weakness,
3. Source Address Validity,
4. Attack Rate Dynamics,
5. Possibility of Characterization,
6. Persistent Agent Set,
7. Victim Type,

8. Impact on Victim parameters.

Finally, in this study we categorized the taxonomies as effect and attack strength-focused, IT security focused taxonomy, user-oriented, and behaviorist taxonomies according to the literature basically.

Attack strength-focused taxonomies measures attacks as lower, higher and stealthy. Classification is by to attack strength and its measured as lower, higher and stealthy. (Banerjee et al., 1998; Guo & Yuan, 2012). Classification is by to attack strenght and its measured as lower, higher and stealthy. Effect and it security focused taxonomies are use these criterias too. Zhu et al. (2011) describe a taxonomy developed with an ICS focus, more specifically.

User oriented taxonomies use the parameters as cyber-bullying, awareness, phishing victims (Franz et al., 2021). Kjarland (2006), who also has a mixed evaluation perspective, analyzed Computer Emergency Response Team (CERT) related to computer crime profiling, highlighting cyber-criminals and victims. Method of Operation, Target, Source, and Impact analyzed. It can be understood from the scale of the target that the attack is for commercial, political or personal purposes.

IT security focused taxonomy presented by Specht and Lee (2004) divide into two DDoS attacks as bandwidth depletion and resource depletion attacks, which is IT security and also crime based oriented too. The work of Lee and Spetch (2000, p. 18) has raised important questions about DDoS taxonomies. As victims of attacks often fail to trace back to the attacker, there is the question of who is responsible for an attack in terms of contributory negligence. Can owners or agencies responsible for secondary victims be held responsible for participating in an attack? Are software and hardware vendors also responsible for cyber attacks? Do network providers have to keep victims away from DDoS packet traffic sent to the network?

Sabillon, Cavaller, Cano, and Serre Ruiz (2016b) presented to comprehensive a cyber crime taxonomy in twenty-seven titles as child pornography, cyberhate speech, cyber offenses against intellectual property, cyberbullying, cyberespionage, cyberextortion, cyberfraud, cybergrooming, cyberheist, cybering, cyberlaunderin, cyberstalking, cybertheft, cyberwarfare, data breach, disgruntled employees and former employees, identity theft, online gaming, online obscenity, phishing, racism and xenophobia-related cyber offences, religion-related cyber offences, revengeporn, spam and which we are focused in the study, the cyber terrorism, hacking and cyber vandalism. They define the distributed denial of service attacks (ddos) and social media account hijacking, website defacement, using malware to delete data, categorized as cyber vandalism different from cyber crime. They define hacktivism as a part of organized crime networks, operating with specific motives and a high degree of sophistication, which has been becoming illegal once it crosses the threshold of gaining unauthorized access to computer systems. Finally, they related the hacking with cyberterrorists who engage in terrorist activities that exploit computer vulnerabilities, and that will impact mostly civilians in metropolitan areas because of motivated by political ideology, religious beliefs, hacktivist proclivities or personal reasons.

Behaviourist studies, which focused on actors of cyber-attack or suspects and their decision mechanisms, are based on self-determination theory generally. The theory of self-determination distinguishes between autonomics and oppressive and controlled behaviours of cyber attackers. They are intrinsically motivated behaviour (Ryan & Deci, 2000). With regard to extrinsic regulators, research has shown that evident that compliant security behaviour greatly influences the protection of information assets on the social climate, software measures and facilitating conditions and these studies pointed out the importance of human motivation. Sherizen (1990) add the taking risk,

low self-control and opportunistic behaviour to factors that promote a maladaptive to compliant security behaviour. Posey et al. (2013) proposed a protection-motivated behaviour to protect information resources by insider. Venkatraman (2008) defined cyber deviant behaviour as violating organizational norms and endangering the organization, and proposed three measurable categories: members, institutionalization, and technical skill. Internalized norms such as embarrassment or shame, fear of informal sanctions from peers and internalization of legal norms may also be deterrents to crime. The aforementioned theory moderated by certainty of detection, severity of punishment and the celerity of detection is also known as the classical deterrence theory (Grasmick & Bursik, 1990).

Kumar and Carley (2016) revealed that new international events affect social media and sometimes the hacker community differently. It measured a general mood swing for countries through social media analytics and tracked cyber attack vulnerability. Kumar and Carley's (2016) taxonomy helped to find an answer this study's question. Cyber attack taxonomies may classify to focal points as IT and cyber security, attack impact, attack strength and behavior focused studies (Hansman & Hunt, 2005; Meyers, Powers, & Faissol, 2009; Kjarland, 2006).

As Abhistha et al. (2000) stated in the research compared and associated with DDoS attacks and eventful days (according to Google Alert) holistic perspective is imperative to accurately map threats and take appropriate protective measures against DDoS attacks.

Method

This is an interdisciplinary study carried out in the fields of mass communication and informatics, which is essential in terms of associating the movements toward cyberspace with the theories of mass communication and the use of public space. The aim of study is to evaluate the motivational dimension of cyber activism and to review the competency of cyber attack taxonomies to distinguish cyber activism from other cyber crimes. The research is based on seconder data and has a qualitative method and descriptional design. Research questions are: Is a democratic public space possible in cyberspace? And DDoS attacks are defined as hacktivism, cyber terrorism or the struggle to conquer cyberspace, depending on what conditions?

In the first part of the study, DDoS attacks in the cyber activism dimension was discussed in the context of new media and digital democracy. It has been investigated how to find the criterion that determines the distinction between activism and cybercrime. In the second part, basic concepts such as cyber threats, crime, war and cyber diplomacy are explained. A literature review is conducted to specify the focal points, criteria of current cyber threat taxonomies and purpose and motivations of DDoS attacks. The existence of taxonomies suitable for the concepts of digital democracy and activism and their contribution to the measurement of hacktivist activities and the evaluation of social protests have been questioned. Scope and criterion validity was ensured by examining the messages of hackers who carried out effective newsworthy DDoS attacks, which is a type of cyber activism in Turkey, in the context of moving the public agenda to the cyber space. (Coleman, 2011, p.138). Researchers who will examine the history of hacker messages and ddos attacks from the archives of scanned online news sites will see the impact of the social agenda on the risk of ddos attack and will understand a positive correlation between social conflict and attacks.

Sampling Research

Common cyberthreath and DDoS taxonomies in the literature were examined for determining their priority criterion. The secondary data was analysed, by non-experimental and descriptive design within the framework of cyber activism. DDoS attacks in the Turkish mainstream news media were subjected to content analysis in terms of new social movements. The three most clicked internet news sites from Alexa data were selected according to their belonging to different media organizations. The archives of Ensonhaber.com, Hurriyet.com.tr and Sözcü.com were scanned with the keywords "hacker", "cyber hacker", "crashed", "DDoS", and the perpetrators were analyzed by examining the history and perpetrators. In addition, the messages given by the hackers were examined to see if the DDoS attacks were related to the public agenda and to make the cyber activism dimension visible.

Findings

To evaluate the examples of cyber threath and DDoS taxonomies, the archives were scanned and the cyber attacks that had the most impact on Turkey's agenda were identified. The archive was scanned with the keywords "hacker, "cyber hacker", "crashed", "DDoS". The news includes the messages shared at the time of the attack and/or social media assuming and explanations. In this section, content analysis of the messages given in the hacking actions in the context of new social movements has been applied.

Table 2. Messages of cyber hactivists

Victim	***Date/Hacker***	***Messages of hackers***
www.bbm.gov.tr	2/5/2008 The Karan	Mr. Prime Minister, since you do not hear our voice, we will announce it like this.
*www.maliye.gov.tr	9/11/2011 ColdHacker	Get your dirty hands off the people of Kurdistan
www.osym.gov.tr	21/4/2011 V.O	**The system ıs fully off for now. frıends who want to use ıt can use the defıcıt and transfer ınformatıon. good luck:::))))
www.disisleri.gov.tr	3/7/2012 Red Hack	"It's not foreign affairs, it's war and slavery business.
ankara.pol.tr kirikkale.pol.tr POLNET	28/2/2012 RedHack	We have been working on the servers of Ankara-based POLNET and Ankara Police Department for about three weeks. The police will be stunned when they see how far we've come when the documents are released." We are protesting the green army Ankara Police of the community that killed Ethem Sarısülük by shooting him in the head!
www.diyanet.gov.tr	30/10/2012 RedHack	We will stop you playing the people like sheep by being a religious trader!"
www.thy.com.tr	26/8/2012 Anonymous	It's not the THY brand or planes that bring us to our loved ones, it's their workers.
www.tgc.org.tr	14/9/2012 Turkish Ajan Hacker	"You will apologize to Anadolu Agency.
www.yok.gov.tr	8/1/2013 Redhack	We said let's hack the institution that is the head of the snake.
www.yargitay.gov.tr	16/1/2013 Redhack	N.C. We will throw a firewood on your fire for every drop of tears that we do not know, maybe hundreds of our sisters."
İzmir İl Özel İdare	27/3/2013 RedHack	We open to the public all the electricity, gas, adsl, etc. invoice transactions of the Istanbul Administration ;)' Freedom for Palestine
www.basbakanlik.gov.tr	5/6/2013 Anonymous & SEA	Fear changed sides: Turkish people are not afraid, oppressors are afraid

www.rtuk.gov.tr	12/6/2013 Anonymous	you punished the media organizations that wrote the truth. Now Anonymous has punished you”
www.ulusalkanal.com	25/6/2013 RedHack	Pull like it's nation Panpa
www.chpankara.org	10/7/2013 Ayyıldız Team	Don't force us to do things we haven't done in years
www.tkib.gov.tr	15/10/2013 RedHack	Since #Berkin gave the orders, #Melis, #Ozan, #Serdar gave the orders; this run will be run without breath” The holiday of those who do not forget what happened in #Rojava, #Latakia, #Kirkuk
Kurtlar vadisi	17/11/2013 PKK Hack Team	Your site has been destroyed by PKK Hack Team
idrisnaimsahin.com.	21/5/2013 Cold Hackers	Martyrs of May are immortal.
Akp Ordu İl Başkanlığı	29/11/2013 RedHack	We will not leave Taylan alone either. Innocence is fearless.
www.tcmb.gov.tr	16/01/2014 RedHack	Has the Central Bank become uf?
www.taraf.com.tr	28/3/2014 Gözcü	"You Have Betrayed the Homeland and Nation! This Nation Will Not Forgive You!"
Türk İşbirliği ve Koordinasyon Ajansı	19/5/2014 RedHack	Email and user login disclosure
www.egm.gov.tr	5/9/2013 RedHack	Pull the plug, tidy up, tidy up,tidy up! :)
www.burhankuzu.com.tr	13/5/2013 RedHack	This is our wedding gift, it comes all the way from Hatay. We will not only enjoy your wedding, but also you.. The people of Hatay are not alone! We will not forget, we will not forgive!' also
www.emniyetyurdu.pol.tr www.polder	13/6/2013 RedHack	Our oppressed, self-sacrificing, long-suffering people have been playing a game for days... We are not slaves! They are not masters either! We are the People and the Peoples never bow You can't forget berkin elvan, you can't protect his murderer
HDP, PKK, Abdullah Öcalan etc.	25.7.2015 TürkhackTeam Anonymous	We love this country and we will not give anyone an inch of land no matter what the cost.
Nearly 400 thousand addresses with “.tr”	14/12/2015 Anonymous	If you do not stop supporting ISIS, we will continue to attack”**
www.rtuk.gov.tr	4/10/2016 RedHack	We condemn attacks agaınst the free press
www.Fgulen.com	14/8/2016 Akıncılar	Hail to the Tall Man. In memory of the Martyrs of July 15.*
700	2/11/2018 Turkz	Cumhuriyet Bayramı hediyesi
www.garantibbva.tr Turk Telekom	27/10/19 Cetinkaya	-
Sinovac	30/12/2020 Root Ayyıldız	"Greetings from the red flag, to the sky flag. May Allah grant us to perform the Friday prayer on the Great Wall of China.

The content analysis applied to DDoS attack news in Turkey provided us with the following outputs:

1. DDoS attacks can be carried out on a local and international scale, as well as organized or individually.

2. Different individuals and groups, positioned for or against the political power in the country, have made their reactions visible by attacking many different targets, local or global, especially on issues and times when freedom of expression is restricted. Due to the anonymous structure and organization of the contractors, especially for DDoS attacks, the issue is both collective action and a foreign policy issue.

3. It has been seen that the target selection is compatible with the desired message. In the attacks targeting the government and the current bureaucrats, the reputation of the state and the nation was taken into consideration,

and the material damage caused did not go beyond being a measure of the effect of the attack and did not become a matter of interest.

4. The DDoS attacks carried out are designed to take into account the messages published by the contractors and do not aim to provide a benefit or cause permanent harm and aimed to ensure that contractors' messages are taken into account.

5. Attacks are actions aimed at becoming a party to a power struggle in cyberspace. It has been observed that the target selection is compatible with the desired message. In the attacks targeting the government and the current bureaucrats, the reputation of the state and the nation was taken into consideration, and the material damage caused did not go beyond being a measure of the effect of the attack and did not become a matter of interest.

6. The motivation for DDoS attacks coincides with the culture of hackers. In other words, it has been seen that DDoS attacks, which have a high economic and social impact, have a reaction mission in the face of ethical and political issues. Following the cyber-piracy culture literature, DDoS attacks have the idea of showing will against unfair practices, disproportionate use of force, oppressive practices and anti-democratic rhetoric. The manifestation of the pirate culture, which wants to show that it will not obey the rules (including language rules) is defiance, sarcasm, humour and slang language.

7. High-impact DDoS-type hacktivist actions are in the range of follow-up activity periods between long sleep periods (overlap with Abhistha et al., 2000).

8.DDoS attacks and broad-based social conflict periods in the country show parallelism. The existence of cyber attacks, where the broadest impact is created, is an expression that the conflict has moved into cyberspace.

Discussion and Conclusion

Cyber crime and threats and DDoS taxonomies in the literature were examined, and priority criteria were determined in this study. The introduction part includes digital democracy and cyber activism in new media opportunities discussed. In the second chapter, in which the literature review of cybercrime taxonomies is presented, DDoS attack taxonomies are outlined. To contribute to the understanding of the hacktivist actions of the information on the public agenda, content analysis including the date, contractor, and messages of the DDoS attacks on the country's agenda applied. First research question, “democratic public space possible in cyberspace? answered by the new media and democracy frame. Cyber public opinion is the socialization and public sharing area of the new media. All new media help to ensure democracy theoretically by providing the function through access to resources, freedom of expression, and justice in equal voting rights, electoral justice, freedom to use alternative news sources, freedom of association and participation. As we seen in the findings of the study with like literature, the new media now offers more opportunities for users to access accurate information or synthesize data, although information pollution causes it to increase exponentially. The propaganda ability, in the hands of the sovereign powers, turns into an opportunity for users who upload and share the information they want to the internet. This makes it possible for all people who can make their voices heard and representatives of different views to make propaganda according to their own ideologies and provides a fairer environment. The second question, depending on what conditions are DDoS attacks defined as hacktivism, cyber terrorism, or the struggle to conquer cyberspace? It is answered in cyber activism, hacking and legal practices. Cybersecurity efforts that do

not follow the public agenda miss the motivation behind cyber activist actions. For this reason, prevalence, message forwarded, number of organic interactions, and official and public agenda should be taken into account in cyber attacks and DDoS classifications. In addition, big data, locators and wearable technology data, forums and social media analytics should be used to follow the agenda of the cyber public. The conquest of cyberspace is determined by the norms to which the explorer is subject, and also the consequences of translation, use, and management of digital spaces lack a universal legal framework. The actions such as cyber warfare, cyber diplomacy and cyber terrorism can be distinct by the guidance of political powers and the maker's motivation, as mentioned in the linked sections of the study. In addition, broad participation in collective actions during high political tension is a substantive criterion, too. DDoS attacks should be handled in the context of cyber public opinion and new social movements. Because they do not aim to conquest cyberspace, but a struggle for existence when cyber actions.

As a mobilization tool, new media is both a tool and a target of cyber activism, which enables participation in contemporary social movements and social/political protests. The power of social media has become more visible to Gezi and conflicts based on internet-based organizations such as Arab Spring and Occupy Wall Street. Howbeit, we should remember the messages that can unite viewers around certain values are also open to manipulation in the new media. There are risks of information pollution, manipulation of society, excessive support of certain groups, polarization, and conflict. The use of social media as a propaganda tool by terrorist and criminal organizations is another dimension of cyber activism (Zizek, 2013). In contrast, we should accept that social media is a quality and popular resource for setting the public agenda. The findings of the study showed parallelism between DDoS attacks and the public agenda of political pressures and anti-democratic practices. However, it cannot be said that DDoS attacks occur every time the public agenda is tense. Challenge-oriented DDoS attacks based on the struggle for existence in cyberspace are not a type of attack for financial gain. On the contrary, they represent cyber public opinion and generally even have the quality of political resistance. Therefore, hacktivism can be considered as a kind of cyber activism aimed at liberating the internet.

National cyber security is gaining importance day by day. New media-based actions need to be accurately questioned and evaluated in today's conditions. Contemporary cybersecurity studies should focus on threat intelligence aimed at preventing cyber attacks before they happen (Robertson et al., 2017). Unfortunately, popular DDoS attacks taxonomies do not measure the criteria to distinguish cyber activist actions from other cyber crimes and do not show cyber activism motivations. As a result, it is suggested to develop taxonomies of cybercrime that are sensitive to the digital activism motivation of actions that receive widespread support and are organized with broad participation and represent the public agenda. Cyber security efforts should not be seen as an obstacle to the democratic and fair use of cyberspace. Official governments should consider the need for democracy and the nature of protest actions against disinterested attacks on the population.

Cyber-activist actions other than hacktivism can be analysed by using social media analyses by extensive subsequent studies. In addition, it will provide valuable data for the cybersecurity field when the international background in the timing of effective DDoS attacks is questioned.

Geniş Özet

Giriş

İnsanlara kendisi olma performansını sergileyecek mecra olarak yeni medya platformları benzer görüşlere sahip insanlarla tanışma ve sosyalleşme imkânı sağlıyor. Böylece, yöndeşik yeni medya akışkan bir kamuoyu oluşturuyor. Fiziksel gerçeklik zaman ve mekân içine sıkışmış ve özgür olmayan bir dünyadır. Siber gerçeklikte doğan, demokratik katılımın sağlanabildiği sanal bir kamuoyunda çeşitli ifade yöntem ve tarzları bulunuyor. DDoS saldırıları, siber saldırıların en yaygın türlerindendir ve beyaz bilgisayar korsanlarınca sıklıkla tercih edilen bir saldırı türüdür.

Gerçek dünyanın siber yansımasını inşaa ederken hacking etkinlikleri naif bir konumda bulunur. Hackerlar, egemen güçlerin, gerçek dünyayı ve eşitsizlikler yeniden inşa ettiği baskıcı varlıklarının siber yansımayla karşı çoğunluğun temsilini sağlarlar. Siber kamuoyunun demokrasi bekçisi konumunda değilseler de bilgisayar korsanları siber uzayda, kamunun iktidar mücadelesinin temsilcisidir. Bu çalışmanın amacı, DDoS saldırılarını siber aktivizm bağlamında incelemektir ki bu çerçevede Türkiye'de yaşanan etkili DDoS saldırıları incelenmiş, amaç motivasyonları yeni toplumsal hareketler bağlamında değerlendirilmiştir.

Yeni medya, taşınabilirlik özelliği ile bilgiye erişimi kolaylaştırarak bilgi okuryazarlığı oranını artırmasına karşın eşitsiz ve sınırlı internet erişimi ekonomik eşitsizliğin yeniden üretilmesine yol açıyor (Giddens, 2012, s.445; Noris, 2001). Taşınabilir ve giyilebilir ortamlarıyla yeni medya, doğal olarak egemenlik mücadelesine dayalı bir siber alandır (Müller & Kramer, 2014). Dijital kamusal alan olarak yeni medya özel ve siyasi alanları hatta bireyleri ve kurumları kapsayan ve birleştiren bir söylem ve eylem siber alanıdır. Yeni medya bağlamında siber kamuoyu toplumsal hareketler ve siyasi çatışmaların mevcudiyetinde aktivist pratiklerin yaygınlaştırılması için uygundur (Castells, 2008; Zizek, 2013). Yeni toplumsal hareketlerin yapısına uygun olarak kadın hareketi, savaş karşıtı ve barış hareketi, çevre hareketi, çiftçi hareketi, nükleer enerji, düşük ücretli işçilere karşı hareket, işçi hareketi ve AIDS hareketi gibi temalarda toplumsal duyarlılık gösteren siberaktivizm eylemleri gerçekleştirilmektedir (Kalafatoğlu, 2010). Dijital aktivizm faaliyetleri tıklama, meta-seslendirme, iddia, politik tüketicilik, dijital dilekçeler, botivizm, e-finansman, veri aktivizmi, ifşa ve hacktivizm olarak sıralanabilir. George ve Leidner (2019) literatürdeki dijital aktivizm fonksiyonlarını fonksiyon ve mekanizma ilişkisini özdeşleşme, inşaat, saldırganlık, aldatma, görünürlük, amplifikasyon olarak sıralamıştır. Siber aktivizmi dijital izleyici etkinlikleri, dijital geçiş faaliyetleri ve dijital gladyatör etkinlikleri başlıkları altında sınıflandırmıştır. Hacktivizm hükümetleri, kamu ve özel kuruluşları ve bireyleri hedef alan ve bir olay veya politika tarafından veya bir grup diğerine göre ayrıcalıklı bir avantaj sağladığında tetiklenen ifşa, verileri yok etme veya kesintiye uğratma eylemleridir (Coleman, 2011). Dijital aktivizm olgusu özellikle sosyal medyanın takibi ve analizleriyle daha net anlaşılır kılacak ve siber suç ile ayrımının sağlanmasını kolaylaştıracaktır.

Siber korsanlarca en popüler eylemi DDoS saldırılarının mantığı, hizmet sitelerinin sunucuları engellemek için sisteme hizmet edemediği kadar sahte kullanıcı göndermek ve işleyişi kesintiye uğratmaktır. Bu eylemlerin amacı şahsi fayda sağlamak değil, düşünce özgürlüğü ve çok sesliliğe olanak sağlayarak siber kamuoyunda baskıcı uygulamalardan uzak tutmaktır.

Siber alanın dostane görünümü ve internetin arkasındaki ağ örgütlenmesi ekonomik süper güçleri maskelemektedir (Başaran, 2010). Gerçek dünyada olduğu gibi, iktidarı bölen sınırlı grubun sömürü ve baskısının varlığı, yeni

medyayı bir aktivizm ve mücadele alanı olarak görmemizi gerektiriyor. Bireyler siber uzayda gerçek dünyada paralel varoluşlar yaşarken, sanal kamunun çok hızlı bir toplumsal oluşumunu ve tüketimini sağlamaktadır. Siber uzay gerçek dünya gibi kirlenmektedir.

Yöntem

Bu, disiplinler arası bir nitel araştırma çalışmasıdır. Çalışmanın amacı, siber aktivizmi diğer siber suçlardan ayırt edecek kriterlerin belirlenmesine yardımcı olmaktır. Literatürün ilk bölümde DDoS saldırılarının arka planı siber aktivizm bağlamında ele alınmıştır. İkinci bölümde siber tehditler, suç, savaş ve siber diplomasi gibi temel kavramlar tanımlanmış ve son bölümünde siber tehdit taksonomilerinde kullanılan ölçütler sorgulanmıştır. Araştırma soruları “siber uzayda "demokratik bir kamusal alan" mümkün müdür?” ile " DDoS saldırıları hangi koşullara bağlı olarak hacktivizm, siber terörizm veya siber uzayı fethetme mücadelesi olarak tanımlanır?” Bulgular aşamasında Türkiye gündemini en çok etkileyen siber saldırılar, arşivler taranarak tespit edilmiştir. Alexa verilerine göre farklı medya kuruluşlarına ait en çok tıklanan üç internet haber sitesi seçildi. Ensonhaber.com, Hurriyet.com.tr ve Sözcü.com arşivleri taranmıştır. Arşiv "hacker, "cyber hacker", "crashed", "DDoS" anahtar kelimeleri ile taranmıştır. Siber saldırı haberleri; üstlenici, tarih ve mesajlar ölçütleri ile incelenmiştir. Hacking eylemlerinde verilen mesajlara , yeni toplumsal hareketler bağlamında, içerik analizi uygulanmıştır. Sonuç bölümünde ise elde edilen bulgular literatür ışığında değerlendirilerek DDoS saldırısı taksonomilerinde hukuk ve etiği koruma motivasyonlarla gerçekleştirilen siber aktivist eylemlerin ayırt edilebilmesi için bütünleşik bir yaklaşım önerilmiştir.

Sonuç

Yeni medyanın sağladığı imkanlar, paylaşım ve demokrasi kültürünü geliştirir. Siber uzayda insan temelli, siber aktivizm yoluyla canlı ve dinamik bir kamuoyu oluşmaktadır. Bu kamuoyu, yeni toplumsal hareketler çerçevesinde ele alındığında, siber aktivizmin agresif bir türü olan haktivizm genellikle kar amaçlı değil, meydan okuma, baskılara direnme ve siyasal duyarlılık kökenlidir. Geniş bir katılımın söz konusu olduğu haktivist eylemler gerçek bir yerel ve küresel kamuoyu gündemi ile paralellik gösteriyor ise demokratik egemenlik mücadelesi olarak tanımlanabilir. Siber uzayın demokratikliğini sağlamak için, tüm çatışmaları ile toplumsal gruplar da özgürce temsil edilebilmelidir. Mevcut güç mücadelelerini siber alana taşıyan devletler ve egemen kullanıcılar siber demokrasiyi kısıtlamaktadır. Yeni medya ve siber aktivizm çerçevesinde ele alınan bu çalışmada, siber aktivizmin marjinal ve saldırgan bir türü olan hacktivizm motivasyonu siber alanda varlığını ve gücünü kanıtlamak olarak kabul edilmektedir (Coleman, 2011).

Günümüzde en yaygın görülen siber saldırılar dağıtık hizmet engelleme (DDoS), Man in the Middle (MiM), oltalama, yetki ihlali, bombalar (Mantık veya Zaman), tarama, kontrolleri atlama, veri değişiklikleri, hizmet reddi, gizli dinleme, yasadışı kullanım bilgi sızıntısı, veri engelleme/değiştirme, girişim, veri tabanı sorgu analizi, maskeleme, fiziksel izinsiz giriş, reddetme, kaynak tüketme, sabotaj, süpürme, casusluk, hizmet sızdırma, sniffers, ikame, terör, hırsızlık, trafik analizi, tuzak kapı/arka kapı, Truva Atı, tünel açma, yetkisiz erişim, izin ihlalleri, yetkisiz erişim, bindirme, virüs ve solucanlar olarak örneklendirebiliriz.

Siber saldırı türleri; hırsızlık, dolandırıcılık, siber terörizm, sanal zorbalık, taciz, şantaj, veri sızdırma ve ifşa yoluyla şantaj gibi çeşitli suç motivasyonlarına göre gerçekleştirilir. Bilişim sistemleri aracılığıyla işlenen bu

suçlar fiziksel gerçeklikte cezalandırılmaktadır. Siber suçlar, gerçek suçların siber dünyadaki yansımasıdır. Korsan kültürü çevresinde, temel motivasyonları meydan okuma, gündeme paralel tepki gösterme ve adalet arayışı olan ve maddi çıkara dayanmayan en popüler siber saldırı türü ise DDoS'tur ve sadece çevrimiçi olarak gerçekleştirilen, fiziksel hayatta karşılığı olmayan bir eylemdir. Bu nedenle suç vasfını değerlendirme aşamasında daha fazla parametrenin analizi gereklidir. DDOS saldırıları siber uzayda iktidar ve kamu yönetimi mücadelesinin temsilcisi olan korsanlar tarafından en çok tercih edilen saldırı türlerinden biridir. Literatürde incelenen başlıca siber suç ve DDOS taksonomilerinde odak noktaları suçun amacı, suçlunun pozisyonu, hedefi, şiddeti, yarattığı hasar, kurban ve suçlunun kullandığı donanım, yazılım ve tekniklerdir. İncelenen ölçütler değişiklik gösterse de bu odak noktalarına göre seçilerek analiz edilmektedir. Saldırganın amaç motivasyonu ağırlıklı olarak maddi çıkar sağlama, suistimal ya da siber milislik yönelimlerini ölçen kriterlerdir. Bu taksonomilerin genel olarak toplumsal çatışma süreçlerini yansıtmadığı ve kamu gündeminden de kopuk olduğu görülmüştür. Siber aktivizmi diğer siber suçlardan ayırt edebilmek için Türkiye'de haber değeri görülen DDoS saldırıları tarihleri, üstleniciler ve onların mesajlarını içeren bir tablo ile bulgular sunulmuş ve literatür çerçevesinde yorumlanmıştır

Kamuoyu gündemini gözetmeyen siber güvenlik çalışmalarında, siber aktivist eylemlerin demokratik motivasyonunu gözden kaçırılması kaçınılmaz olacaktır. Siber demokrasinin sağlanması için siber uzayda var oluş mücadeleleri ve egemenlik mücadeleleri sınırlandırılmamalıdır. Siber uzay bir savaş alanından ziyade sonsuz bir varoluş pratiği ve iktidar mücadelesi olarak tanımlanmalıdır. Kamunun da yansımasını kapsayan siber uzayın savaş olanı olarak tanımlanması siber diplomasi ve siber güvenlik endişeleri demokrasiyi karanlıkta bırakmasına yol açmaktadır.

Sonuç olarak dijital aktivizm motivasyonuna duyarlı, kamu gündemini takip eden, yaygın destek alan ve geniş katılımla organize edilen eylemleri gözeten siber suç taksonomilerinin geliştirilmesi önerilmektedir. Siber saldırı taksonomilerinde siber aktivist motivasyonları görünür kılmak için yaygınlık, katılımcı sayısı, desteklenme yüzdesi, iletilen mesajların analizi, organik etkileşim sayısı, resmi gündem ve kamuoyunda gündemi gibi belirleyici ölçütlerin de DDOS taksonomilerine dahil edilmesi önerilmiştir. Mobil haberleşme uygulamaları, forumlar ve sosyal medyanın organik hareketiliği, lokasyon belirleyiciler ve giyilebilir cihazların verilerinin de gerçek dijital kamuoyu gündemini belirlemeye yardımcı olabileceği düşünülmektedir. Bu konuda gerçekleştirilecek daha geniş çaplı çalışmalarda sosyal medya analizlerinden yararlanılarak hacktivism dışındaki siber aktivist eylemler de analiz edilebilir. Siber suç taksonomilerinde güvenilir bir kamuoyu gündemi verisinin değerlendirilmesi siber güvenlik çalışmaların anlamlı bir katkı sağlaması beklenmektedir. Ek olarak etkili DDoS saldırılarının zamanlamasındaki uluslararası arka planının sorgulanması siber güvenlik alanı için değerli veriler sağlayacaktır.

Teşekkür ve Bilgilendirme

Bu araştırma makalesi özgündür ve bir tez ya da projenin bir parçası olarak üretilmemiştir. Bu araştırma makalesi için bir fon ya da kurum tarafından destek alınmamıştır. / This article is not submitted as a proceeding and is not a part of a project or dissertation. This article is not supported by a research institution or a fund.

Yayın Etiği Bildirimi

Bu araştırma makalesinin etik sorunu olmadığını beyan ederim. / I hereby declare that this research article does not have an unethical problem.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Bu makale tek bir araştırmacı tarafından hazırlanmıştır. / The article is prepared by one author. No contribution rate by another researcher.

Çıkar Çatışması / Conflict of Interest

Bu araştırma makalesinde bir çıkar çatışması bulunmamaktadır. / The study has no conflicts of interest.

Fon Bilgileri / Funding

Bu araştırma makalesi için bir fon ya da kurum tarafından destek alınmamıştır./ This article is not supported by a research institution or a fund.

Etik Kurul Onayı / The Ethical Commitee Approval

Bu araştırma makalesinin etik sorunu olmadığını beyan ederim. / I hereby declare that this research article does not have an unethical problem.

Kaynakça / References

Abhishta, A., Van Heeswijk, W., Junger, M., Nieuwenhuis, L. J., & Joosten, R. (2020). Why would we get attacked? An analysis of attacker's aims behind DDoS attacks. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 11*(2), 3-22.

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2010, October). Dealing with the problem of cybercrime. in International Conference on Digital Forensics and Cyber Crime (pp. 1-18). Springer, Berlin, Heidelberg.

Arendt, H., Dworkin, R., Habermas J., Galtung M.L., Saner H., Rawls J., Thoreau H.D., (1997). *Sivil itaatsizlik*. İstanbul, Ayrıntı.

Averweg, U. R., & Leaning, M. (2018). The qualities and potential of social media. In *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 7106-7115). IGI Global.

Başaran, F. (2000). İletişim ve emperyalizm: Türkiye'de telekomünikasyonun ekonomi-politiği. Ütopya Yayınevi

Bayhan, V. (2014). Yeni toplumsal hareketler ve Gezi Parkı direnişi. *Birey ve Toplum Sosyal Bilimler Dergisi, 4*(1), 23-58.

Bjola, C., & Holmes, M. (2015). *Digital diplomacy* . Taylor & Francis.

Bıçakcı, S., Ergun, F. D., & Çelikpala, M. (2015). The Cyber security scene in Turkey. EDAM: The Centre for Economics and Foreign Policy Studies, Istanbul, Turkey. http://edam. org. tr/document/CyberNuclear/edam_cyber_security_ch2. pdf.

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace.* Santa Barbara, California: Praeger.

Castells, M. (2008). Enformasyon Çağı: Ekonomi, Toplum ve Kültür, Birinci Cilt: Ağ Toplumunun Yükselişi, çev. *Kılıç, İstanbul: İstanbul Bilgi Üniversitesi*.

Chandra, A., & Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems, 38*, 100467.https://doi.org/10.1016/j.accinf.2020.100467

Choo, K. K. R., Smith, R. G., McCusker, R., & Choo, K. K. R. (2007). Future directions in technology-enabled crime: 2007-09. *Research and Public Policy series 78*, Canberra: Australian Institute of Criminology.

Crowley, D., & Heyer, P. (2015). *Communication in history: Technology, culture, society.* Routledge.

Dahl, R. A. (2001). *Political Equality in the Coming Century. In Challenges to Democracy* (pp. 3-17). Palgrave Macmillan, London.

Davenport, T., & Prusak, L. (2000) *Working Knowledge: How Organisations Manage What They Know.* New preface edition, Harvard Business School Press, Boston, MA.

Denning, D. E. (2000). *Barriers to Entry: Are They Lower for Cyber Warfare*? Calhoun, Dudley Knox Library. http://hdl.handle.net/10945/37162

Derbyshire, R. , Green, B., Prince, D.,İ, Mauthe, A. and Hutchison D., (2018). An Analysis of Cyber Security Attack Taxonomies," 2*018 IEEE European Symposium on Security and Privacy Workshops. (EuroS&PW), 2018*, pp. 153-161, doi: 10.1109/EuroSPW.2018.00028.

Faritha, B., J, Revathi, R., Suganya, M.,& Gladiss M. N. (2020). IoT based Cloud Integrated Smart Classroom for smart and a sustainable Campus. *Procedia Computer Science*, *172*, 77-81. https://doi.org/10.1016/ j.procs.2020.05.012

Flynn, I. (2021). *Deliberative democracy*. John Wiley & Sons.

Franz, A., Zimmermann, V., Albrecht, G., Hartwig, K., Reuter, C., Benlian, A., & Vogt, J. (2021). SoK: Still Plenty of Phish in the Sea—A Taxonomy of User-Oriented Phishing Interventions and Avenues for F u t u r e Research. In Seventeenth Symposium on Usable Privacy and Security ({SOUPS} 2021) (pp. 339-358).

Friedman, L. W., & Friedman, H. H. (2008). The new media technologies: Overview and research framework. Available at SSRN 1116771.

Gazeteciler Cemiyeti. (2019). İfade ve Basın Özgürlüğü Eylül 2019 Raporu.http://media4democracy.org/public/uploads/reports_4696242.pdf.

George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization, 29*(3), 100249.https://doi.org/10.1016/j.infoandorg.2019.04.001

George, J. J., & Leidner, D. E. (2018). Digital activism: A hierarchy of political commitment. https://doi.org/10.24251/HICSS.2018.288

Golman, R., & Loewenstein, G. (2015). Curiosity, information gaps, and the utility of knowledge. Information Gaps, and the Utility of Knowledge (April 16, 2015), 96-135.

Goode, L. (2015). Anonymous and the political ethos of hacktivism. *Popular Communication, 13* (1), 74-86. https://doi.org/10.1080/15405702.2014.978000

Grasmick, H. G., & Bursik, R. J. (1990). Conscience, significant others, and rational choice: Extending the deterrence model. *Law & Society Review, 24*(3), 837–861. https://doi.org/10.2307/3053861

Gürdal, E. (2021). Dijital Diplomatlar: Dijital Diplomaside Yeni Nesil Diplomatlar. *Bitlis Eren Üniversitesi İktisadi ve İdari Bilimler Fakültesi Akademik İzdüşüm Dergisi, 6*(1), 114-127.

Hansman S. & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computer and Security*. https://doi.org/10.1016/j.cose.2004.06.011

Harry, C., & Gallagher, N. (2018). Classifying Cyber Events: A Proposed Taxonomy. *Journal of Information Warfare, 17*(3), 17–31. https://www.jstor.org/stable/26633163

Howard, J. D, & Longstaff, T. A. A (1998). Common language for computer security incidents. United States. https:// doi.org/10.2172/751004

Hunsinger, J. & Schrock, A. (2016). Democratization of hacking and construction. New Media and Society, 18 (4), 535-538.Indrajit, R. E., et al., "The Taxonomy of Cyber Threats to National Defense and Security," 2021 Sixth International Conference on Informatics and Computing (ICIC), 2021, pp. 1-8, doi: 10.1109/

Johnson, P. & Robinson, P. (2014), Civic Hackathon: Procurement or Civic Engagement? *Review of Policy Research*, *31*: 349-357. https://doi.org/10.1111/ropr.12074

Kang, D. J., Lee, J. J., Kim, S. J., & Park, J. H. (2009, October). Analysis on cyber threats to SCADA systems. In 2009 *Transmission & Distribution Conference & Exposition: Asia and Pacific* (pp. 1-4). IEEE.

Kaur, S., Kumar, K., Aggarwal, N., & Singh, G. (2021). A Comprehensive Survey of DDoS Defense Solutions in SDN: Taxonomy, Research Challenges, and Future Directions. *Computers & Security*, 102423.https://doi.org/ 10.1016/j.cose.2021.102423

Kjaerland, M. (2005). A Classification of Computer Security Incidents Based on Reported Attack Data. *Journal of Investigative Psychology and Offender Profiling*, *2*(2), 105–120. https://doi.org/10.1002/jip.31 .

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*, *25*(7), 522-538.

Kumar, S., & Carley, K. M. (2016, September). Understanding DDoS cyber-attacks using social media analytics. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 231-236). IEEE.

Keleş, A.,R. & Sal, Y. (Edt.)(2013) *Hack kültürü ve hacktivizm.* Alternatif Bilişim

Kelsey, J. T. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. *Michigan Law Review, 106*(7), 1427–1451. https://search.informit.org/doi/10.3316/ agispt.20191230022228

Lough, D. L. (2001). A taxonomy of computer attacks with applications to wireless networks (Doctoral dissertation, Virginia Polytechnic Institute and State University).

Nazario, J. (2008). DDoS attack evolution. *Network Security*, (7), 7-10.

Losh, E. (2012). Hacktivism and the humanities: Programming protest in the era of the digital university. Gold& Klein (Edt.), Debates in the digital humanities, 161-186. University of Minnesota.

Magklaras, G. B., & Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, *21*(1), 62-73.

Manovich, L. (2002). *The language of new media*. MIT press.

Meyers, C. A, Powers, S. S., & Faissol, D M. (2009). *Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches*. United States. https://doi.org/10.2172/967712.

Mirkovic J. & Reiher, P. (2004). A taxonomy of ddos attack and ddos defense mechanisms, *Computer Communication Review*, *34*, (2). https://doi.org/10.1145/997150.997156

Moitra, S. D. (2004). Cybercrime: Towards an assessment of its nature and impact. *International Journal of Comparative and Applied Criminal Justice*, *28*(2), 105-123.

Müller, B.,& Kremer, J. F. (Eds.)(2014). Cyberspace and International Relations. Berlin: Springer. https://doi.org/10.1007/978-3-642-37481-4.

Nazario, J. (2008). DDoS attack evolution. Network Security, (7), 7-10.

Nikolskaia, K. & Minbaleev, A. (2020). Legal Regulation of Incidents Related to DDoS Attacks, 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), p. 53-55, doi: 10.1109/ITQMIS51053. 2020.9322874.

Norris, P. (2001). Digital divide: Civic engagement, information poverty, and the Internet worldwide. Cambridge university press.

O'Malley, G. (2013). Hacktivism: Cyber Activism or Cyber Crime. *Trinity College Law Review*, *16*, 137-160.

Onat, N. (2013). Kamusal Alan ve Sınırları: Hannah Arendt ve Jürgen Habermas'ın Yaklaşımları, İstanbul, Durakistanbul.

Pedersen, I. (2013). *Ready to wear: A rhetoric of wearable computers and reality-shifting media*. Parlor Press LLC.

Riordan, S. (2016). Cyber diplomacy vs. digital diplomacy: a terminological distinction. CPD Blog.

Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). Darkweb cyber threat intelligence mining. Cambridge: Cambridge University Press. doi:10.1017/9781316888513

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist*, *55*(1), 68. https://doi.org/10.1037/0003-066X.55.1.68

Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016a). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, *4* (6).

Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016b). Cybercriminals, cyberattacks and cybercrime," *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 2016, pp. 1-9, doi: 10.1109/ICCCF.2016.7740434.

Schäfer, M. S. (2015). Digital public sphere. *The international encyclopedia of political communication*, *1*(7).

Schrock, A. R. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. New media & society, 18(4), 581-599.Selander, L., & Jarvenpaa, S. L. (2016). Digital Action Repertoires and Transforming a Social Movement Organization. *MIS Quarterly*, *40*(2), 331–352. https://www.jstor.org/stable/26628909

Schultz, P. W. (2002). Knowledge, information, and household recycling: Examining the knowledge-deficit model of behavior change. New tools for environmental protection: Education, information, and voluntary measures.

Sherizen, S. (1990). Criminological concepts and research findings relevant for improving computer crime control. *Computers & Security, 9(*3), 215-222.

Shorter, C. R. (2014). Digital Diplomacy in an Era of Rising Social Powers: How New Media Impacted the Practice of Public Diplomacy by Empowering Citizens and Terrorist Organizations (Doctoral dissertation, Webster University, London).

Singh, M. P., & Bhandari, A. (2020). New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges. *Computer Communications, 154*, 509-527.https://doi.org/10.1016/j.comcom.2020.02.085

Simmons, C.B., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2014, June). AVOIDIT: A cyber attack taxonomy. In 9th Annual Symposium on Information Assurance (ASIA'14) (pp. 2-12).

Sousa, H., Pinto, M. Silva, E.C. (2013). Digital public sphere: weaknesses and challenges.*Comunicação e Sociedade, 23*, pp. 9 – 12

Specht, S.M., & Lee, R.B. (2004). Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. PDCS.

Timisi, N. (2003). *Yeni İletişim Teknolojileri ve Demokrasi*. Ankara: Dost Kitabevi Yayınları.

Urbas, G., & Choo, K. K. R. (2008). Resource materials on technology-enabled crime. Australian Institute of Criminology,Technical Bacground Paper no:28

Venkatraman, S. (2008). *The "Darth" side of technology use: Cyberdeviant workplace behaviors*. University of Arkansas.

Yengin, D., & Bayrak, T. (2017). Digital public in social media. *The Turkish Online Journal of Design, Art and Communication, 7* (2), 376-386.

Yu, S. (2014). *Distributed denial of service attack and defense.* Springer.

Zhu, B., Joseph, A., & Sastry, S. (2011, October). A taxonomy of cyber attacks on SCADA systems. In 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing (pp. 380-388).

Zizek, S. (2013). *Tehlikeli rüyalar görme yılı* (M. Öznur ve B. Özkul, Çev.). İstanbul: Encore Yayınları.

2022

4(2), 197-226

Uzaktan Eğitimde Veri Madenciliği Yöntemi Kullanılarak Yapılmış Araştırmalarda Öğrenme Çıktıları Üzerine Sistematik Bir İnceleme

Elif Akgün*[1], Özlem Maral Karanfil[2]

Anahtar Sözcükler

Veri madenciliği
Uzaktan eğitim
Öğrenme çıktısı
Sistematik inceleme

Makale Hakkında

Gönderim Tarihi
15 Haziran 2022
Kabul Tarihi
18 Aralık 2022
Yayın Tarihi
28 Aralık 2022
Makale Türü
Araştırma Makalesi

Öz

Bulunduğumuz çağın ve sürekli değişen teknolojinin sonucunda elde edilen veriler her geçen gün artmaktadır. Bu veriler ile en hızlı, anlamlı ve ileriye yönelik doğru tespitler elde etmek, veri madenciliği ile mümkün olmaktadır. Kısaca ifade etmek gerekirse elde edilen ham bilgiyi veriye, verileri bir sanatkâr gibi işleyip bir esere dönüştürülmesine veri madenciliği olarak tanımlanmaktadır. Veri madenciliği birçok alan için büyük öneme sahiptir. Veri madenciliği sağlık, teknoloji, eğitim gibi geniş kullanım alanları bulunmaktadır. Bu alanların eğitim başlığının kapsamında bulunan alt başlığı ise eğitsel veri madenciliğidir. Eğitsel veri madenciliğinin konusu geleneksel ve uzaktan eğitim çalışmalardır. Bu araştırmada da uzaktan eğitimde veri madenciliği kullanılarak ulaşılan sonuçlardan öğrencilerin öğrenme çıktısına etkisinin ilgili araştırmalardaki eğilimler sonucunda belirlenmesi amaçlanmıştır. Araştırmada uzaktan eğitim ve veri madenciliği kavramları kapsamında Web of Science veri tabanından ulaşılan çalışmaların sistematik incelemesi yer almaktadır. Bu kapsamda bu çalışma literatürdeki çalışmaların analizini sunmayı ve bu yönüyle araştırma uzaktan eğitimin öğrenme çıktılarına etkisinin veri madenciliği ile sonucunu görebilmelerini sağlayacaktır. Ayrıca sistematik inceleme sonucunda araştırma alanında ihtiyaç duyulan çalışmaların belirlenmesi, araştırmacılar için yol gösterici olacağı düşünülmektedir.

A Systematic Analysis on Learning Outcomes in Researches Using Data Mining Method in Distance Education

Keywords

Data mining
Distance education
Learning output
Systematic review

Article Info

Received
June 15, 2022
Accepted
December 18, 2022
Published
December 28, 2022
Article Type
Research Paper

Abstract

The data obtained as a result of the age we live in and the constantly evolving technology is increasing day by day. With this data, it is possible to obtain the fastest, most meaningful, and more accurately predictable decisions through data mining. To put it briefly, data mining is defined as the act of processing raw information obtained into data, processing that data like an artist, and transforming it into a work. Data mining is of great importance in many fields. Data mining has a wide scope of usage in numerous industries, including health, technology, and education. Within the scope, educational data mining is the sub-title. Traditional and distant education studies are the focus of educational data mining. The aim of this study is to determine the effect of the results obtained by using data mining in distance education on the students' learning outcomes as a result of the trends in related research. In the research, studies accessed from the Web of Science database were systematically reviewed within the scope of the concepts of distance education and data mining. In this context, this study will provide an analysis of the studies within the literature and therefore, the effect of distance education on learning outcomes as seen by data mining. In addition, it is thought that determining the studies needed in the research area as a result of a systematic review will be a guide for researchers.

***Atıf*:** Akgün, E. & Maral Karanfil, Ö. (2022). Uzaktan eğitimde veri madenciliği yöntemi kullanılarak yapılmış araştırmalarda öğrenme çıktıları üzerine sistematik bir inceleme, *Bilgi ve İletişim Teknolojileri Dergisi, 4*(2), 197-226. https://doi.org/10.53694/bited.1131475

***Cite*:** Akgün, E. & Maral Karanfil, Ö. (2022). A systematic analysis on learning outcomes in researches using data mining method in distance education, *Journal of Information and Communication Technologies*, *4*(2), 197-226. https://doi.org/10.53694/bited.1131475

*__Sorumlu Yazar/Corresponding Author__: elifakgunn98@gmail.com
[1] M.Sc. Student, Bartin University, Bartin/Turkey, elifakgunn98@gmail.com , https://orcid.org/0000-0003-2580-9896
[2] M.Sc. Student, Bartin University, Bartin/Turkey, ozlemmaral890@gmail.com , https://orcid.org/0000-0002-2378-6945

Extended Abstract

Introduction

Information in today's age is turning to data mining. Data mining is a method used to analyze data stacks so they can serve the purpose of being used and transformed into new data, and as a result, relate to each other. One of the areas where data mining is used is educational data mining. Traditional and distance education types are two important subject areas of educational data mining. The factors that will affect students' success and performance are changing as education policies change and develop. For this reason, the study includes a systematic review of the effect of distance education on students' learning outcomes using the data mining method. This study will provide an analysis of the studies included within the literature, and in this respect, the effect of distance education on learning outcomes will be observed with data mining. In addition, it is thought that by determining the studies needed in the research area through systematic review, it will be a future guide for researchers. The results of the research were examined according to the years, the keywords extensively used, the methods used, the data collection tools, the participant profiles, the country where the study was carried out, the learning areas, the technology used, the data mining classification method used, and the learning outcomes examined in scientific studies.

Method

A systematic review design was used in this study based on the literature review. It is thought that determining the studies needed in the research area as a result of the systematic review will be a guide for researchers. In this context, it consists of studies published in the Web of Science database up until April 2022 without any year limitation, only in English, with the keywords "data mining" and "distance education." The result of the established criteria and examinations was an analysis of 93 studies, recorded on a Microsoft Excel form. The data was analyzed after the review of all the studies was completed.

Findings

Within the scope of this study, data was presented within the context of the related research questions. First of all, when we look at the years from the sub-problem titles, it is seen that there were at most 13 scientific studies in 2016, and the data set used the most was a quantitative research method and data collection tool with a maximum rate of 53%. In addition, as a result of the analysis according to the participant profile, it was determined that the student profile in distance education mostly consisted of university students. As a result of the analyses, most studies were done in China, as well as a majority were in the field of computers, and the keywords "distance education" and "educational data mining" were used the most in related studies. The studies were examined based on the technology support used, taking into account the technological environments in which the data were obtained and the environments in which the data were analyzed As a result of the examinations, Moodle was preferred the most as the environment to obtain data, but the LMS used in nine studies was not specified. For the analysis of the obtained data, Weka (N = 9) was mostly preferred as the data mining software tool. In the studies examined, it is seen that the clustering (N = 31) method is mostly used in the context of data mining classification methods. In the second place, it was determined that the decision tree (N = 21) was used in high numbers, while the other methods were: the Bayes classifier was used in ten studies, the artificial neural network in seven studies,

the association rule in six studies, and the support vector machines in two studies. Within the scope of this study, it was determined that the highest achievement (N = 12) was considered as a learning outcome. Then, other topics that were considered as learning outcomes were found to be motivation (N = 7), performance (N = 6), quitting (N = 5), self-regulation (N = 2), and learning environment atmosphere (N = 2). As a conclusion of these results related to learning outcomes, the success rate of students in distance education is inversely proportional to their age. This shows that as the age of the students increases, the success score decreases. When distance education and formal education scores were compared, it was found that the scores were higher in formal education. It has been revealed that student activities in distance education are affected by teacher activities. In this case, when teachers make more active efforts, students become passive. It has been concluded that the greater the number of students logging in to the distance education system platform, the more difficult it is for the students, but the better their performance. Studies show that teaching self-regulation is important not only in lessons but also in life.

Discussion and Conclusion

Modeling student performance with data mining according to the data obtained from the online environment is important in terms of predicting possible failures of students who have a tendency to drop out or have inadequate motivational self-regulation skills. The obtained data can be adapted by making models suitable for the user or student. On the other hand, it is important to monitor the academic performance of students in online learning environments where the number of students is much higher when compared to traditional learning environments in terms of analyzing them. As a result of the information obtained by focusing on the effects of the online learning environment on the students, it is observed that the data is made meaningful by data mining and has a positive effect on the students.

Giriş

Günümüzde içinde yaşadığımız bilişim ve teknoloji çağında var olan veri kaynaklarının ve bilginin artması nedeniyle ilk olarak veri depolama ihtiyaçları ortaya çıkmıştır. Veri, en genel tanımıyla ham, işlenmemiş kayıt anlamını ifade etmektedir. Verilerin analiz ve sentezlenmesi birlikte elde edilen kavrama ise bilgi denilmektedir. Bilgi, nihai sonuç için etkili bir karar sürecidir (Bezerra & Silva, 2020). Bu verilerin ya da bilgilerin artmasıyla birlikte kavramları işleyebilen depolayabilen teknikleri kullanmak, büyük oranda önem kazanmaktadır. Milyarlarca veri kaynağına sahip yazılım sistemlerinin, verilerini ve bilgilerini kıymetli hale getirmek için yapılan çalışmalara da veri madenciliği denir. Veri madenciliği var olan eldeki veriler ile örüntüler kurarak gelecek çağda veriler üzerinde anlamlı tahminlerde bulunmasını mümkün kılmaktadır. Bu bağlamda veri madenciliği kurumlardan ve kişilerden sağlanabilecek veriler üzerinde işe yarayabilecek verileri bulmak için süzme işlemini belirli yöntemler ile yaparak elverişli veri haline getirme amacı taşımaktadır. İlgili amaç doğrultusunda veri madenciliği her alanda kısacası verilerin üretildiği ve depolandığı her yerde kullanılabilmektedir (Erten, 2015). Bu kullanım alanlarına örnek olarak; sağlık ticaret, risk analizleri, bankacılık, pazar araştırması ve eğitimdir sayılabilmektedir.

Veri Madenciliği Nedir?

Veri Madenciliği, büyük boyuttaki verilerin içerisinden birbirleri ile anlamlı verileri alıp uygun yöntemler ile verilerin geleceği hakkında en doğru öngörüde bulunup ve çok sayıda keşfedilmemiş bilgiyi ortaya çıkarıp var olmasında kullanılır (Uzun, Uzun, & Çakar, 2021). Veri madenciliği belirli bir amaç doğrultusunda kullanılabilecek bilgiye ulaşmak için büyük veri kümelerinde analiz yapma işlemidir. Veri madenciliğine uygun amaçlar 3 başlıkta toplanabilmektedir (Zang & Lin, 2003). Bu amaçlar;

Tahmin-Risk: Herhangi bir ürünün detaylı incelenmesinden sonra satın almayan dijital kullanıcıların sayısını ya da geçmişte işlerin neden iyi neticelenmediğini belirlemek, bir firmanın ileriki zamanlarda satışa sunulup alacak müşterinin olumlu karar vermesine yardımcı olabilir.

Gruplandırma: Dijital kullanıcılar tarafından temin edilen veri kaynakları, firmaların müşterilerini beğendikleri ya da ziyaret ettikleri uygulamalardan cinsiyetini, yaşını, kazancını, bulunduğu yeri ve tüketim alışkanlıklarını dayanarak farklı yollarla kategorileştirmeyi sağlar. Bu nedenle, kişiye özel teklifler veya mesajlar ihtiyacı olan kullanıcılara uygun şekilde ulaşılması hedeflemektedir.

Davranış Analizi: Elde edilen verilerin detaylı incelenmesi ile firmaların, müşterilerin nasıl uygulamalardaki uyarıcılara tepki verildiğini anlar. Örnek olarak bazı kullanıcıların ya da grupların belirlenmiş tekliflere veya e-postalara belirli bir zaman aralığında ya da haftanın belirlenmiş bir gününde daha çok tepki verildiği anlaşılabilmektedir.

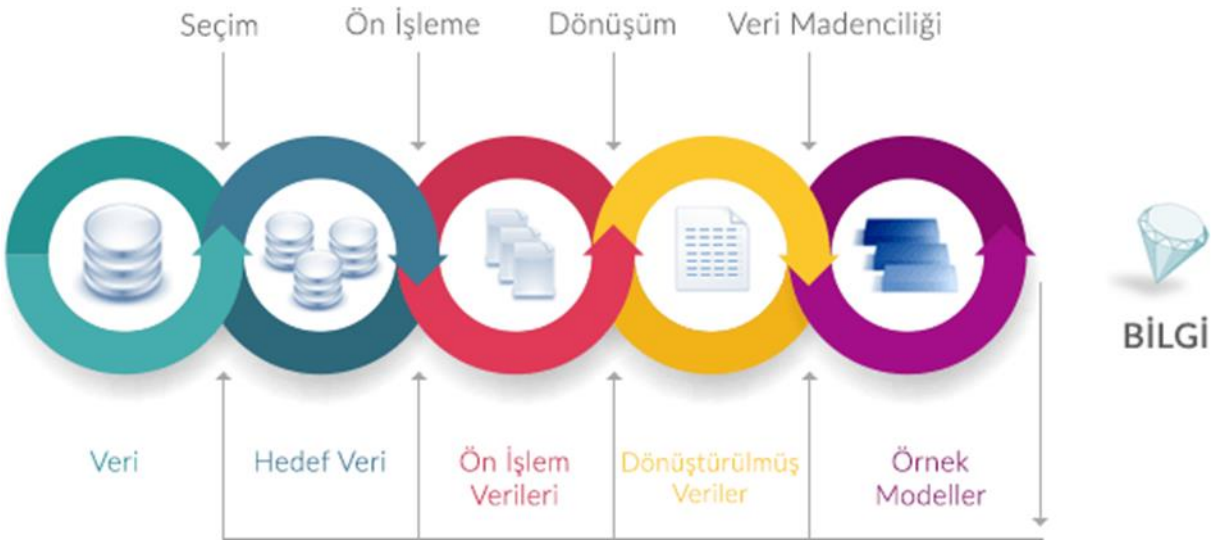
Veri Madenciliği Süreçleri

Veri madenciliğinde bir bilgiye ulaşmak için genel olarak şu adımların gerçekleşmesi gerekmektedir (Çoşlu, 2013):

- İlk adımı veri yığını tespit edilir. Verilerin güvenliği sağlanır.
- Elde edilen verilerden uygun olmayan bir anlam ifade etmeyenleri süzgeçten geçirilir.
- Kalan veriler analiz edilip sentezlenir ve dönüştürülür.

- Kalan verileri, veri madenciliğine uygun olan sınıflandırma, kümeleme, karar destek ağacı gibi yöntemler ile veriler kategorileştirilir.
- Sonuçlar, test edilir ve sonuçlar değerlendirilir.

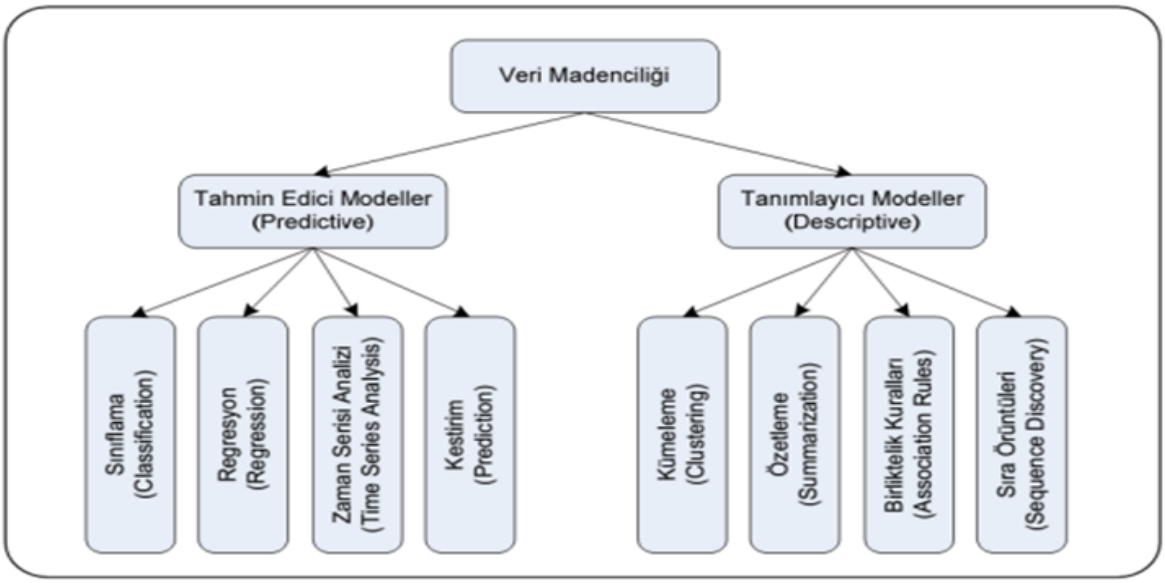
Veri madenciliği sürecinin aşamaları Şekil 1'de görülmektedir.



Şekil 1. Veri Madenciliği Süreçleri (Çoşlu, 2013)

Veri Madenciliği Yöntemleri

Veri madenciliği kapsamında planlanmış her bir verinin işlenmesi için birbirinden farklı yöntemler bulunmaktadır. Yöntemler probleme uygun olan yöntem seçilip hedeflenen nihai amaca hizmet etmelidir. Bu yöntemler ayrıntılı olarak incelendiğinde birbirinden farklılık gösterdiği gözlenmektedir. Yöntemin ortaya konulması için temel olarak problem ortaya konmalıdır. Bu ana temayla birlikte veri madenciliği sınıflandırılmıştır. Sınıflandırılan yaklaşımlar Şekil 2'deki gibidir.



Şekil 2. Veri madenciliği yöntemleri (Aydın, 2007)

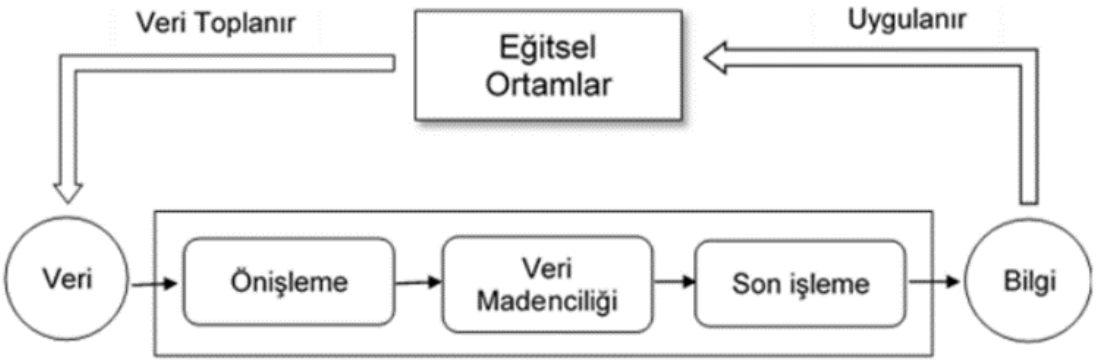
Tahmin edici modellerde amaç verileri işlenerek bir anlamlı örüntüler oluşturulup, bu anlamlı örüntü birlikte elde edilen veriler ile tahminde bulunulmaya çalışılıyorsa, bu sonuç ile birlikte kullanılabilecek veri madenciliği yöntemleri tahmin edici kategori başlığında gruplandırılmıştır. Tanımlayıcı model ise elde bulunan veriler hakkında bilgi çıkarılmaya ve bu verilerin özellikleri farklı şekillerde ifade edilmeye çalışılıyorsa, tanımlayıcı başlığı altında toplanmıştır. Veri madenciliğinin kullanılan temel yöntemleri birçoğu istatistiksel yöntemlerle belirlenmektedir. Veri madenciliğinde yaygın olarak kullanılan bazı standart yöntemler aşağıdaki gibidir.

- Sınıflandırma
- Kümeleme
- Karar ağaçları
- Sinir ağları
- Bayes Teoremi

Sınıflama verilerin daha önceden belirlenmiş olan gruplarda hangisine ait olduğunu tespit eden yöntemler bütünüdür. Sınıflama problemi olarak ele alınabilecek her problemde kullanılabilmektedir (Aytaç, 2018). Kümeleme (clustering) birbirlerine benzeyen veri kaynaklarını ayrıştırma işlemidir. Kümeleme yöntemlerinin çoğu veri parçaları arasındaki mesafeyi kullanarak rota sağlar. Kümeleme yöntemi denilince akla ilk en yakın komşu algoritması gelmektedir (Özkan, 2016). Karar ağaçları verileri birbirinden ayırarak bir ağaç gibi yapı oluşturmak bu yapıda doğru kolayca karar vermeyi amaçlamaktadır. Karar ağacı yönteminin ana teması makine öğrenmesi fikrine dayanmaktadır (Aytaç, 2018). Yapay sinir ağları biyolojik olarak canlıda bulunan sinir sisteminin benzerinin taklit edilmesi ve bu kavramdan yola çıkarak matematiksel bir modellemedir (Yurtoğlu, 2005). Bayes teoremi, matematiksel istatistikte yer alan önemli bir teorem olarak bulunmaktadır. Herhangi bir problemin temasını oluşturmak için evrensel gözlemleri tespit ederek sonuçlandırmayı amaçlamaktadır (Çelebi, 2019).

Eğitsel Veri Madenciliği (EVM)

Eğitim ve öğretim ortamlarından paylaşılan verilerin elde edilmesi için belirli yöntemler geliştirilmesi dahilinde ilgili yöntemler öğrencilerin öğrendikleri veri ve bilgi kaynaklarının verimli bir şekilde anlamlandırılmasında kullanılan kavram olarak tanımlanmaktadır (Siemens & Baker, 2012). Bunun yanında EVM'nin öğretici uygulamalarda elde edilen işlenmemiş verinin eğitim programlarına, yansıması bu sayede, eğiticilerin ve araştırmacıların kolay bir şekilde kullanabileceği veri kaynaklarına dönüştürme olarak da tanımı bulunmaktadır (García, Romero, Ventura, & Castro, 2011). Bu sürece ilişkin bilgi Şekil 3'te görülmektedir.



Şekil 3. Veri Kaynaklarını Eğitsel Olarak Dönüştürme (Cihan, 2018)

Eğitsel veri madenciliğinin gün geçtikçe kullanımının yaygınlaşmasının başlıca sebeplerinden bir tanesi öğrenci sayılarındaki artış oranları bununla birlikte eğitmen sayısının ise az olmasından kaynaklanmıştır. Öğrencilere ayrılan zamanın artmasını sağlamak aldıkları eğitimin verimliliğini arttırabilmek için veri madenciliği eğitim alanında yüksek oranda kullanılmaktadır.

Uzaktan Eğitim

Uzaktan eğitimin ortaya çıkışı 300 yıl öncesine kadar uzanmaktadır. Öğrenen, öğreten ve içerik arasında sınırları kaldıran ve mevcut teknolojileri kullanan disiplinler arası bir alandır (Bozkurt, 2017). Öğrencinin kendi kendine çalışma formunun sistematik planlanması yapılmaktadır (Akyürek, 2020). Uzaktan eğitimde öğrenci ve öğretmen eş zamanlı ya da eş zamansız olarak iletişim kurmaktadır (Dinçer, 2016). Uzaktan eğitimin dünyadaki ilk örneği mektup yoluyla gerçekleştirilmiştir. Sonrasında içinde bulunulan dönemin teknolojisi uzaktan eğitim faaliyetinin değişmesinde etken olmuştur. Bu sebeple uzaktan eğitimin gelişim evreleri birbirini tamamlayan bir yapı içerisindedir. Uzaktan eğitimde kurulan iletişim ortamlarını Moore ve Kearsley (2005) şu şekilde belirtmektedirler:

1. Mektupla eğitim
2. Radyo ve televizyon ile eğitim
3. Açık üniversiteler ile eğitim
4. Telekonferans ile eğitim
5. İnternet ile eğitim

Uzaktan eğitimin tarihsel gelişiminde geleneksel eğitim sisteminin yetersizliği nedeniyle genelde yetişkinlerin eğitim almasını sağlamak amaçlı hayatımızda yerini aldığı görülmektedir. Uzaktan eğitimin en önemli amacı,

belirli bir öğrenen kitlesinin gerek duydukları eğitimi istenilen yerden ve istenilen zamanda almalarını sağlamaktır (Dinçer, 2016). Bu bağlamda öğrenme ihtiyacının giderilmesi için belirli fiziksel mekâna ihtiyaç duyulmamakta, bireylerin eğitimlerine devam etmesine olanak sağlamaktadır. Uzaktan eğitim sistemiyle bireyler arasında fırsat eşitliği sağlanmaktadır. Öğrenenler için eğitimi kolaylaştırarak kendi öğrenme hızına göre eğitim almayı mümkün hale getirmektedir.

Uzaktan eğitimin Türkiye'de tartışma konusu olması 1927 yılında başlamış ancak 1960 yılında mektupla öğretim faaliyete geçirilmiştir. Ancak uzaktan eğitim küresel anlamda önceden yüz yüze eğitimin alternatifi olarak bulunurken yaşanan covid-19 pandemi salgını nedeniyle eğitim ihtiyacını gidermek amaçlı yüz yüze eğitim ile aynı kategoride yer almaktadır.

Öğrenme Çıktılarının Veri Madenciliği ve Uzaktan Eğitim Bağlamı

Uzaktan eğitimde öğrenciler için hazırlanan materyaller ilk olarak davranışçı yaklaşım kapsamında hazırlanmış ve öğrencilerin materyalleri incelemeleri sonucunda başarılı olmaları planlanmaktadır (Yılmaz, 2017). Ancak günümüzde eğitimde yapılandırmacı yaklaşım kullanımı uzaktan eğitimde sunulan bilginin sosyal öğrenmeye doğru yönelmesini sağlamaktadır (Zhang ve diğerleri, 2015). Nitekim uzaktan eğitimde forum, blog gibi etkileşimli ortamların kullanılması öğrenen, öğreten ve içerik arasında iletişimi olumlu etkilemektedir.

Uzaktan eğitimde öğrenme çıktısı olarak beklenen başarının elde edilmesinde öğrenci motivasyonu, memnuniyeti ve algısı dikkate alınmalıdır (Kumtepe ve diğerleri, 2019). Öğrenme çıktıları öğrenci için önerilen faydaları sunmaktadır (Maher, 2004). Nitekim öğrenme çıktılarının başarı üzerinde etkisi bulunmaktadır. Ancak uzaktan eğitimde öğrenme çıktılarının ölçülmesi çok mümkün olmamakla birlikte sadece belirli değerlendirmeler ile sonuç alınabilmektedir (Erfidan, 2019).

Çevrimiçi kurslarda öğrenci ile içerik etkileşimi başarılı bir öğrenme çıktısına ve kursun tamamlanması üzerinde katkı sağlamaktadır. Alanyazında araştırmacılar çevrimiçi öğrenme çıktılarını başarı açısından, öğrenci memnuniyeti ve öz yönelim düzeyi açısından ölçmüşlerdir (Zimmerman, 2012). Mullen ve Tallent Runnels (2006), çalışmalarında geleneksel ve çevrimiçi sınıflar arasında daha iyi öğrenme çıktısının hangisi olduğunu incelerken öğrenci motivasyonu, öz düzenleme ve eğitmen desteği değişkenleri bağlamında karşılaştırmışlardır. Ayrıca öğrenme çıktıları belirlenirken öğrenci, öğretmen ve içerik arasındaki etkileşim temel inceleme alanı olmaktadır.

Hämäläinen ve Vinni (2011), öğrenci notları ve öğrenme çıktıları ile veri madenciliği çalışması gerçekleştirerek bir derste geçme, kalma, terk etme ve öğrenci puanını tahmin etmeyi hedeflemiştir. Bu bağlamda eğitim ve öğretimin bir sonucu olarak bireylerde meydana gelen değişiklikleri tanımlamak amacıyla öğrenme çıktıları kullanılmıştır. Aslında öğrenme çıktısı, bilginin öğrenci tarafından nasıl bir süreçten geçirildiğine bağlıdır (Demirel, 1993). Maher (2004) öğrenme çıktıları öğrenci başarısına odaklanmayı sağlayacak bir araç sunarken, sunulan eğitimin değerinin ölçüsünü göstermektedir. Öğrenme deneyimi ya da bir kursun sonunda öğrenenin ne anladığının incelenebilir ve ispatlanabilir ifadeler kümesini belirtmektir (Yeung & Ong, 2012; Akt. Yurdugül & Menzi Çetin, 2015).

Trigwell ve Prosser'a (1991) göre öğrenci öğrenimine yönelik çalışmalarda öğrenme çıktılarındaki farklılıklara yoğunlaşılması gerekmektedir. Yurdugül ve Menzi Çetin'e (2015) göre çevrimiçi öğrenme ortamlarında öğrenme çıktılarının etkileyen faktörlerin araştırması önerilmektedir. Alanyazında uzaktan eğitimin öğrenme çıktıları üzerine çalışmalar var olmaktadır. İlgili çalışmaların veri madenciliği yöntemi kullanılarak ulaşılan sonuçlarının

sistematik olarak incelenmesi gelecekteki çalışmalar açısında önemlidir. Bu çalışmada incelenen öğrenci öğrenme çıktıları akademik başarı, motivasyon, öz düzenleme gibi değişkenler için yapılmıştır.

Araştırmanın Amacı ve Araştırma Soruları

Eğitim alanında veri madenciliği çalışmalarının gerçekleştirilmesi gelecekteki eğitim ortamlarının tasarımında etki yaratabilecektir (Özbay, 2015). Öğrenci verilerinden öğrenme çıktılarının veri madenciliği ile tespit edilmesi daha etkili ortamların oluşturulmasına yardımcı olacaktır. Veri madenciliğinin eğitim ortamında gerçekleştirilen çalışmaları geleneksel sınıf ve uzaktan eğitim ortamlarında gerçekleştirilmektedir. Ancak geleneksel sınıf ortamında öğrenme çıktılarını görmek uzaktan eğitim ortamından daha zor olduğu için veri madenciliği çalışmaları daha az kullanılmaktadır. Günümüzde uzaktan eğitimde öğrencilerin öğrenme ortamıyla etkileşimlerinin ve öğrenci hareketliliğinin anlamlandırılması amacıyla veri madenciliği kullanılmaktadır. Bu araştırmada da uzaktan eğitimde veri madenciliği kullanılarak ulaşılan sonuçlardan öğrencilerin öğrenme çıktısına etkisinin ilgili araştırmalardaki eğilimler sonucunda belirlenmesi amaçlanmıştır. Çalışma amacı doğrultusunda uzaktan eğitimin öğrencilerin öğrenme çıktısına etkisinin veri madenciliği ile incelenen çalışmaların sistematik incelemesi bu çalışmada yer almaktadır. Yurdugül ve Menzi Çetin'e (2015) göre yükseköğretim içerisinde e-öğrenme ortamlarının çalışmasının öğrenme çıktılarındaki etkisinin araştırılması gerekliliği bulunmaktadır. Bu kapsamda bu çalışma literatürdeki çalışmaların analizini sunmayı ve bu yönüyle araştırma uzaktan eğitimin öğrenme çıktılarına etkisinin veri madenciliği ile sonucunu görebilmelerini sağlayacaktır. Ayrıca sistematik inceleme sonucunda araştırma alanında ihtiyaç duyulan çalışmaların belirlenmesi, araştırmacılara yol gösterici nitelikte olacağı düşünülmektedir.

Bu araştırma kapsamında aşağıdaki araştırma sorularına yanıt aranmıştır.

İncelenen bilimsel çalışmalarda;

1. Çalışmaların yıllara göre,
2. Yoğun olarak kullanılan anahtar kelimelere göre,
3. Kullanılan yönteme göre,
4. Veri toplama araçlarına göre,
5. Katılımcı profiline göre,
6. Çalışmanın gerçekleştirildiği ülkelere göre,
7. Öğrenme alanlarına göre,
8. Kullanılan teknolojilere göre,
9. Kullanılan veri madenciliği sınıflandırma yöntemine göre dağılımları nasıldır?
10. Veri madenciliği yönteminin kullanıldığı bilimsel çalışmalarda hangi öğrenme çıktıları incelenmiştir?
11. Öğrenme çıktıları ile ilgili sonuçlar nelerdir?

Yöntem

Araştırmanın Deseni

Bu araştırmada alanyazın incelemesine dayalı olarak sistematik inceleme deseni kullanılmıştır. Sistematik incelemeler bilimsel bilgi sunması ve güçlü kanıtlar ortaya çıkarmaları sebebiyle önemli çalışmalardır (Karaçam, 2013). Bu desende benzer çalışmaların kapsamlı sentezi sunulmaktadır. Genellikle planlanan belirli bir araştırma

sorusunu cevaplamak için ilgili literatürün önceden planlanan ölçütler kapsamında analiz edilmesi ile gerçekleştirilir (Yılmaz, 2021). Sistematik bir literatür taraması ile araştırma konusuna dahil mevcut araştırmalar değerlendirilip yorumlanmaktadır (Kitchenham, 2004). Sistematik inceleme araştırmalarında incelenecek çalışmaları belirlemek için dahil etme ve dışlama ölçütleri kullanılarak incelenme kapsamı oluşturulmaktadır (Karaçam, 2013).

Newman ve Gough'a (2020) göre sistematik incelemenin aşamaları şu şekilde bulunmaktadır:

- İlk olarak araştırma sorusunun geliştirilmelidir,
- İkinci olarak kavramsal çerçeve planlanmalıdır,
- Üçüncü olarak seçim kriterleri düzenlenmelidir,
- Dördüncü olarak arama stratejisinin düzenlenmelidir,
- Beşinci olarak seçim kriterleriyle çalışmaların seçimi yapılmalıdır,
- Altıncı olarak belirli kodlama çalışması yapılmalıdır,
- Yedinci olarak çalışmaların incelenmesiyle kalitesi değerlendirilmelidir,
- Sekizinci olarak araştırma sorusuna cevaben çalışmaların sonuçları incelenmelidir,
- Son olarak bulgular raporlanmalıdır.

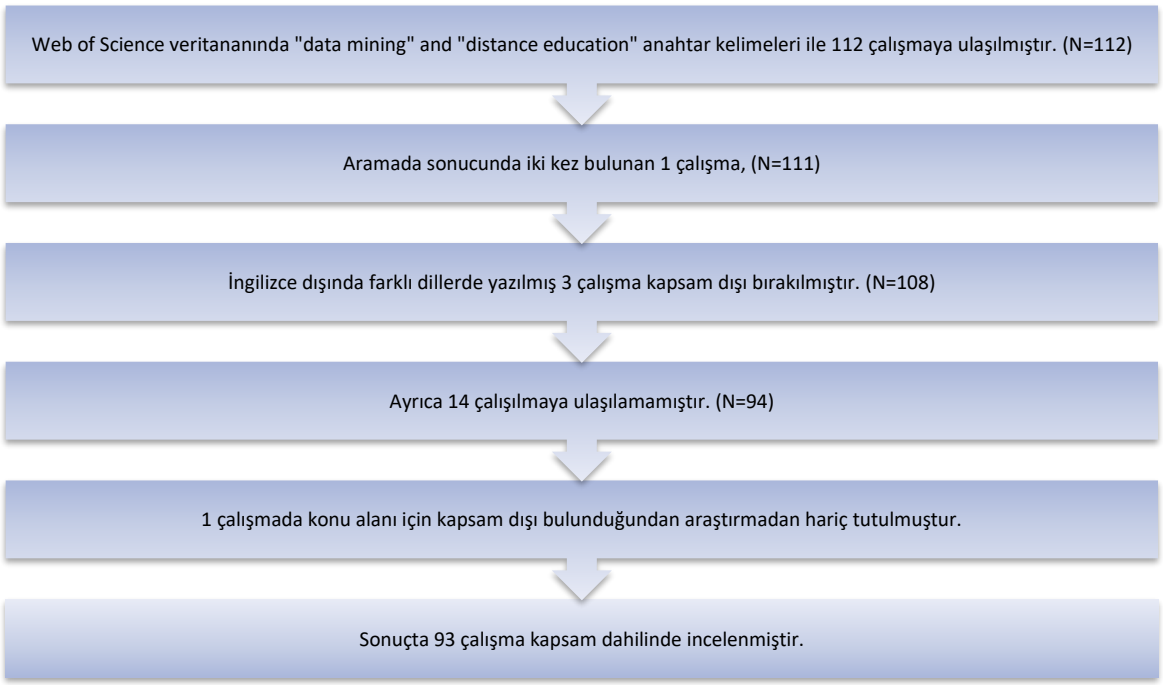
Çalışma Grubu

Bu araştırmanın çalışma grubunu, ("data mining" AND "distance education") kavramları bağlamında ulaşılan ve veri madenciliği yöntemi kullanılarak uzaktan eğitimin öğrenciler üzerinde öğrenme çıktısının etkisinin belirlemek amaçlı ulaşılan 93 bilimsel çalışma oluşturmaktadır**.** İncelemeye alınan çalışmaların türleri hakkında herhangi bir kısıtlama yapılmamıştır. Bu nedenle incelemeye alınan çalışmalar "article, proceeding paper, book chapters, review article, book review" türlerini barındırmaktadır.

Verilerin Toplanması

Araştırmada incelenip değerlendirilen bilimsel çalışmalar; çok sayıda farklı akademik ve bilimsel çalışma için atıf yapılan tüm referansları indeksleyen hem güvenilir keşif hem de güvenilir değerlendirmeyi desteklemek için kapsamlı ve eksiksiz alıntı yapılmasına olanak sağlayan kullanıcı abonelik tanımlı web sitesi Web of Science'da yapılmıştır.

Araştırma kapsamına dahil edilecek çalışmaların kriterleri şunlardır: Web of Science'da, herhangi bir yıl sınırlaması olmaksızın Nisan 2022 yılına kadar yayınlanmış, sadece İngilizce dilinde bulunan, anahtar kelimeleri arasında "data mining" AND "distance education" var olduğu çalışmalardan oluşmaktadır. Araştırma kapsamına dahil etme ve hariç tutma ölçütlerine göre incelenen bilimsel çalışmaların seçimi Şekil 4'te görülmektedir.



Şekil 4. Araştırma Kapsamında Dahil Etme ve Hariç Tutma

Belirlenen kriterler sonucunda 112 (N=112) bilimsel çalışma listelenmiştir. Listelenen 112 çalışma için istenilen ölçütler dahilinde yapılan inceleme sonrasında; bir çalışma aynı olduğu için (N=111), 3 çalışma İngilizce dışında farklı bir dil (N=108) olduğu için araştırma kapsamından çıkarılmıştır. Toplamda 108 bilimsel çalışma ile detaylı incelemeye alınmıştır. İncelenen çalışmalardan 14 çalışmaya ulaşılamadığı için ve 1 çalışma kapsam dışı olduğu için araştırma kapsamından hariç tutulmuştur. Sonuçta 93 çalışmanın belirlenen kriterler çerçevesinde analizi gerçekleştirilmiştir.

Veri Analizi

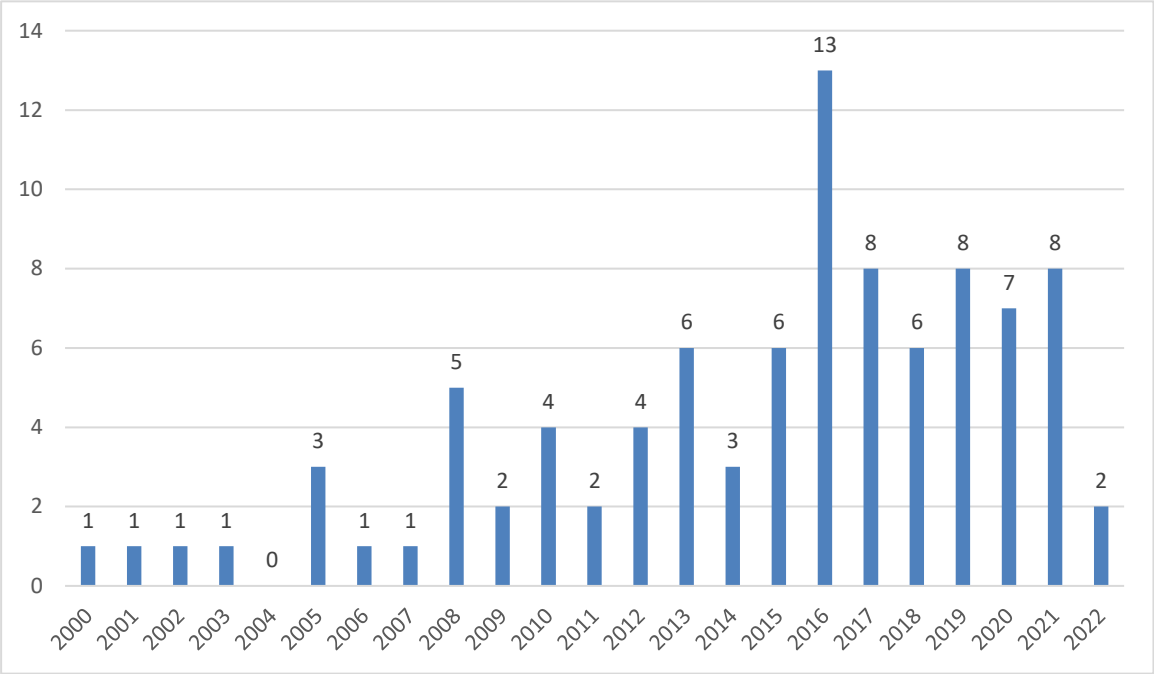
Ulaşılan ve bu araştırma kapsamına dahil edilen bilimsel çalışmalar araştırma sorularına yanıt aranacak şekilde incelenmiştir. Araştırmada; çalışmanın yılı, anahtar kelime, yöntemi, veri toplama araçları, katılımcı profili, çalışmanın gerçekleştirildiği ülke, öğrenme alanları, kullanılan teknolojiler, kullanılan veri madenciliği sınıflandırma yöntemi, çalışmalardaki öğrenme çıktıları ve öğrenme çıktıları ile ilgili sonuçlar ölçüt olarak belirlenmiştir. Bu ölçütlerden alınan veriler Microsoft Excel formuna işlenmiştir. Tüm çalışmaların incelemesi tamamlandıktan sonra veriler analiz edilmiştir.

Bulgular

Bu bölümde araştırma sorularına yönelik olarak araştırma kapsamında incelenen 93 çalışmaya ait veriler sunulmuştur.

1. Çalışmaların Yıllara Göre Dağılımı

Araştırma kapsamında incelenen çalışmalar ilk olarak çalışmanın gerçekleştirildiği yıl bakımından incelenmiştir. İncelenen çalışmaların yıllara göre dağılımlarına ilişkin veriler Şekil 5'te verilmiştir.



Şekil 5. Çalışmaların Yıllara Göre Dağılımı

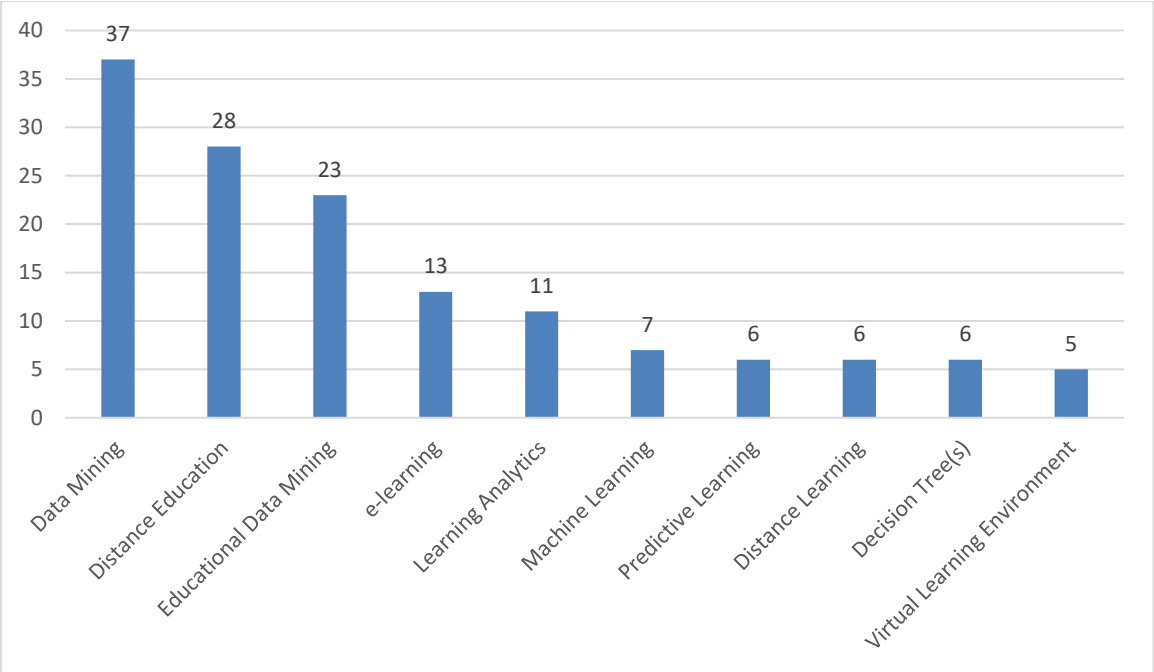
Şekil 5'e göre

- Yıllara baktığımızda en fazla 2016 yılında 13 tane bilimsel çalışma olduğu görülmektedir.
- Bunu 8 bilimsel çalışma ile 2017-2019-2021 yılları takip etmektedir.
- En az 1 bilimsel çalışma ile 2000-2007 yılları arasında olduğu görülmektedir.

Bilimsel çalışmaların sayılarına bakıldığında günümüze doğru uzaktan eğitimde veri madenciliği ilgili yapılan çalışmalarda yıllara göre dalgalanmalar görülmektedir.

2. Yoğun Olarak Kullanılan Anahtar Kelimelere Göre Dağılım

Araştırma kapsamında incelenen çalışmalar ikinci olarak anahtar kelimeleri bağlamında incelenmiştir. İncelenen çalışmalarda yoğun olarak kullanılan (N>=5) anahtar kelimelere göre dağılıma ilişkin veriler Şekil 6'da verilmiştir.

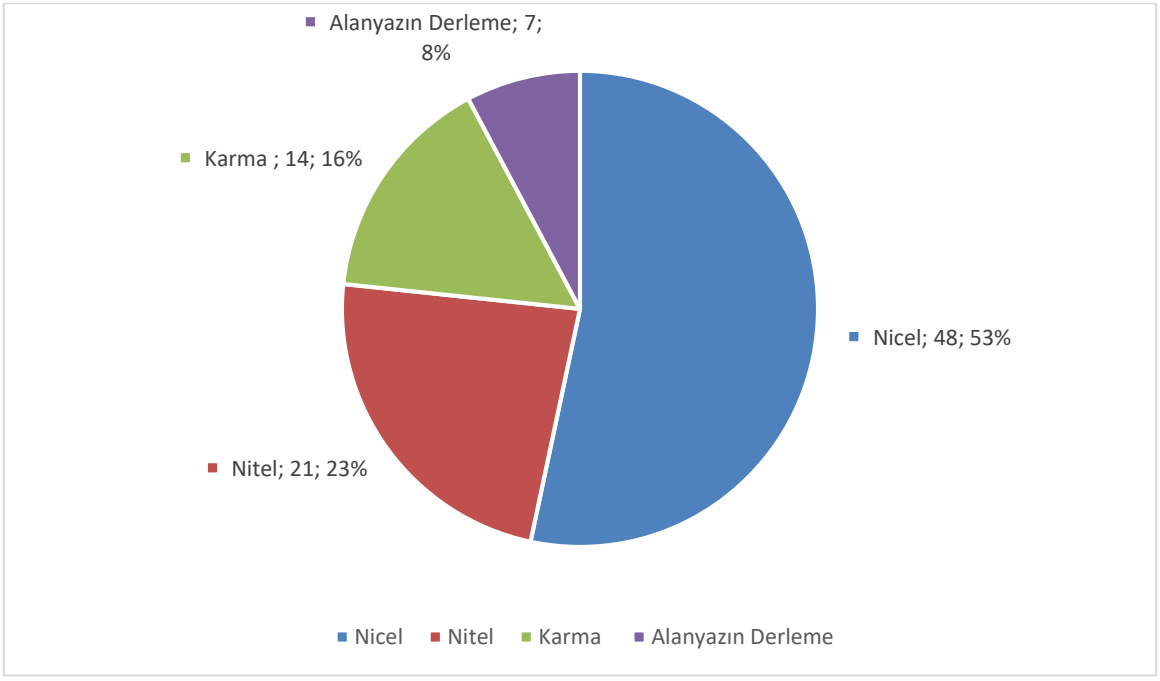


Şekil 6. Yoğun Olarak Kullanılan Anahtar Kelimelere Göre Dağılım

Şekil 6'da görüldüğü üzere çalışmalarda anahtar kelime olarak en fazla "data mining" kelimesinin kullanıldığı, ardından "distance education" (N=28), "educational data mining" (N=23), e-learning (N=13), "learning analytics" (N=11) tercih edilmiştir.

3. Çalışmalarda Kullanılan Yönteme Göre Dağılım

Araştırma kapsamında incelenen çalışmalar üçüncü olarak çalışma yöntemi bağlamında incelenmiştir. İncelenen çalışmaların yöntemlerine göre dağılımlarına ilişkin veriler Şekil 7'de verilmiştir.

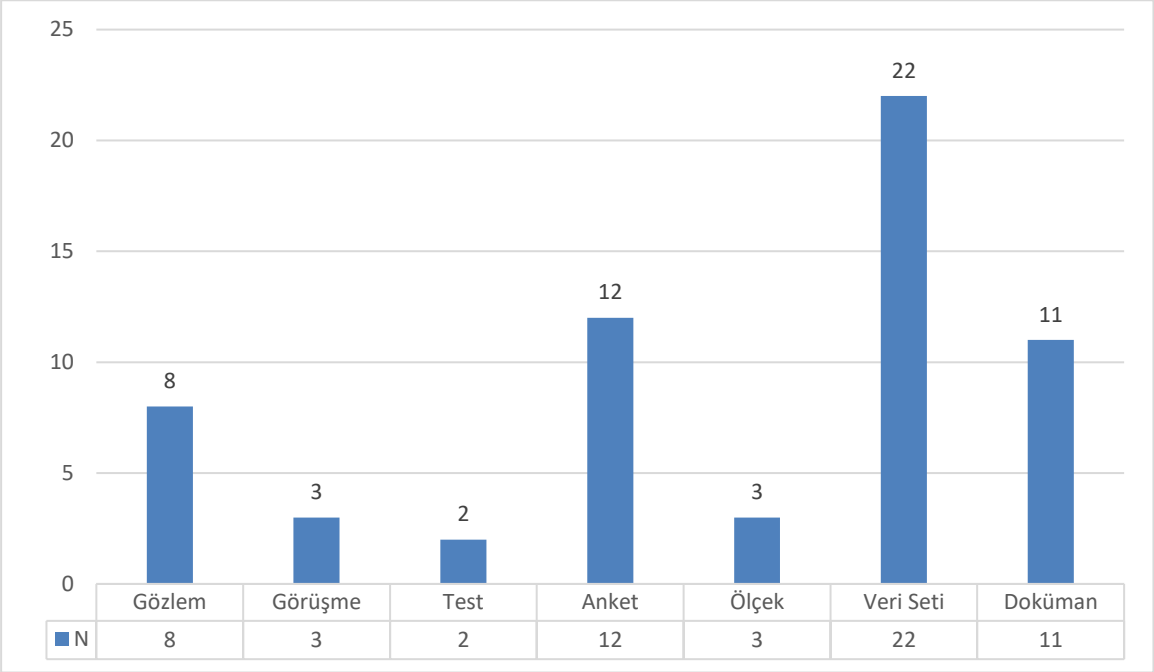


Şekil 7. Çalışmaların Yöntemlerine Göre Dağılımı

Şekil 7'ye göre incelenen çalışmalarda en fazla %53 oranıyla nicel araştırma yöntemi kullanıldığı görülmektedir. Nitel araştırma yöntemi %23, karma araştırma yöntemi %16 ve alanyazın derleme yöntemi %8 oranında tercih edilmiştir. Bu durumda incelenen çalışmaların yarısının nicel yöntemi tercih etmiştir.

4. Çalışmalarda Kullanılan Veri Toplama Araçlarına Göre Dağılım

Araştırma kapsamında incelenen çalışmalar dördüncü olarak kullanılan veri toplama araçları bağlamında incelenmiştir. Çalışmalarda kullanılan veri toplama araçlarına ilişkin veriler Şekil 8'de verilmiştir.

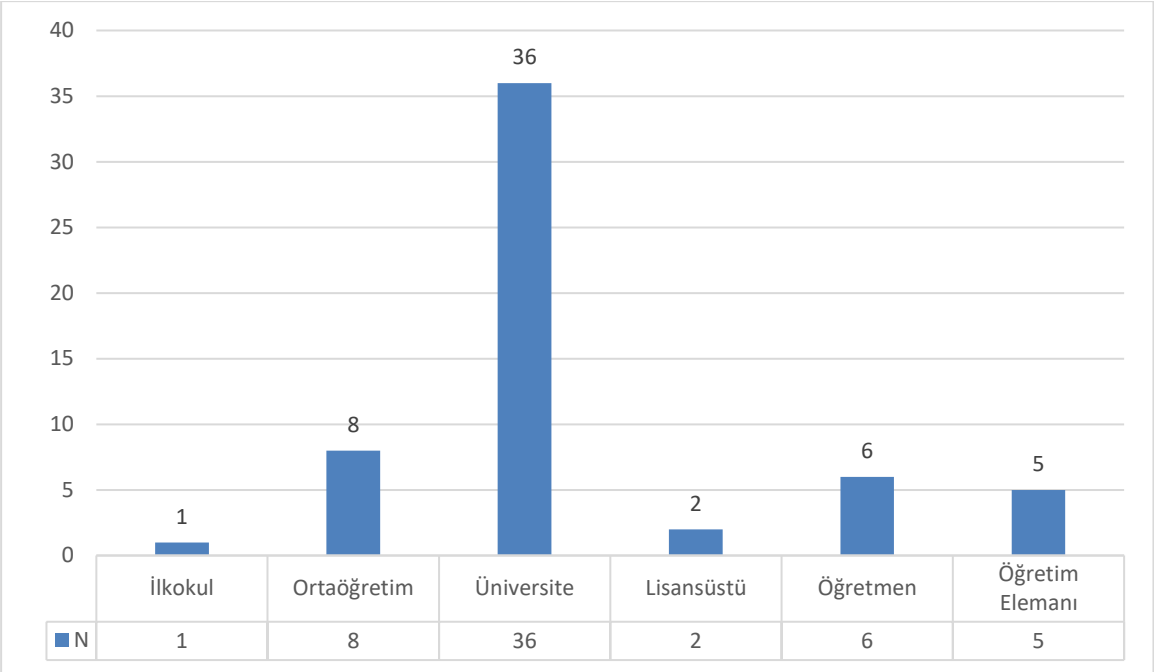


Şekil 8. Kullanılan Veri Toplama Araçlarına Göre Dağılım

İncelenen çalışmalarda veri toplama aracı olarak en fazla hazır veri seti (N=22) kullanılmıştır. Ardından anket (N=12), doküman (N=11) ve gözlem (N=8) kullanılmıştır. Çalışmalarda ölçek (N=3), görüşme (N=3) ve test (N=3) diğer veri toplama araçlarına göre daha az tercih edilmiştir.

5. Çalışmalardaki Katılımcı Profiline Göre Dağılım

Araştırma kapsamında incelenen çalışmalar beşinci olarak çalışmalardaki katılımcı profiline göre incelenmiştir. İncelenen çalışmalardaki katılımcı profiline ilişkin veriler Şekil 9'da verilmiştir.



Şekil 9. Katılımcı Profiline Göre Dağılım

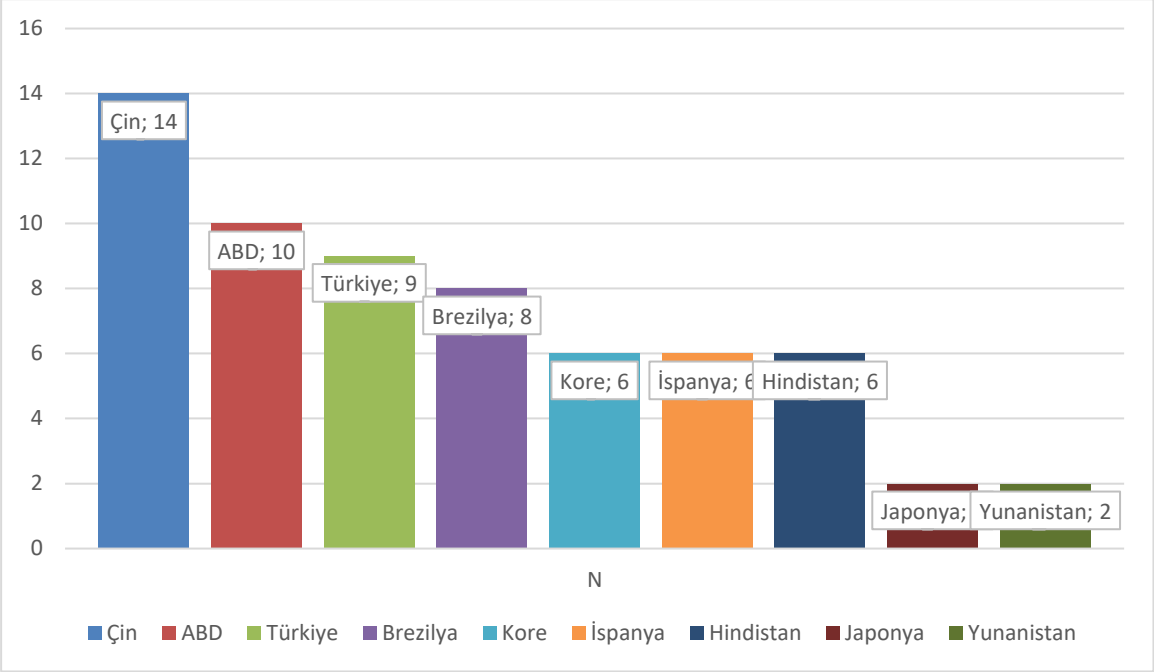
Şekil 9 incelendiğinde uzaktan eğitimde öğrenci profilini çoğunlukla üniversite öğrencilerinin (N=36) oluşturduğu görülmektedir. Ardından ortaöğretim (N=8), öğretmen (N=6), öğretim elemanı (N=5), lisansüstü (N=2) ve ilkokul (N=1) öğrencileri katılımcı olarak bulunmaktadır.

6. Çalışmaların Gerçekleştirildiği Ülkelere Göre Dağılım

Araştırma kapsamında incelenen çalışmalar altıncı olarak çalışmaların gerçekleştirildiği ülke bağlamında incelenmiştir. Çalışma yapılan ülkelerin isimleri Şekil 10'da verilmiştir.

Şekil 10. Çalışma Yapılan Ülkeler

Şekil 10'da verilen ülke isimlerinden aynı renkli olan çalışmalar eşit sayıdadır. Böylece Finlandiya, Litvanya, Belçika, Tayvan, Suudi Arabistan, İsviçre ve Cezayir ülkelerinde aynı sayıda (N=1) çalışma bulunmaktadır. Buradan hareketle siyah renkli ülkelerin en az çalışma sayısına sahip olduğu söylenebilmektedir. İncelenen çalışmaların yoğun olarak (N>=2) gerçekleştirildiği ülkelere ilişkin frekans verileri Şekil 11'de verilmiştir.

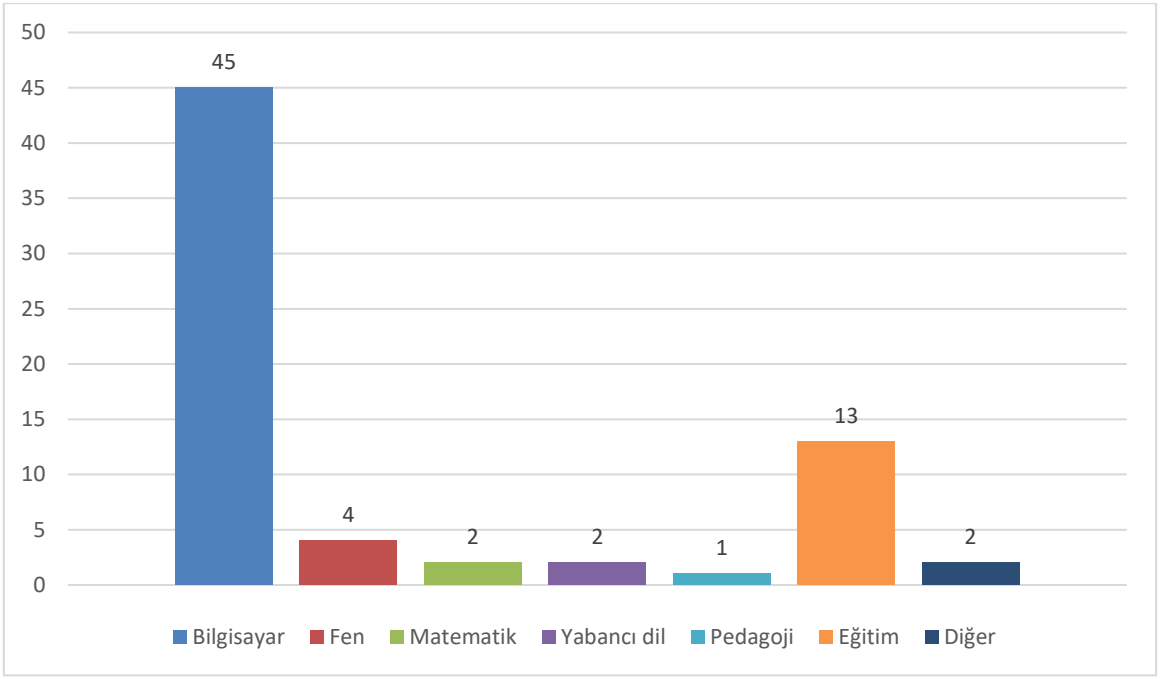


Şekil 11. Ülkelere Göre Dağılım

Şekil 11'de ülkelere göre dağılım incelendiğinde araştırma konusuna yönelik en fazla çalışmanın Çin'de (N=14) yapıldığı görülmektedir. İkinci sırada ABD (N=10), üçüncü sırada Türkiye (N=9), dördüncü sırada Brezilya (N=8), beşinci sırada 6'şar çalışma Kore, İspanya ve Hindistan yer almaktadır.

7. Çalışmalardaki Öğrenme Alanlarına Göre Dağılım

Araştırma kapsamında incelenen çalışmalar yedinci olarak çalışmalardaki öğrenme alanları bağlamında incelenmiştir. İncelenen çalışmalardaki öğrenme alanlarına ilişkin veriler Şekil 12'de verilmiştir.

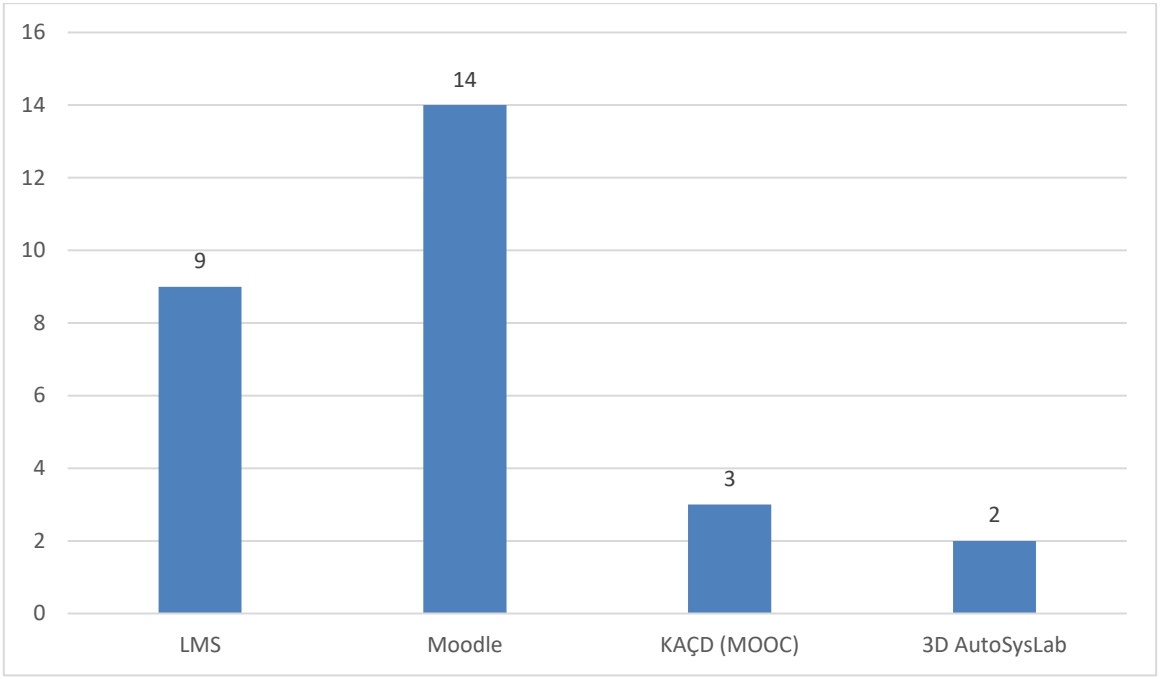


Şekil 12. Öğrenme Alanlarına Göre Dağılım

Şekil 12 incelendiğinde bilgisayar alanında 45 çalışmanın bulunması en fazla çalışma yapılan alan olmasını sağlamaktadır. Diğer alanlarda düşük seviyede çalışmalar gerçekleştirilmiştir. Ayrıca 13 çalışmanın eğitim alanında yapıldığı ancak öğrenme alanının belirsiz olduğu tespit edilmiştir.

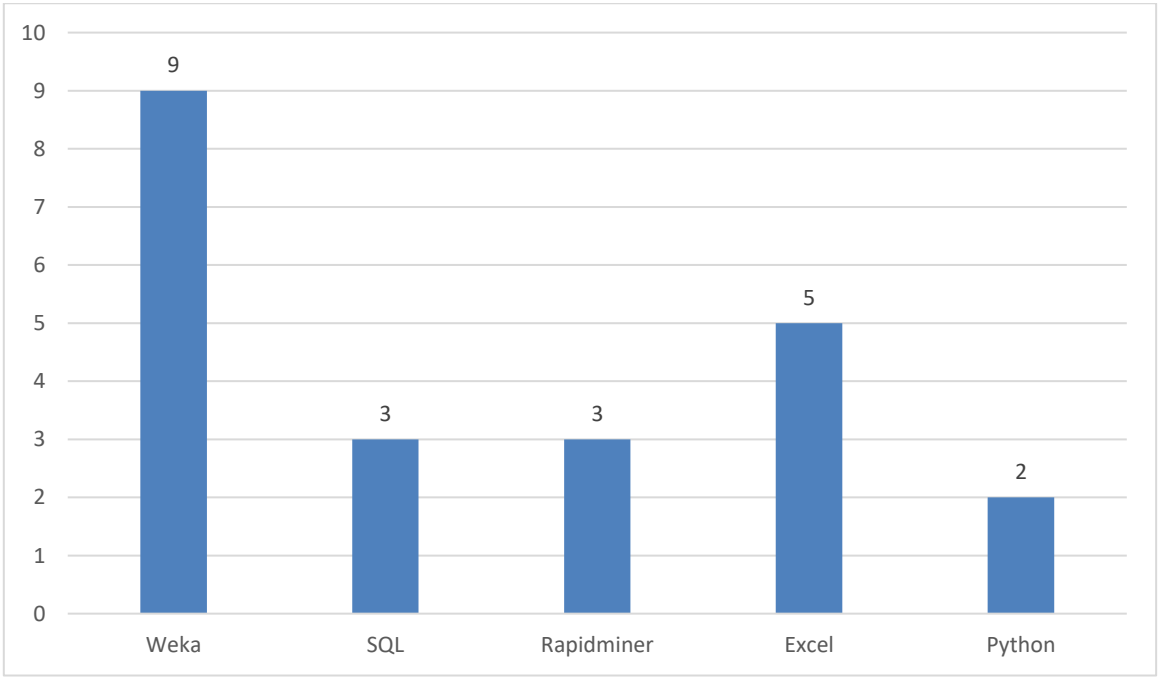
8. Çalışmalarda Çoğunlukla Kullanılan Teknolojilere Göre Dağılım

Araştırma kapsamında incelenen çalışmalar sekizinci olarak çalışmalarda çoğunlukla kullanılan teknolojiler bağlamında incelenmiştir. İncelenen çalışmalarda verilerin çoğunlukla (N>=2) elde edildiği teknolojik ortamlara ilişkin veriler Şekil 13'te verilmiştir.



Şekil 10. Verilerin Elde Edildiği Teknolojik Ortamlar

Şekil 13'e göre incelenen çalışmalarda verilerin elde edildiği ortam olarak en çok öğrenme yönetim sistemi Moodle (N=14) tercih edilmiştir. Dokuz çalışmada kullanılan LMS belirtilmemiştir. Bunun yanında öğrenme ortamı olarak MOOC üç çalışmada ve 3D AutoSyslab iki çalışmada kullanılmıştır. Toplanan verilerin ilgili ortamlardan elde edildikten sonra verilerin çoğunlukla (N>=2) analiz edildiği ortamlara dair veriler Şekil 14'te verilmiştir.

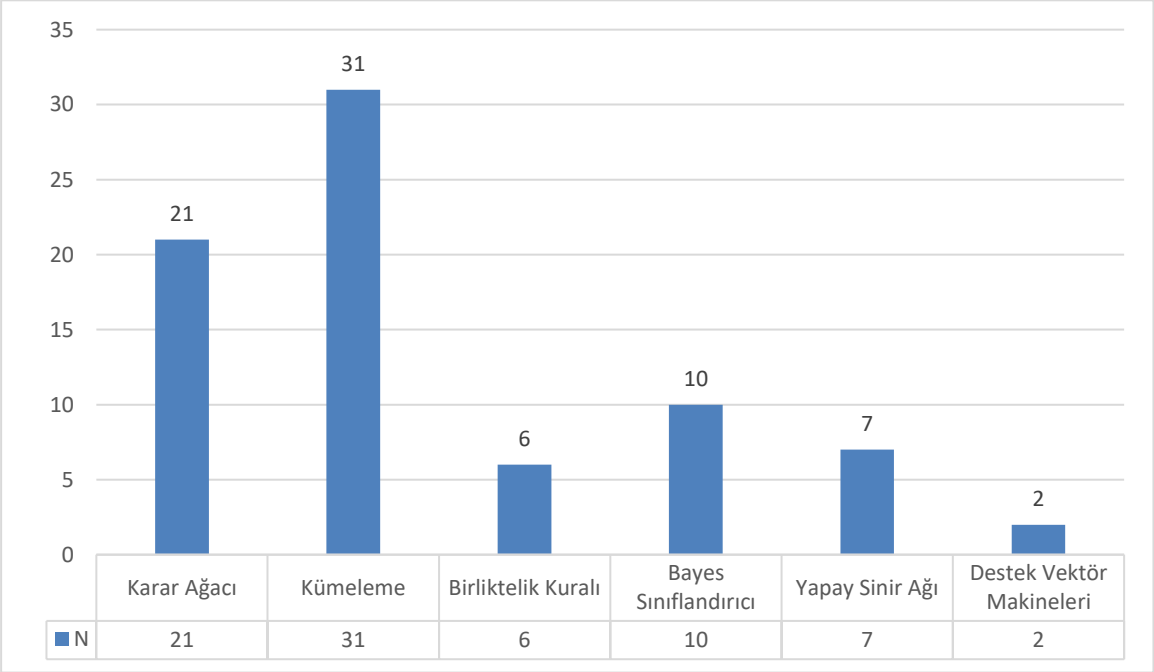


Şekil 14. Verilerin Analiz Edildiği Ortamlar

Şekil 14 incelendiğinde elde edilen verilerin analizi için en çok veri madenciliği yazılım aracı olarak Weka (N=9) daha fazla tercih edilmiştir. Ayrıca incelenen çalışmalar arasında alanyazın derlemeler olduğu için Excel (N=5) kullanılmıştır. Bunun yanında verileri analiz etmek için SQL ve Rapidminer üçer çalışmada, Python iki çalışmada kullanılmıştır.

9. Çalışmalarda Kullanılan Veri Madenciliği Sınıflandırma Yöntemlerine Göre Dağılım

Araştırma kapsamında incelenen çalışmalar dokuzuncu olarak kullanılan veri madenciliği sınıflandırma yöntemleri bağlamında incelenmiştir. İncelenen çalışmalarda kullanılan veri madenciliği sınıflandırma yöntemlerine ilişkin veriler Şekil 15'te verilmiştir.

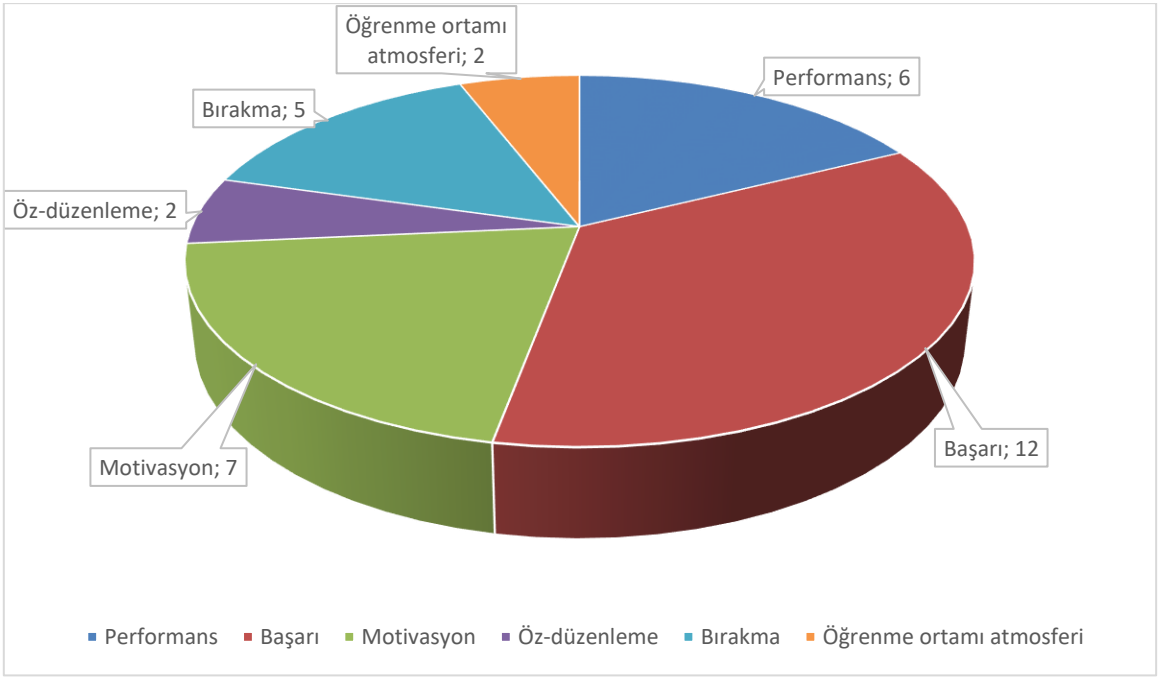


Şekil 15. Veri Madenciliği Sınıflandırma Yöntemlerine Göre Dağılım

Şekil 15'e göre en çok kümeleme (N=31) yönteminin kullanıldığı görülmektedir. İkinci sırada ise karar ağacının (N=21) yüksek sayıda kullanıldığı tespit edilmiştir. Diğer yöntemlerden bayes sınıflandırıcı 10 çalışmada, yapay sinir ağı 7 çalışmada, birliktelik kuralı 6 çalışmada ve destek vektör makinelerinin 2 çalışmada kullanıldığı tespit edilmiştir.

10. Veri Madenciliği Yönteminin Kullanıldığı Çalışmalardaki Öğrenme Çıktıları

Araştırma kapsamında incelenen çalışmalar onuncu olarak çalışmalar öğrenme çıktıları bağlamında incelenmiştir. İncelenen çalışmalarda kullanılan öğrenme çıktılarına ilişkin veriler Şekil 16'da verilmiştir.



Şekil 16. Veri Madenciliği Yönteminin Kullanıldığı Çalışmalardaki Öğrenme Çıktılarına Göre Dağılım

Şekil 16 incelendiğinde öğrenme çıktısı olarak en fazla başarının (N=12) ele alındığı tespit edilmiştir. Ardından öğrenme çıktısı olarak ele alınan diğer başlıklar motivasyon (N=7), performans (N=6), bırakma (N=5), öz-düzenleme (N=2) ve öğrenme ortamı atmosferi (N=2) olarak bulunmuştur.

11. İncelenen Çalışmalardaki Öğrenme Çıktıları ile İlgili Sonuçlar

Veri madenciliği yönteminin kullanıldığı çalışmalardaki öğrenme çıktıları ile ilgili sonuçlar alt başlıklar bağlamında verilmiştir.

11.1. Başarı ile İlgili Sonuçlar

Başarı ile ilgili sonuçlar incelendiğinde;

- Uzaktan eğitimde öğrenciler canlı derslere katıldığında akademik başarıda artış gözlenmektedir. Bu sayede elde edilen sonuçlar öğrencilerin derse katılımının ve çevrimiçi sınavlara girmenin onların başarısını iyileştirdiğine dair ikna etmek için kullanılabilir (Al-Musharraf & Alkhattabi, 2016).
- Öğrencilerin uzaktan eğitimde başarı oranı yaşı ile ters orantıya sahiptir. Bu durum öğrencilerin yaşının arttıkça başarı puanının düştüğünü göstermektedir. Uzaktan eğitim ile örgün eğitim puanları karşılaştırıldığında örgün eğitimde puanların daha yüksek olduğu gözlemlenmektedir (Sen & Ucar, 2012).
- Ailelerin geliri arttıkça üniversiteye yerleştirme puan ortalamalarının ve genel not ortalamalarının arttığını göstermektedir. Bu doğrultuda gelir dağılımı düzenli olan öğrencilerin diğer öğrencilere göre daha başarılı olduğu gözlenmektedir (Akmeşe, Kör, & Erbay, 2021).
- Yapılan araştırmaların sonuçlarına göre teknoloji kullanımı ve bilgisayar kullanımında yeterli olmayan veya bu tür bir çevrimiçi eğitim platformuna adapte olamayan öğrencilerin puanları düşük olma eğilimindedir (Zang & Lin, 2003).
- Öğrenme davranışları başarı performansı için belirleyici olarak bakılırken öğrencinin kişilik özellikleri başarı performansını etkilediği göz önünde bulundurulmalıdır.

- Aydoğdu (2020), yaptığı sistematik inceleme sonucunda farklı örneklem düzeyleri kapsamında çalışmaların yapılmasını ayrıca öğrenci başarısı için öğrenme ile ilgili farklı değişkenlerinde ele alınarak araştırılmasını önermektedir.

11.2. Motivasyon İle İlgili Sonuçlar

Motivasyon ile ilgili sonuçlar incelendiğinde;

- Uzaktan eğitim içerisinde öğrenci etkinliklerinin öğretmen etkinliklerinden etkilendiği ortaya çıkmıştır. Bu durumda öğretmenler daha çok etkinlik çabası gösterdiğinde öğrenciler pasif duruma düşmektedir (Preidys & Sakalauskas, 2010).
- Değerlendirmeye yönelik sonuçlar yerine eğitimcilerin öğrencilerin ya da kullanıcıların sorgulamaya dayalı uygulayıcı projeler üzerinde çalışmasına fırsat vererek öğrencilerin zaman içerisinde tartışma formlarına katılanların kitlesel açık çevrimiçi derslerde daha fazla oranda başarılı olduklarını bu sebeple iç motivasyonlarını geliştirdiğini tavsiye etmektedir (Hampel & Pleines, 2013).

11.3. Performans ile İlgili Sonuçlar

Performans ile ilgili sonuçlar incelendiğinde;

- Öğrencilerin uzaktan eğitimde canlı sanal derslere katılım sağlamasıyla akademik performansı arasında olumlu yönde ilişki bulunmaktadır. Ayrıca öğrencilerin çevrimiçi sınavlara girme sıklığı ile akademik performansı arasında da olumlu bir ilişki bulunmaktadır. Bu durum öğrencilerin çevrimiçi sınav olma sıklığının artması ile başarısızlık oranının düştüğü sonucu meydana getirir (Al-Musharraf & Alkhattabi, 2016).
- Öğrenci başarı verilerinin karar ağacı ile analizi sonucunda farklı kökenli öğrencilerin performansları arasında da farklılık bulunmaktadır. Bu performans farklılıklarının nedeni görselleştirme grafiği kullanarak açıkça görülebilmektedir (Fok ve diğerleri, 2014).
- Dersi geçen öğrencilerin-kullanıcıların çoğunluğunun, hem nicelik (daha fazla mesaj ve kelime yazarak) hem de nitelik (ortalama puan mesajları, merkezilik ve prestij için daha yüksek değerler elde ederek) foruma en aktif olarak katılan öğrenciler olduğunu göstermektedir (Romero, López, Luna, & Ventura, 2013).
- Öğrencilerin uzaktan eğitim sistemi platformunda oturum açma sayısı fazla olması öğrencilerin bir o kadar zorlandıklarını ancak performanslarının bir o kadar iyi olduğu sonucuna ulaşılmıştır (Gao & Zhang, 2018).
- Yeni teknoloji yaklaşımlarının öğrencilerin performans değişimlerine yüksek oranda olumlu katkı sağladığı sonucuna ulaşılmaktadır (Cheng, Chu, & Shiue, 2015).

11.4. Bırakma ile İlgili Sonuçlar

Okulu bırakma ile ilgili sonuçlar incelendiğinde;

- Uzaktan eğitim alan öğrencilerin bırakma davranışı ile demografik değişkenleri arasındaki ilişki incelenmiştir. Öğrencilerin çalışan ve evli olma durumları onların okulu bırakma potansiyellerinin yüksek olduğunu göstermiştir. Ayrıca öğrencilerin bu demografik özellikleri bırakma riski altında oldukları sonucunu ortaya çıkarmıştır. Bu nedenle potansiyel risk altında bulunan öğrenciler uzaktan eğitim

kurslarını almaktan dışlanmamalı ya da vazgeçirilmemelidir. Bunun yerine risk grubundaki öğrenciler belirlenmeli ve bu süreçten öğrencilere etkin bir şekilde hizmet eden politikalar geliştirilmek, iyileştirmek için faydalanılmalıdır (Yasmin, 2013).

- Uzaktan eğitimde öğrencilerin okulu bırakma davranışını belirlemek için veri madenciliği ile öğrenme analitiklerinin kullanımı artmaktadır. Ancak öğrencilerin okulu bırakma davranışını azaltmak kalıcılığı artırmak için Active Metodolojileri ile yapılan çalışma sayısı az bulunmaktadır (Andrade, Rigo, & Barbosa, 2021).
- Andrade ve diğerleri (2021) gelecek araştırmalarda okulu terk etmeyi azaltma performansı artırmak, öğrencinin dersten başarısızlık ve dersten ayrılma risklerini azaltmak için aktif yöntemi kullanan bir tavsiye sisteminin geliştirilmesini önermektedirler.
- Uzaktan eğitimde bırakma davranışını engellemek için öğrenci gruplarının davranışının veri madenciliği analizinin yapılarak sonucun bilinmesi gelecekteki sınıf yöneticisine yardımcı olacaktır. Hatta öğrenci grubu bir sonraki sınıfa geçtiğinde önceki sınıfın davranışının sürüp sürmediğini değerlendirebilmek için haftalık olarak analiz edilmelidir (Bezerra & Silva, 2020).

11.5. Öz-düzenleme İle İlgili Sonuçlar

Öz-düzenleme ile ilgili sonuçlar incelendiğinde;

- Uzaktan eğitimde öğrenciler öz-düzenlemeli öğrenme ile bireyin kendisinin kabiliyetlerini tanıması ve kendi kendine öğrenebilmesini destekleme yolunda kullandığı işlem, taktik, teknik ve stratejiler olarak tanımlanabilir (Anaya, Luque & Peinado 2016).
- Öğrencinin kendine uygun amaçlarını belirlemesinde gelecekteki hedefleri için bilişsel olarak kendi kendini motive etmesini sağlama işidir. (Çiltaş, 2011). Bu nedenle yapılan araştırmalarda öz düzenleme ile öğretim sadece derslerde kullanımı için değil de hayat boyu kullanımının önemli olduğunu vurgulayan nitelikte olduğunu göstermektedir.

11.6. Öğrenme Ortamı Atmosferi İle İlgili Sonuçlar

Öğrenme ortamı atmosferi ile ilgili sonuçlar incelendiğinde;

- Öğrenen olumsuz bir durumdaysa, öğrenme ortamı geliştirilerek öğrenme verimliliği artırılabilir. Öğrenci olumlu bir durumdaysa, çevresindeki öğrencilerin olumlu öğrenme durumu onun mevcut durumunu korumasına yardımcı olabilir (Chen, Dai, Gao, Han, & Shan, 2019).
- Detaylı ve yüzeysel öğrenenler video izleme davranışları açısından karşılaştırıldığında, iki grup arasında yalnızca ileriye doğru arama sayısı açısından istatistiksel olarak anlamlı farklılıklar bulunduğunu göstermiştir. Çalışma yapılan bu iki grup öğrencinin ortalama durumu kıyaslandığında, bir uygulama ya da etkinlik yapıldığında yüzeysel öğrenenlerin derin öğrenenlere göre daha fazla ileriye baktığı anlaşılmıştır. İleriye dönük arayış sayıları ile yüzeysel yaklaşımlar ölçeği puanları arasında pozitif yönde ve anlamlı düzeyde bir ilişki olduğunu ortaya koyan korelasyon analizi de bu bulguyu desteklemektedir (Akcapinar & Bayazit, 2018).
- Öğrencilerin kurs etkileşimlerinin belirlenmesi sonucunda; eğer öğrencilerin sınavlar ve kaynaklar ile etkileşimi yüksek olursa ve yaş aralığı 25-29 arasında ve medeni durumu bekarsa sanal kurs etkileşim yüksek bulunmaktadır. Ayrıca öğrencinin kaynaklar ile etkileşimi ortalama ve yaş aralığı 25-29 arasında

kadınsa yine sanal kurs etkileşimi yüksektir. Ek olarak sınav etkileşimi ortalama, yaşı 29'dan büyük ve çalışmıyorsa yine kurs etkileşimi yüksek bulunmuştur (Viloria ve diğerleri, 2019).

Tartışma ve Sonuç

Uzaktan eğitimde veri madenciliği kullanılarak ulaşılan sonuçlardan öğrencilerin öğrenme çıktısına etkisinin ilgili araştırmalardaki eğilimler sonucunda belirlenmesini amaçlayan bu araştırmada. Uzaktan eğitimde veri madenciliği kullanılarak ulaşılan sonuçlardan öğrencilerin öğrenme çıktısına etkisinin ilgili araştırmalardaki eğilimler sonucunda belirlenmesi amaçlanan mevcut çalışmada sistematik inceleme sonucunda ulaşılan bulgular bağlamında sonuçlar tartışılmıştır. Bu makalede incelenen çalışmaların en çok 2006 yılında yayınlandığı görülmektedir. Ancak diğer yıllar dalgalanmalara ve özellikle günümüzde uzaktan eğitim kavramı çerçevesinde veri madenciliği kullanımı ile ilgili az çalışmaya rastlanmaktadır. Ancak günümüzde uzaktan eğitim kavramı yerine çevrimiçi öğrenme kavramının kullanılması bu duruma sebep olabilmektedir.

İncelenen çalışmalar anahtar kelimeler bağlamında analiz edildiğinde en fazla veri madenciliği kelimesinin kullanıldığı ardından uzaktan eğitim, eğitsel veri madenciliği, e-öğrenme anahtar kelimeleri tercih edilmiştir. Araştırma amacı bağlamında bu anahtar kelimelerin görülmesi beklenen bir durumdur. İncelenen çalışmalarda kullanılan araştırma yönteminin analizine göre %53 oranında nicel, %23 oranında nitel, %16 oranında karma ve %8 oranında alanyazın derleme yöntemi kullanıldığı belirlenmiştir. İncelenen çalışmalar belirlenirken herhangi bir çalışma türü tercih edilmediği için çalışmaların yöntem çeşitliliği bulunmaktadır. Ayrıca incelenen çalışmalar kullanılan veri toplama araçlarına göre analizden en fazla hazır veri seti kullanıldığı görülmektedir. Bu durum ise veri madenciliği çalışmalarında uzaktan eğitim sistemleri üzerinden çoklu verilerin temin edilebilmesinden kaynaklanmaktadır. İncelenen çalışmalar katılımcı profili bağlamında analiz edildiğinde uzaktan eğitimi en fazla üniversite düzeyindeki öğrencilerin aldığı görülmektedir. Bunun dışında incelenen çalışmaların en fazla Çin'de yapıldığı, en fazla bilgisayar alanında yapıldığı, çalışmalarda verilerin en fazla Moodle'dan elde edildiği, en fazla Weka yazılım aracıyla verilerin analiz edildiği ve veri madenciliğinde çoğunlukla kümeleme yönteminin kullanıldığı tespit edilmiştir. Veri madenciliği çalışmalarında kümeleme yönteminin kullanılması son zamanlarda çalışmalarda yaygın olarak kullanılmaktadır (Koldere Akın, 2008). Bu durum araştırma sonucunu desteklemektedir.

İncelenen çalışmalar öğrenme çıktıları bağlamında analiz edildiğinde, öğrencinin eğitim aldığı çevrimiçi ortamdan elde edilen veri kaynaklarına göre veri madenciliği ile modellenmesi, aldığı eğitimi yarıda bırakma eğilimi olan öğrencilerin ya da motivasyon, öz düzenleme yetersizliklerini, her öğretim dönem sonucunda meydana gelebilecek başarısızlıkların erkenden tahmin edilmesi ve önceden müdahale edilmesi açısından önemlidir. Burada elde edilen veriler kullanıcı ya da öğrenciye uygun modeller yapılarak yapılandırılabilir. Öğrencilerin öğrenme ortamlarına göre derse aktif katılım sağlaması otomatik olarak kategorileştirilmesi ya da sınıflandırılmasında uyarlamaların otomatikleştirilebilmesi neticesinde kullanılabilirdir (Akçapınar, 2014). Farklı bir perspektiften bakıldığında çevrimiçi öğrenme ortamları öğrenci performansını değerlendirme noktasında ve değerlendirmelerin analiz yapılabilmesini sağlaması yönüyle önemli bulunmaktadır. Öğrenci performans verilerinin analizi için çeşitli sınıflama yöntemlerinden elde edilen veriler kıyaslanarak öğrenciler için en etkili tahmin algoritmasının belirlenmesi hedeflenmektedir (Akçapınar, 2014). Seçilen algoritma yöntemleriyle öğrencilerin ileriye dönük akademik başarılarını önceden tahmin edilip edilemeyeceği araştırılabilmektedir. Veri madenciliğinde verilerin

analiz sürecinde anlamsız verilerin sentezlenerek anlamlı ve değerli veri setlerini ortaya çıkarmak için incelenen çalışmalarda çoğunlukla kümeleme ve karar ağacı tercih edilmektedir. Bu durumda öğrenme ortamında yapılan tahmin çalışması için amaç öğrencinin bilinen yeteneklerinden bilinmeyen farklı yeteneklerini ortaya çıkarmaktır (Romero & Ventura, 2010). Bu kapsamda öğrenci performansıyla ilgili kullanılan yöntemler geleceğe yönelik tahmin modelleriyle öğrenme ortamlarını öğrenciye uygun ya da öğrencinin performansına göre öğrenme ortamını uyarlanabilmektedir. Veri madenciliği ile elde edilen sonuçlar öğrencilerin yeteneklerinin farkına varmasına ve kendisine özgü farkındalık oluşturmasını sağlamak amacıyla kullanılabilmektedir (Bienkowski, Feng, & Means, 2012). Veri madenciliği çalışmalarında öğrenci performansını tahmin etmek amaçlı yöntem ve model kullanılması öğreticilerin bu sonuca ulaşabilmesi, onların çaba ve zamandan tasarruf etmesini sağlayabilmektedir (Lopez, Luna, Romeo, & Ventura, 2012). Veri madenciliği yöntemleri kullanılarak öğrencilerin akademik performansı ders öncesinde tahmin edilerek olası başarısızlıklar için müdahaleler oluşturulabilir. Bu sayede performansının yüksek olması için uygulanan müdahaleler başarısızlıkların önlenmesine yardımcı olabilir (Johnson, Smith, Willis, Levine, & Haywood, 2011). Bu noktada öğreticiler, öğrencilerin gelişimlerini izleme ve müdahale etmek için uygun yöntemler geliştirebilir. Burada elde edilen veriler kişiye ait öğrenme ortamları oluşturulması yönüyle önemlidir (Bienkowski ve diğerleri, 2012). Öğrenme ortamlarının ayrılmaz parçası ise otomatik sınıflama işlemidir. Bu işlemi gerçekleştirmeden önce öğrencilerin mevcut durumu hakkında sınıflandırma yapılmalıdır (Hämäläinen & Vinni, 2010). Bunun dışında öğrenci verileri üzerinde kümeleme analizi yapılması benzer özellikli değişkenlerin bir arada görülmesi açısından önemli bulunmaktadır. Bu sayede öğrenci verilerinde kümeleme analizi yapmak öğrenme grubuna yeni katılacak öğrencilerin gruplandırılmasını sağlamak amaçlı kullanılabilir (Bouchet, Harley, Trevors, & Azevedo, 2013). Sonuç olarak çevrimiçi öğrenme ortamının öğrenciler üzerindeki etkilerine odaklandığı sonucunda elde edilen bilgiler neticesinde veri madenciliği ile veriler anlamlı hale getirilip öğrenciler üzerinde olumlu bir etkiye sahip olduğu gözlenmektedir.

Sınırlılıklar ve Öneriler

Bu sonuçlar dışında mevcut araştırmanın birtakım sınırlılıkları vardır. Bu çalışmada veri madenciliği ve uzaktan eğitim kavramları ele alınırken günümüzde çoğunlukla kullanılan çevrimiçi eğitim ve çevrimiçi öğrenme kavramları ele alınmamıştır. Gelecek araştırmalarda hem uzaktan eğitim hem de çevrimiçi öğrenmenin veri madenciliği ile incelendiği çalışmalar üzerine araştırma yapılabilir. Bunun yanında çalışmada Nisan 2022 yılına kadar Web of Science'da yayınlanmış ve veritabanı üzerinden ulaşılabilen çalışmaların incelenmesini kapsamaktadır. Bu nedenle ulaşılamayan çalışmalar kapsam dışı bırakılmıştır. Gelecek araştırmalarda ise diğer veritabanları üzerinde de inceleme yapılarak geniş bir araştırma yelpazesi kullanılabilir.

Yayın Etiği Bildirimi / Research Ethics

Çalışma sürecinde hiçbir etik kural ihlal edilmemiştir. / No ethical rules were violated during the study process.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Çalışmada yazarların katkı oranı eşittir. / The contribution rate of the authors in the study is equal.

Çıkar Çatışması / Conflict of Interest

Yazarlar arasında herhangi bir çıkar çatışması bulunmamaktadır. / There is no conflict of interest between the authors.

Fon Bilgileri / Funding

Araştırmadan herhangi bir fon elde edilmemiştir. Herhangi bir kurum tarafından desteklenmemiştir. / No funding was obtained from the research. It is not supported by any institution.

Etik Kurul Onayı / The Ethical Commitee Approval

Araştırmada, açık, uluslararası veri tabanında bulunan veriler kullanıldığından etik kurul kararı gerektirmemektedir. / Since the data in an open, international database were used in the study, it does not require an ethics committee decision.

Kaynakça / References

Akcapinar, G., & Bayazit, A. (2018). Investigating video viewing behaviors of students with different learning approaches using video analytics. *Turkish Online Journal of Distance Education, 19*(4), 116-125.

Akçapınar, G. (2014). *Çevrimiçi öğrenme ortamındaki etkileşim verilerine göre öğrencilerin akademik performanslarının veri madenciliği yaklaşımı ile modellenmesi.* (Yayımlanmamış Doktora Tezi). Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara.

Akmeşe, Ö. F., Kör, H., & Erbay, H. (2021). Use of machine learning techniques the forecast of student achievement in higher aducation. *Information Technologies and Learning Tools, 82*(2), 297-311.

Akyürek, M. İ. (2020). Uzaktan Eğitim: Bir Alanyazın taraması. *Medeniyet Eğitim Araştırmaları Dergisi, 4*(1), 1-9. Retrieved from https://dergipark.org.tr/tr/pub/mead/issue/56310/711904

Al-Musharraf, A., & Alkhattabi, M. (2016). An educational data mining approach to explore the effect of using interactive supporting features in an LMS for overall performance within an online learning environment. *International Journal of Computer Science and Network Security (IJCSNS), 16*(3), 1.

Anaya, A. R., Luque, M., & Peinado, M. (2016). A visual recommender tool in a collaborative learning experience. *Expert Systems with Applications, 45*, 248-259.

Andrade, T. L. D., Rigo, S. J., & Barbosa, J. L. V. (2021). Active Methodology, Educational Data Mining and Learning Analytics: A Systematic Mapping Study. *Informatics in Education, 20*(2).

Aydın, S., (2007). *Veri madenciliği ve Anadolu Üniversitesi uzaktan eğitim sisteminde bir uygulama*. (Yayımlanmamış Doktora Tezi). Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Eskişehir.

Aydoğdu, Ş. (2020). Educational data mining studies in Turkey: A systematic review. *Turkish Online Journal of Distance Education, 21*(3), 170-185.

Bezerra, L. N. M., & Silva, M. T. (2020). Educational Data Mining Applied to a Massive Course. *International Journal of Distance Education Technologies, 18*(4), 17–30. doi:10.4018/ijdet.2020100102

Bienkowski, M., Feng, M., & Means, B. (2012). Enhancing Teaching and Learning through Educational Data Mining and Learning Analytics: An Issue Brief. Office of Educational Technology, US Department of Education.

Bouchet, F., Harley, J. M., Trevors, G. J., & Azevedo, R. (2013). Clustering and profiling students according to their interactions with an intelligent tutoring system fostering self-regulated learning. *Journal of Educational Data Mining, 5*(1), 104-146. https://doi.org/10.5281/zenodo.3554613

Bozkurt, A. (2017). Türkiye'de uzaktan eğitimin dünü, bugünü ve yarını. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi, 3*(2), 85-124.

Chatti, M. A., Dyckhoff, A. L., Schroeder, U., & Thüs, H. (2012). A reference model for learning analytics. *International Journal of Technology Enhanced Learning, 4*(5), 318-331. doi: 10.1504/IJTEL.2012.051815

Chen, H., Dai, Y., Gao, H., Han, D., & Li, S. (2019). Classification and analysis of moocs learner's state: The

study of hidden markov model. *Computer Science and Information Systems*, *16*(3), 849-865.

Cheng, L. C., Chu, H. C., & Shiue, B. M. (2015). An innovative approach for assisting teachers in improving instructional strategies via analyzing historical assessment data of students. *International Journal of Distance Education Technologies (IJDET)*, *13*(4), 40-61.

Cihan, P. (2018). *Veri madenciliği yöntemleriyle hayvan hastalıklarında teşhis, prognoz ve risk faktörlerinin belirlenmesi*. (Yayımlanmamış Doktora Tezi). Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Coşlu, E. (2013). Veri madenciliği. *Akademik bilişim*, 23-25.

Çelebi, V. (2019). Bayes teoremi bağlamında olasılıkçı bayes epistemolojisinin kapsamı üzerine bir inceleme. FLSF *Felsefe ve Sosyal Bilimler Dergisi* (28):319–43.

Çiltaş, A. (2011). Eğitimde öz-düzenleme öğretiminin önemi üzerine bir çalışma. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *3*(5), 1-11.

Demirel, M. (1993). Öğrenme stratejilerinin öğretimi. *Eğitim ve Bilim, 17*(88).

Dinçer, S. (2016). Bilgisayar Destekli Eğitim ve Uzaktan Eğitime Genel Bir Bakış. *Adana, Seyhan, Türkiye*.

Erfidan, Ali. (2019). *Derslerin uzaktan eğitim yoluyla verilmesiyle ilgili öğretim elemanı ve öğrenci görüşleri Balıkesir Üniversitesi örneği*. (Yayınlanmamış Yüksek Lisans Tezi). Balıkesir Üniversitesi Fen Bilimleri Enstitüsü, Balıkesir.

Erten, H. (2015). *Veri Madenciliği Teknikleri ile Organ Nakli İçin Uygun Donör Oranının Hesaplanması*. (Yayınlanmamış Yüksek lisans tezi). Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

Fok, W. W., Chen, H., Yi, J., Li, S., Yeung, H. A., Ying, W., & Fang, L. (2014). Data mining application of decision trees for student profiling at the Open University of China. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 732-738). IEEE.

Gao, Y., & Zhang, S. (2018). Design of and research on autonomous learning system for distance education based on data mining technology. *Educational Sciences: Theory & Practice*, *18*(6).

García, E., Romero, C., Ventura, S., & De Castro, C. (2011). A collaborative educational association rule mining tool. *The Internet and Higher Education*, *14*(2), 77-88.

Hämäläinen, W., & Vinni, M. (2010). Classifiers for educational technology. *Handbook on educational data mining*.

Hämäläinen, W., & Vinni, M. (2011). Classifiers for educational data mining. *Handbook of Educational Data Mining, Chapman & Hall/CRC Data Mining and Knowledge Discovery Series*, 57-71.

Hampel, R., & Pleines, C. (2013). Fostering student interaction and engagement in a virtual learning environment: An investigation into activity design and implementation. *Calico Journal*, *30*(3), 342-370.

Johnson, L., Smith, R., Willis, H., Levine, A. & Haywood, K. (2011). The 2011 horizon report, Austin, TX: The New Media Consortium.

Karaçam, Z. (2013). Sistematik derleme metodolojisi: Sistematik derleme hazırlamak için bir rehber. *Dokuz Eylül Üniversitesi Hemşirelik Yüksekokulu Elektronik Dergisi*, *6*(1), 26-33.

Kitchenham, B. (2004). *Procedures for performing systematic reviews*. Joint technical report Software Engineering Group, Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd, Australia.

Koldere Akın, Y. (2008). *Veri madenciliğinde kümeleme algoritmaları ve kümeleme analizi.* (Yayınlanmamış Doktora Tezi). Marmara Üniversitesi, Sosyal Bilimler Üniversitesi, İstanbul.

Kumtepe, A. T., Atasoy, E., Kaya, Ö., Uğur, S., Dinçer, G. D., Erdoğdu, E., & Aydın, C. H. (2019). An Interaction Framework for Open and Distance Learning: Learning Outcomes, Motivation, Satisfaction, Perception. *AJIT-e: Bilişim Teknolojileri Online Dergisi, 10*(36), 7-26.

Lopez, M. I., Luna, J. M., Romero, C., & Ventura, S. (2012). Classification via clustering for predicting final marks based on student participation in forums. *International Educational Data Mining Society*.

Maher, A. (2004). Learning outcomes in higher education: Implications for curriculum design and student learning. *Journal of Hospitality, Leisure, Sport and Tourism Education, 3*(2), 46-54.

Moore, M. G., & Kearsley, G. (2011). *Distance education: A systems view of online learning*. Cengage Learning.

Mullen, G. E., & Tallent-Runnels, M. K. (2006). Student outcomes and perceptions of instructors' demands and support in online and traditional classrooms. *The Internet and Higher Education*, 9, 257-266.

Newman, M. & Gough, D. (2020). Systematic reviews in educational research: methodology, perspectives and application. In O. Zawacki-Richter, M. Kerres, S. Bedenlier, M. Bond, K. & Buntins (Eds.), *Systematic reviews in educational research*: Methodology, perspectives and application (pp. 3-22). Wiesbaden: Springer VS.

Özbay, Ö. (2015). Veri madenciliği kavramı ve eğitimde veri madenciliği uygulamaları. *Uluslararası Eğitim Bilimleri Dergisi*, (5), 262-272.

Özkan, Y. (2016). *Veri Madenciliği Yöntemleri* (4.Baskı), Ankara: Papatya Yayınları.

Preidys, S., & Sakalauskas, L. (2010). Analysis of students' study activities in virtual learning environments using data mining methods. *Technological and economic development of economy*, *16*(1), 94-108.

Romero, C., & Ventura, S. (2010). Educational data mining: a review of the state of the art. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *40*(6), 601-618.

Romero, C., & Ventura, S. (2012). Data mining in education. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 3(1), 12–27.* doi:10.1002/widm.1075

Romero, C., Espejo, P. G., Zafra, A., Romero, J. R., & Ventura, S. (2010). Web usage mining for predicting final marks of students that use Moodle courses. *Computer Applications in Engineering Education, 21*(1), 135–146. doi:10.1002/cae.20456

Romero, C., Espejo, P. G., Zafra, A., Romero, J. R., & Ventura, S. (2013). Web usage mining for predicting final marks of students that use Moodle courses. *Computer Applications in Engineering Education, 21*(1), 135-146. doi: 10.1002/cae.20456

Romero, C., López, M. I., Luna, J. M., & Ventura, S. (2013). Predicting students' final performance from participation in on-line discussion forums. *Computers & Education, 68*, 458-472.

Romero, C., Ventura, S., & García, E. (2008). Data mining in course management systems: Moodle case study and tutorial. *Computers & Education, 51*(1), 368-384. doi: http://dx.doi.org/10.1016/j.compedu.2007.05.016

Romero, C., Ventura, S., Espejo, P. G., & Hervás, C. (2008). Data mining algorithms to classify students. *In Educational data mining 2008*.

Sen, B., & Ucar, E. (2012). Evaluating the achievements of computer engineering department of distance education students with data mining methods. *Procedia Technology, 1*, 262-267.

Siemens, G., & Baker, R. S. D. (2012). Learning analytics and educational data mining: towards communication and collaboration. In *Proceedings of the 2nd international conference on learning analytics and knowledge* (pp. 252-254).

Tekin, A. (2018). Tıp'ta veri madenciliği uygulamaları: Yenidoğan sepsisi veri seti analizi/Data mining applications in medicine: Newborn sepsis data set analysis.

Trigwell, K., & Prosser, M. (1991). Improving the quality of student learning: the influence of learning context and student approaches to learning on learning outcomes. Higher *Education, 22*(3), 251–266. doi:10.1007/bf00132290

Uzun, Y., Uzun, F. N., & Çakar, E. (2021). *Veri madenciliği ve kullanım alanları*. Uluslararası Mühendislik, Doğa ve Sosyal Bilimler Sempozyumu, Batman.

Viloria, A., López, J. R., Payares, K., Vargas-Mercado, C., Duran, S. E., Hernández-Palma, H., & David, M. A. (2019). Determinating Student Interactions in a Virtual Learning Environment Using Data Mining. *Procedia Computer Science, 155*, 587–592. doi:10.1016/j.procs.2019.08.082

Yasmin, D. (2013). Application of the classification tree model in predicting learner dropout behaviour in open and distance learning. *Distance Education, 34*(2), 218-231.

Yılmaz, K. (2021). Sosyal bilimlerde ve eğitim bilimlerinde sistematik derleme, meta değerlendirme ve bibliyometrik analizler. *Manas Sosyal Araştırmalar Dergisi, 10*(2), 1457-1490.

Yilmaz, R. (2017). Problems experienced in evaluating success and performance in distance education: A case study. *Turkish Online Journal of Distance Education, 18*(1), 39-51.

Yurdugül, H.& Menzi Çetin, N. (2015). Investigation of the relationship between learning process and learning outcomes in e-learning environments. *Eurasian Journal of Educational Research*, 59, 57-74. http://dx.doi.org/10.14689/ejer.2015.59.4

Yurtoğlu, H. (2005). *Yapay Sinir Ağları Modellemesi ile Öngörü Modellemesi: Bazı Makroekonomik Değişkenler için Türkiye Örneği*. (Uzmanlık Tezi). DPT, Ankara.

Zang, W., & Lin, F. (2003, August). Investigation of web-based teaching and learning by boosting algorithms. In *International Conference on Information Technology: Research and Education, 2003. Proceedings*. *ITRE2003.* (pp. 445-449). IEEE.

Zhang, X., Gao, Y., Yan, X., de Pablos, P. O., Sun, Y., & Cao, X. (2015). From e-learning to social-learning: Mapping development of studies on social media-supported knowledge management. *Computers in Human Behavior, 51*, 803-811.

Zimmerman, T. D. (2012). Exploring learner to content interaction as a success factor in online courses. *The International Review of Research in Open and Distributed Learning, 13*(4), 152. doi:10.19173/irrodl.v13i4.1302

2022

4(2), 227-246

Otizm Spektrum Bozukluğu Gösteren Öğrenciler için Oyun-tabanlı Artırılmış Gerçeklik Uygulaması Tasarlama ve Geliştirme

Hakan Özcan*[1], Haluk Şahin[2], Onurcan Çıra[3], Pembe Pelin Koca[4]

Anahtar Sözcükler
Artırılmış gerçeklik
Mobil uygulama
Otizm spektrum
Oyun-tabanlı
Özel eğitim

Makale Hakkında
Gönderim Tarihi
20 Eylül 2022
Kabul Tarihi
18 Aralık 2022
Yayın Tarihi
28 Aralık 2022
Makale Türü
Araştırma Makalesi

Öz

Teknolojik gelişmeler eğitim programlarında bireysel farklılıklardan kaynaklı oluşabilecek boşlukların doldurulmasına yardımcı olabilecek imkanlar sunmaktadır. Bu çalışmada, yazılım geliştirme ve etkinlik değerlendirme süreçlerini içeren disiplinler-arası bir yaklaşım izlenmiştir. Otizmli öğrenciler için trafikte ilk yardımı ilgilendiren temel konular çerçevesinde üç özgün materyal geliştirilmiştir. Bunlardan ilki, öğrencilerin gördüklerini veya duyduklarını bir etkileşim senaryosu dahilinde yansıtabilecekleri bir oyun kitabıdır. İkincisi, bu oyun kitabı ile bütünleşik çalışan bir artırılmış gerçeklik uygulamasıdır. Üçüncüsü ise öğrenme sürecinin okul-dışı ortamlarda da sürdürülebilmesi için bir Web-tabanlı veli katılım sistemidir. Bir durum çalışması kapsamında nitel araştırma yöntemlerinden yararlanılmıştır. Teknolojik bileşenler ve etkileşimler görüşme yoluyla belirlenmiştir. Öğrencilerin objeleri kaydırma, çekme, yapıştırma gibi işlemlere yatkın oldukları, fakat eşleştirme, birleştirme ve duyduklarına eşlik etmede zorluk yaşadıkları gözlemlenmiştir. Bu çalışma, "herkese uyan" tek tipte bir yaklaşımın otizmli öğrenciler için uygun olmadığının altını çizmektedir. Uygulamalarda bireyselleştirilmiş destek önerilmektedir. Bulguların ilgili uygulama tasarımlarına ve diğer çalışmalara fikir vermesi umulmaktadır.

Designing and Developing a Game-based Augmented Reality Application for Students with Autism Spectrum Disorder

Keywords
Augmented reality
Mobile application
Autism spectrum
Game-based
Special education

Article Info
Received
September 20, 2022
Accepted
December 18, 2022
Published
December 28, 2022
Article Type
Research Paper

Abstract

Technological developments offer opportunities that can help fill the gaps that may arise from individual differences in education programs. In this study, an interdisciplinary approach was followed, including software development and activity evaluation processes. Three original materials have been developed for students with autism within the basic concepts concerning first aid in traffic. The first is a playbook with which students can reflect on what they see or hear within an interaction-based scenario. Second, it is an augmented reality application that works integrated with the playbook. The third is a Web-based parent participation system for the continuation of the learning process in out-of-school environments. Qualitative research methods were used in a case study. The technological components and interactions were determined through interviews. It has been observed that students are prone to engage in activities such as shifting, pulling, and pasting objects, but they have difficulties in matching, combining, and accompanying what they hear. This study underlines that a "one-size-fits-all" approach is not suitable for students with autism. Individualized support in the applications is recommended. The findings may give insights to the related application designs and similar studies to be carried out.

Atıf: Özcan, H., Şahin, H., Çıra, O., & Koca, P. P., (2022). Otizm spektrum bozukluğu gösteren öğrenciler için oyun-tabanlı artırılmış gerçeklik uygulaması tasarlama ve geliştirme. *Bilgi ve İletişim Teknolojileri Dergisi*, *4*(2), 227-246.https://doi.org/10.53694/bited.1177541
Cite: Ozcan, H., Sahin, H., Cira, O., & Koca, P. P., (2022). Designing and developing a game-based augmented reality application for students with autism spectrum disorder. *Journal of Information and Communication Technologies*, *4*(2), 227-246. https://doi.org/10.53694/bited.1177541

***Sorumlu Yazar/Corresponding Author**: hozcan@amasya.edu.tr
[1] Asst. Prof. Dr., Amasya University, Computer Technology, Amasya/Turkey, hozcan@amasya.edu.tr , https://orcid.org/0000-0002-4352-8716
[2] M.Sc. Student, Amasya University, Computer Education and Instructional Technology, Graduate School of Natural and Applied Sciences, Amasya/Turkey, haluk.sahin97@gmail.com , https://orcid.org/0000-0002-2101-9646
[3] Student, Amasya University, Computer Education and Instructional Technology, Amasya/Turkey, onurcan.cira96@gmail.com , https://orcid.org/0000-0001-8357-1594
[4] M.Sc. Student, Amasya University, Computer Education and Instructional Technology, Graduate School of Natural and Applied Sciences, Amasya/Turkey, pelinkoca.58@gmail.com , https://orcid.org/0000-0002-0058-9578

Extended Abstract

Introduction

Autism is a disorder that arises from birth or arises from neurological-developmental disorders in the first years of development, limits social interaction, causes repetitive behaviors, and complicates learning processes (Korkmaz, 2010). People with autism may have deficiencies in interpreting the events around them, establishing a dialogue with others, and reacting to the instructions given (Ökcün-Akçamuş, 2016). In a report (TOV, 2008), it is recommended that an individual diagnosed with autism should begin early education services within the first three months and this education should be continued for at least twenty hours a week. In the same report, it is underlined that autism-specific programs should be designed according to individual needs (TOV, 2008). Individualized special education based on motivation is of great importance in meeting these needs (Eliçin & Yıkmış, 2015). The main criteria that special education should carry are as follows: Education must be continuous, intense, repetitive, individualized, contain definite goals, be designed not only according to age but also according to developmental level, create a learning environment with objects to be taught, include the family in education to ensure the continuity of learning (TOV, 2008). Such learning environments should be supported with specially designed visual materials and computer-based applications (Serin et al., 2021).

A game is a tool that supports children's research, discovery, imitation of what they see or hear, and therefore improving their various skills (Ünal, 2009). The game has positive effects in expanding and improving cognitive and behavioral flexibility as well as language and motor skills in the developmental process of children, and game-based applications are accepted as an effective method that can be used in special education (Kaytez & Durualp, 2014). A study (Öncül & Çifci Tekinarslan, 2021) has shown that autistic children can reinforce their learning processes through video-based modeling. It has become widespread to use various videos and animations in the creation of game-based instructional materials (Bozkurt, 2017; Jiménez-Muñoz et al., 2022). Augmented reality-based applications that combine printed materials such as books, magazines, and brochures with three-dimensional environments have also started to be used in special education (Yakubova et al., 2021). Studies (Cakir & Korkmaz, 2019; Kandalaft et al., 2012; Pan & Hamilton, 2018) report that augmented reality is beneficial when the real conditions are not easily accessible or experimental environments are difficult to set up. Therefore, we preferred augmented reality applications for environments that concern security and portray what should be done in an emergency.

In this study, we developed an application to help children with autism understand the basic rules and concerns related to first aid in traffic easily. The output of this study, unlike plain book applications in this field, integrates the augmented reality application with a book consisting of interactive and dynamic pages designed with the "Pop-Up" method and includes videos and animations, all of which are prepared specifically to the application. In addition, a Web-based parent participation system is offered to ensure the continuity of the education. The main research questions of the study: 1) What should be the material/application that supports the teaching needed by the target group within the framework of the basic concepts in the curriculum related to first aid in traffic? 2) How difficult is it from the teacher's point of view for students to complete the target tasks for a sample material application developed according to the identified needs?

Method

An interdisciplinary approach was followed, which includes software development and evaluation processes over the real environment. Analysis, design, development, implementation, and evaluation stages were conducted in the production of software components (Branch, 2009; Rosenberg, 1982). The research method involved a case study using the qualitative methods of both interviews and observations (Subaşı & Okumuş, 2017). The scope of this study is limited to the development of an application for students with autism spectrum disorder and the teaching activities carried out with this application. The ethics committee approval, institutional permission, and parental consent were obtained before the study.

The technological components, interactivity features and flow of the application were determined through semi-structured interviews with special education certificated teachers (N=4) and instructional technology experts (N=4) (Creswell, 2013). Vuforia Engine (Xiao & Lifeng, 2014) software development kit was used on the Unity game engine (Kim et al., 2014) to create the augmented reality infrastructure. HTML5, Javascript, MySQL and PHP technologies (Stoeva, 2014) were used in the web-based parent participation system, and 3D Studio MAX (YANG et al., 2004) was used for three-dimensional models. Three basic steps were followed in the development process of the mobile application. In the first step, media materials were prepared with storyboards. In the second step, QR codes were generated, and associated with Vuforia Engine in accordance with the flow of activities. In the last step, the interaction modules were coded with the C# programming language. In the development of the web application, a relational database was used for teacher, parent, student, and activity information. A system that works in accordance with the defined roles of each user (parents and teachers) was developed over a dynamic web interface. Android and iOS-based tests of the mobile application and in-class implementations were carried out on Sony Xperia 5 and Apple iPhone 8 Plus.

The implementation of the components was carried out one-on-one in the classroom in a private education institution with 4 male students aged between 8 and 19 with autism spectrum disorder under the guidance of their teachers. Participants were selected from those who were readily available at the time of the case study and agreed to be included in the study (Sedgwick, 2013).Two steps were followed in the interviews. In the first step, the teachers were asked about the "material/application types that supports the teaching needed by the target group within the framework of the basic concepts in the curriculum concerning first aid in traffic " to try to understand what tools they need during the teaching-learning process. Then the opinions of the experts were taken for the selection and determination of applicability of the corresponding technological components. The final application was shaped in accordance with students' learning styles and along with the literature. A task list (activity chart) was created in line with the teacher opinions according to the interactions expected from the students. Then scoring was made between 1 and 5 using a Likert-type evaluation scale for each task (F. Antonak & Livneh, 2000; Likert, 1932). In addition, observed difficulties in completing the activities were also noted at the end of this chart. For the production stage of the study, we followed the analysis, design, development, implementation, and evaluation phases (Branch, 2009; Rosenberg, 1982).

Findings

According to the results of the interviews with the special education teachers, 5 themes were driven: 1) Lack of interaction: The basic concepts related to first aid in traffic were explained only with printed cards and there was

a lack of interaction. All teachers think that there is a need for interactive games that will attract students' attention during the lesson. 2) Concept confusion: Some teachers (n=2) stated that children with autism have difficulty in understanding or distinguishing the concepts of ambulance, police, and fire department, and it is not always possible to show such concepts in real environment. 3) Lack of digital materials: Teachers emphasized that they had difficulty in finding digital materials that they could use during the lesson. 4) Parent involvement: According to some of the teachers (n=3), it was found beneficial for students to continue various in-class activities at home. They highlighted the importance of parental support for the continuity of education.

To respond to these needs, a group of interactive activities that will take place in the application were decided by taking the opinions of the experts. Based on the analysis results, three different application components were developed in accordance with the subject: 1) An interactive book and integrated materials (video, audio, text, and animation); 2) An augmented reality application (A mobile application); 3) A parent participation system (A Web-based application). All components have been improved according to the feedbacks received at the time of development. The general appearance of the application is presented in Figure 2, Figure 3, and Appendix 2.

The application was used by students with autism spectrum disorder accompanied by their respective teachers. Sessions were held individually. In this process, the completion levels of the target tasks (Table 4) were noted by Teacher 1. One (1) point was given for the tasks that were never completed; 5 points were given to the tasks that were completely completed. As for the target tasks completion report, the maximum total score that could be obtained was 90. The student who came closest to this score was Participant 4, while the student who got the least score was Participant 1. It was observed that the participants were generally more prone to engage in activities such as shifting, pulling, and pasting the items in the application. However, they had difficulties in matching and combining activities. The students generally listened to the songs and stories, but they hesitated when they had to repeat.

Discussion and Conclusion

We observed that teachers' explaining the subject through a story-based interactive playbook with an augmented reality application, allowed the students to engage in activities by having fun. According to the teachers’ thoughts, the basic concepts related to first aid in traffic became more interesting for the students.

When the target task completion report is examined as a whole, it has been revealed that age information alone is not explanatory in understanding the task difficulties, and the level of need for special education should also be considered. While using the app, students with autism spectrum disorders performed better on the tasks related to usability (e.g., Task 1, Task 2, Task 3, Task 13, Task 18) but on the tasks that required intellectual effort (e.g., Task 4, Task 7, Task 12, Task 14, Task 17) showed relatively low-level performance. This result implies that the application's usability can be considered at a sufficient level for students with autism spectrum disorder; On the other hand, it points out the necessity of parent or teacher support for intellectual tasks in practice. In addition, while the students performed at similar levels on some tasks such as Task 8, Task 9, and Task 13, they showed different performances in other tasks (e.g., Task 4 and Task 5). This can be seen to be related to the individual differences of the students, and it can give an idea for the teacher and parent support to be provided in the use of such applications, considering the individual characteristics of the student, or allowing for more individualization.

The findings of this study underline that a “one-size-fits-all” approach is not suitable for students with autism spectrum disorder. Even if an app is developed entirely based on the characteristics of students with autism, individualized support is important. In order to improve the educational opportunities of students with autism, it is recommended that augmented reality-based applications be explored in other subject areas and expanded for other academic gains.

This research is limited to a case study. The literature-reported, the application-developed, and the findings-revealed by this study may not be a true representation for the entire population. It was assumed that the interviewees answered the questions in the best possible way. Further studies in larger groups are needed to replicate the findings and to elucidate the designing and application requirements for students with autism.

Giriş

Otizm, doğuştan ortaya çıkan veya gelişimin ilk yıllarında nörolojik-gelişimsel bozukluklardan kaynaklı beliren, sosyal etkileşimini sınırlayan, tekrarlı davranışlara sebep olan ve öğrenme süreçlerini zorlaştıran bir rahatsızlıktır (Korkmaz, 2010). Otistik özellikler gösteren bireylerin çevresindeki olayları yorumlama şekli, akranları ile diyalog kurması ve verilen yönergelere tepkileri eksiklikler taşıyabilmektedir (Ökcün-Akçamuş, 2016). Bu bireylerin yönlendirilmesinde, temel eğitimlerinin sağlanmasında ve değerlendirilmesinde geleneksel eğitime göre önemli farklılıklar bulunmaktadır (Davis ve diğerleri, 2010). Sunulan bir raporda (TOV, 2008), otizm tanısı konulan bir bireyde ilk üç ay içinde erken eğitim hizmetlerinin başlatılması ve bu eğitimin haftada en az yirmi saat sürdürülmesi önerilmektedir. Aynı raporda, erken eğitimi izleyen süreçte otizme özgü programların bireysel ihtiyaçlara göre tasarlanması tavsiye edilmektedir (TOV, 2008). Bu ihtiyaçların sağlanmasında güdülemeye dayalı bireyselleştirilmiş özel eğitimin önemi büyüktür (Eliçin & Yıkmış, 2015). Özel eğitimin taşıması gereken temel kriterler şunlardır: Eğitimin sürekli, yoğun ve tekrarlı olması, bireyselleştirilebilmesi, kesin hedefler içermesi, sadece yaşa göre değil gelişim düzeyine göre tasarlanması, öğrenme ortamının öğretilecek nesnelerle donatılması ve ailenin eğitime dahil edilerek öğrenme sürekliliğinin sağlanmasıdır (TOV, 2008). Böyle öğrenme ortamlarının özel tasarlanmış görsel materyallerle ve bilgisayar-tabanlı uygulamalarla desteklenmesi önemlidir (Serin ve diğerleri, 2021).

Oyun, çocukların araştırmayı, keşfetmeyi, gördüklerini veya duyduklarını taklit etmeyi ve dolayısıyla çeşitli becerilerini geliştirmeyi destekleyen bir araçtır (Ünal, 2009). Çocuklarda oynatılan oyunların eğitim-öğretim süreçlerine yönelik somut katkılar sağlayabildiği bilinmektedir (Ginsburg ve diğerleri, 2007). Oyunun çocukların gelişim sürecinde dil ve motor becerilerin yanı sıra bilişsel ve davranışsal esnekliklerin genişletilmesinde ve iyileştirilmesinde olumlu etkilerinin olduğu görülmekte ve oyun-temelli uygulamalar özel eğitimde kullanılabilecek etkili bir yöntem olarak kabul edilmektedir (Kaytez & Durualp, 2014). Özel eğitimde oyun-temelli yaklaşımlar uygulanırken, çocuğun taklit becerilerine odaklanan sürekli oynama fırsatı sağlayacak serbest oyun ortamlarının sunulması ve gerçek yaşam ile ilişkilendirilmesi önem taşımaktadır (Pişkin, 1993). Yapılan bir araştırma (Öncül & Çifci Tekinarslan, 2021) otistik çocukların video tabanlı model alma yoluyla öğrenme süreçlerini pekiştirebildiklerini göstermiştir. Son zamanlarda, oyun tabanlı öğretim materyallerinin oluşturulmasında canlandırma yoluyla çeşitli video ve animasyonlardan yararlanılması ve öğretim tasarımına adapte edilmesi yaygınlaşmıştır (Bozkurt, 2017; Jiménez-Muñoz ve diğerleri, 2022). Artırılmış gerçeklik olarak da adlandırılan ve kitap, dergi, broşür gibi durağan materyalleri video temelli ve üç boyutlu ortamlarla buluşturan uygulamalar özel eğitimde de kullanılmaya başlamıştır (Yakubova ve diğerleri, 2021). Gerçek koşulların sağlanamadığı ya da deneme ortamlarının zor kurgulandığı durumlarda artırılmış gerçekliğe dayalı çalışmaların fayda sağladığı bilinmektedir (Kandalaft ve diğerleri, 2012; Pan & Hamilton, 2018). Dolayısıyla, bu çalışmada da güvenliği ilgilendiren ve acil durumlarda neler yapılması gerektiğini canlandıran ortamlar için artırılmış gerçeklik uygulamaları tercih edilmiştir.

Bu çalışma kapsamında, otizmli çocukların güvenliğini sağlayabilmek ve acil durumlarda neler yapmaları gerektiği konusunda bilgilendirmek için oyun-tabanlı özgün bir öğrenme ortamı geliştirilmiştir. Bu çerçevede, trafikte ilk yardımı ilgilendiren temel konuların otizmli çocuklarca daha kolay anlaşılmasına destek olmak amacıyla çeşitli teknolojik bileşenleri bir araya getiren bir uygulama oluşturulmuştur. Uygulama, otizm spektrum bozukluğu gösteren çocukların ilk yardım eğitimini desteklemeyi amaçlamaktır. Çalışmanın çıktısı bu alanda

yapılmış sade kitap uygulamalarından farklı olarak artırılmış gerçeklik uygulamasını "Pop-Up" yöntemiyle tasarlanmış etkileşimli ve dinamik sayfalardan oluşan bir kitap ile entegre etmekte, tamamı uygulamaya özgü hazırlanan video ve canlandırmalar içermektedir. Buna ek olarak, uygulamada eğitimin sürekliliğini sağlamak için bir Web tabanlı veli katılım sistemi sunulmaktadır. Özel eğitimdeki motivasyon ve tekrar edebilme faktörlerine yönelik bireyin düzeyine uygun özgün animasyonlar, eğitsel oyunlar ve seslendirmeler bulunmaktadır. Geneli itibariyle, bu proje kapsamında sanal sunumla gerçekliğin iç içe olduğu bir öğretim ortamı otizmli çocuklara özel olarak hazırlanmış ve bir ders destek materyali olarak yerinde uygulanmıştır.

Çalışmanın temel araştırma soruları: 1) Trafikte ilk yardımı ilgilendiren müfredattaki temel konular çerçevesinde hedef grubun ihtiyaç duyduğu öğretimi destekleyen bir materyal/uygulama nasıl olmalı? 2) Belirlenen ihtiyaçlara göre geliştirilen örnek bir materyal uygulaması için öğrencilerin hedef görevleri tamamlaması öğretmenin bakış açısıyla ne gibi zorluklar içeriyor?

Etkileşimli Oyun Kitapları

Günümüzde etkileşimli oyun ortamlarının oluşturulması için video, ses ve çeşitli animasyonlarla artırılmış gerçeklik teknolojisini birleştiren dijital kitaplar geliştirilmektedir. Bu ortamların öğrenmede güçlük çeken öğrencilerin eğitimine katkı sağlayabildiği bilinmektedir (Shamir & Lifshitz, 2013). Etkileşimli oyunlar otizm spektrum bozukluğu gösteren öğrencilerin öğrenme sürecini destekleyebilmekte, ilgilerini çekmekte ve istenilen becerilerin kazandırılmasına yardımcı olabilmektedir (Erişti ve diğerleri, 2017). İstenildiğinde tekrar oynanabilen veya bir bütüne ait kalan parçaların tamamlanmasına teşvik eden uygulamalar ("sosyal sistemleştirme") otizmli öğrenciler için kullanılacak etkin materyallerin tasarımında kullanılabilmektedir (Baron-Cohen ve diğerleri, 2009). Özel eğitimin temel kriterlerinden biri kabul edilen, öğrenme ortamının öğretilecek nesnelerle zenginleştirilmesi prensibi (TOV, 2008) etkileşimli oyun kitapları ve ilişkili olabilecek entegre materyaller ile sağlanabilir. Bu kapsamında, trafikte güvenliği ilgilendiren temel konular bir senaryo dahilinde video, ses ve animasyonlarla entegre çalışacak şekilde bir "etkileşimli" kitap haline getirilmiştir.

Artırılmış Gerçeklik Uygulamaları

Artırılmış gerçeklik, fiziksel dünyadaki belli objeleri tanıma ve algılama özellikleri kullanılarak, sanal nesnelerin gerçek görüntüler üzerine bindirilmesini sağlamakta ve ses, video veya fotoğraf gibi unsurlarla uygulama alanını ve kullanıcı deneyimini zenginleştirmektedir (Chen ve diğerleri, 2019). Günümüzde mobil cihazlarla artırılmış gerçeklik uygulamalarının eğitimde kullanımı oldukça yaygın hale gelmiştir (Avcı ve diğerleri, 2019; Çakir ve diğerleri, 2015; Demirer & Erbaş, 2015; Somyürek, 2014). Otistik çocukların eğitiminde sık tekrarın faydalı olduğu bilinmektedir (Baron-Cohen ve diğerleri, 2009; TOV, 2008). Buna bağlı olarak, bazı gerçek koşulların yeniden sağlanamadığı ya da eğitim amaçlı deneme ortamlarının yeniden kurulmasının zor olduğu durumlarda artırılmış gerçekliğe dayalı çalışmaların fayda sağladığı görülmektedir (Cakir & Korkmaz, 2019; Kandalaft ve diğerleri, 2012). Bu çalışmada da tekrarlanabilir ortamların oluşturulmasındaki kısıtların önüne geçebilmek için artırılmış gerçeklikten yararlanılmıştır.

Veli Katılımının Önemi

Otizmli öğrencilere verilen eğitimin sadece okulla sınırlı kalmamasına, evlerinde ebeveynlerinin kontrolünde bu eğitime devam edebilmelerine vurgu yapılmaktadır (TOV, 2008). Bu kapsamda, öğrencilerin eğitim-öğretim süreçlerine destek verebilecek uygulamalar evde geçirdikleri zamanlarda da velilerinin katılımıyla devam

ettirilebilir (Mazon ve diğerleri, 2022). Bu aynı zamanda öğrencilerin bir nedenle okula gidemediği durumlarda öğretim faaliyetlerinin devamlılığını da desteklemektedir (Álvarez-Guerrero ve diğerleri, 2021). Bu amaçla, bu çalışma kapsamında da öğrencilerin ihtiyaçlarına uygun öğrenme materyallerinin hem ek maliyet olmadan hem de okul dışında, zamandan bağımsız olarak yararlanılabileceği veli rehberliğinde kullanılan bir ortam oluşturulmuştur.

Yöntem

Bu çalışmada, yazılım geliştirme ve gerçek ortam üzerinden değerlendirme süreçlerini içeren disiplinler-arası bir yaklaşım izlenmiştir. Yazılım bileşenlerinin üretilmesinde analiz, tasarım, geliştirme, uygulama ve değerlendirme aşamaları izlenmiştir (Branch, 2009; Rosenberg, 1982). Kullanılan araştırma yöntemi ise görüşme ve gözlem tekniklerini birlikte kullanan bir durum çalışmasıdır (Subaşı & Okumuş, 2017). Bu çalışma kapsamındaki durum otizm spektrum bozukluğu gösteren öğrencilere yönelik bir uygulamanın geliştirilmesi ve bu uygulamayla yapılan öğretim etkinlikleriyle sınırlıdır. Çalışmanın öncesinde Etik Kurul onayı, kurum ve veli izinleri alınmıştır. Uygulamanın teknolojik bileşenleri, bileşen özellikleri ve etkileşim yapıları otizmli bireylerin eğitimi için yeterlilik sertifikasına sahip öğretmenlerle (N=4) ve öğretim teknolojileri alanında uzman öğretim elemanlarıyla (N=4) yapılan yarı-yapılandırılmış görüşmelerle belirlenmiştir (Creswell, 2013). Geliştirilen bileşenlerin uygulanması ise otizm spektrum bozukluğu gösteren öğrencilerle (N=4) öğretmenlerinin rehberliğinde sınıfta gerçekleştirilmiştir. Katılımcılar, durum çalışmasının yapıldığı dönemde uygun olan ve çalışmaya dahil olmayı kabul eden kişilerden seçilmiştir (Sedgwick, 2013).

Katılımcılar

Uygulama, bir özel eğitim kurumunda yaşları 8 ila 19 arasında değişen otizm spektrum bozukluğu gösteren dört erkek öğrenci ile öğretmenleri rehberliğinde gerçekleştirilmiştir. Öğrencilerin özel gereksinim düzeyi (ÖGD) Belirgin, Orta ve Hafif olmak üzere farklılık göstermektedir. Sınıf-içinde gerçekleştirilen uygulama süreleri ortalama 27 dakikadır. ÖGD bilgileri cinsiyetleri ve uygulama kullanım süreleri Tablo 1'de sunulmuştur. ÖGD bilgileri engelliler için bilgilendirme rehberinde verilen mevzuata (T.C. Aile, Çalışma ve Sosyal Hizmetler Bakanlığı, 2019) uygun raporlanmıştır.

Tablo 1. Öğrencilerin Demografik Bilgileri

Katılımcı No	Cinsiyet	ÖGD	Yaş	Süre (dakika)
1	Erkek	Belirgin	19	30
2	Erkek	Belirgin	9	35
3	Erkek	Orta	8	20
4	Erkek	Hafif	10	22

Öğrencilerin her biri ardışık şekilde öğretmeni ile uygulama yapmış, araştırmacılar bu süre boyunca gözlem notu tutmuştur. Uygulama sonunda hedef görev tamamlama çizelgesi (Ek.1) ilgili öğretmenlerin görüşleri alınarak uzman öğretmen (Öğretmen 1) tarafından doldurulmuştur. Öğretmenlerin tamamı Millî Eğitim Bakanlığı onaylı özel eğitim sertifikasına sahiptir. Demografik bilgileri Tablo 2'de sunulmuştur.

Tablo 2. Öğretmenlerin Demografik Bilgileri

No	Unvan	Eğitim	Cinsiyet	Yaş	Deneyim (yıl)
1	Özel Eğitim Öğretmeni	Yüksek Lisans	Kadın	26	4
2	Özel Eğitim Öğretmeni	Üniversite	Kadın	57	25
3	Özel Eğitim Öğretmeni	Üniversite	Kadın	39	16
4	Özel Eğitim Öğretmeni	Üniversite	Kadın	25	4

Hem teknolojik bileşenlerin belirlenmesinde hem de uygun öğretim materyallerinin geliştirilmesinde özel eğitim uzmanlarının yanı sıra Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) alanında uzman, artırılmış gerçeklik, web uygulamaları, materyal geliştirme ve öğrenme güçlüğü çeken öğrencilere yönelik akademik çalışmaları olan dört alan uzmanı ile görüşülmüştür. Uygulamanın akışı, kullanılacak materyaller ve öğretim tasarımı bu aşamada belirlenmiştir. Akademisyenlerin demografik bilgileri ise Tablo 3'te listelenmiştir.

Tablo 3. Uzmanların Demografik Özellikleri

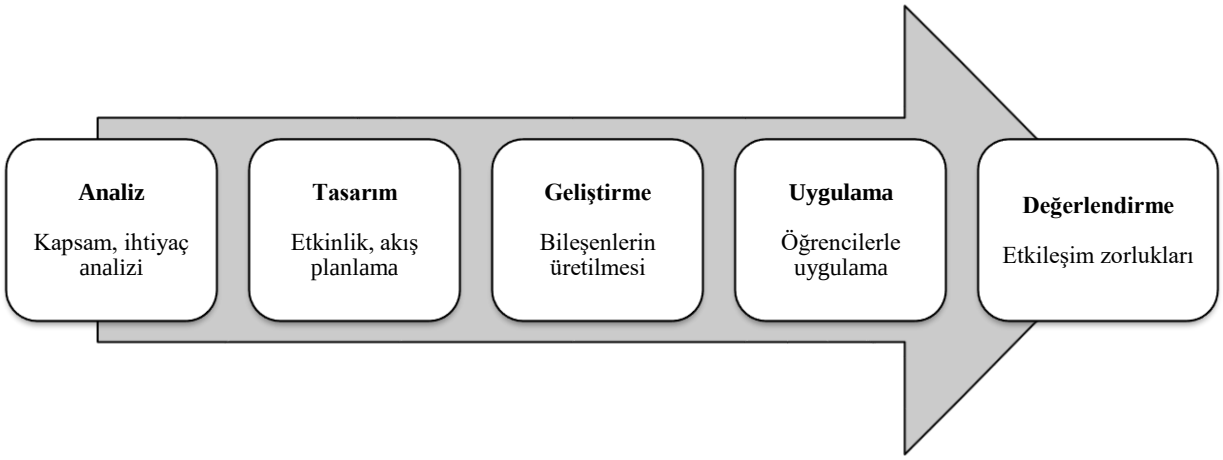
No	Unvan	Bölüm	Cinsiyet	Yaş	Deneyim (yıl)
1	Doçent	BÖTE	Erkek	46	21
2	Dr. Öğr. Üyesi	BÖTE	Erkek	33	9
3	Dr. Öğr. Üyesi	BÖTE	Erkek	34	11
4	Öğretim Görevlisi	BÖTE	Erkek	39	21

Veri Toplama Araçları

Uygulamada olması gereken bileşenler görüşme yoluyla belirlenmiştir. Bu süreçte iki adım izlenmiştir. İlk adımda, öğretmenlere "*Trafikte ilk yardımı ilgilendiren müfredattaki temel konular çerçevesinde hedef grubun ihtiyaç duyduğu öğretimi destekleyen bir materyal/uygulama nasıl olmalı?*" sorusu yöneltilmiştir. Alınan cevapların derinlemesine anlaşılması için duruma göre ek sorular sorulmuştur. Ortaya çıkan ihtiyaç analizine karşılık gelebilecek teknolojik bileşenlerin seçimi ve uygulanabilirliği için ise uzmanların görüşleri alınmıştır. Nihai uygulama, öğrencilerin öğrenme stillerine ve literatüre göre düzenlenmiştir. Öğretmen 1 tarafından diğer öğretmenlerin de görüşü alınarak bir hedef görev tamamlama çizelgesi oluşturulmuştur. Bu sayede, öğrencilerin belli görevleri ne ölçüde tamamlayabildikleri öğretmenin bakış akışından değerlendirilmiştir. Bu çizelgedeki görevler/etkinlikler, önerilen uygulamadaki etkileşimlere göre başlıklandırılmıştır. Bu amaçla, toplam 18 görev tanımı içeren likert-tipte değerlendirme skalasından yararlanılarak 1 ila 5 arasında puanlama yapılmıştır (F. Antonak & Livneh, 2000; Likert, 1932). Ayrıca gözlemlenen etkileşim zorlukları da yine bu çizelgenin altına not edilmiştir.

Teknolojik Bileşenler İçin Geliştirme Süreci

Uygulamada kullanılan içerik ve teknolojik bileşenlerin seçimi literatür taramasına ve müfredat içinde dördüncü sınıf Trafik bölümüne uygun şekilde uzmanların ve öğretmenlerin görüşlerine dayanılarak düzenlenmiştir. Teknolojik bileşenler, tamamı çalışmaya özgün olarak geliştirilen bir adet etkileşimli kitap, cep telefonu uygulaması ve web yazılımı içermektedir (Ek.2). İzlenen aşamalar (Branch, 2009; Rosenberg, 1982) Şekil 1'de gösterilmektedir.



Şekil 1. Teknolojik Bileşenlerin Üretilmesinde İzlenen Aşamalar

Teknolojik bileşenlerin oluşturulmasında, artırılmış gerçeklik altyapısını oluştururken Unity oyun motoru (Kim ve diğerleri, 2014) üzerinde Vuforia Engine (Xiao & Lifeng, 2014) yazılım geliştirme kiti, Web tabanlı veli katılım sisteminde HTML5, Javascript, MySQL ve PHP teknolojileri (Stoeva, 2014), üç boyutlu modellemelerde ise 3D Studio MAX (YANG ve diğerleri, 2004) kullanılmıştır. Mobil uygulamanın geliştirme sürecinde üç temel adım izlenmiştir. İlk adımda görsel taslaklar (storyboard) eşliğinde ortam materyalleri hazırlanmıştır. İkinci adımda QR kodları üretilmiş ve akışa uygun Vuforia Engine ilişkilendirmesi yapılmıştır. Son adımda da etkileşim modülleri C# programlama dili ile kodlanmıştır. Web uygulamasının geliştirilmesinde ise ilişkisel veri tabanı kullanılarak öğretmen, veli, öğrenci ve aktivite bilgileri eşleştirilmiştir. Dinamik bir web arayüzü üzerinden her kullanıcının (velilerin ve öğretmenlerin) tanımlı rollerine uygun çalışan bir sistem geliştirilmiştir. Mobil uygulamanın Android ve iOS temelli testleri ve sınıf-içi uygulamalar Sony Xperia 5 ve Apple iPhone 8 Plus üzerinden gerçekleştirilmiştir.

Etkileşimli kitap kendi içinde video, ses, metin ve animasyon gibi diğer alt bileşenleri harekete geçirebilecek bağlantıları barındırmaktadır. Tüm bileşenler, geliştirme anında alınan geri bildirimlere göre şekillenmiştir. Analiz aşamasında otizmli çocukların özellikleri, öğrenme stilleri, bireysel ve sosyal özellikleri değerlendirilmiştir. Tasarım aşamasında etkileşimlerin akışı bir oyun senaryosu dahilinde planlanmıştır. Dahil edilmesi hedeflenen etkinlikler de yine bu aşamada belirlenmiştir. Geliştirme aşamasında tasarım sürecinde belirlenen senaryo akış planına ve etkinlik tasarımlarına göre fonksiyonlar oluşturulmuş, çizimler ve animasyonlar yapılmıştır. Uygulama aşamasında ise tüm bileşenler bir araya getirilerek gerçek öğrenme ortamında denemiştir. Değerlendirme aşamasında uygulamayı iyileştirebilmek ve revize edebilmek için öğretmenlerin rehberliğinde çalışılmıştır. Her aşamada, iyileştirme gerektiren noktaların belirlenmesi ve çıktı kalitesinin sağlanması için uzmanlardan geri bildirim alınmıştır. Bu çalışma, 2020 yılı içinde Ocak-Nisan aylarında gerçekleştirilmiştir.

Veri Analizi

Yazılım bileşenlerine ait ihtiyaç analizi nitel araştırma yöntemi temel alınarak yürütülmüştür. Bu amaçla, görüşme yolu ile toplanan veriler önce konularına göre parçalara ayrılmış, daha sonra her bir parça vurgulanan ortak başlıklara göre gruplanmış ve analiz edilmiştir (Creswell, 2013). Bu süreçte, ulaşılmak istenen, öğretmenlerin kendi deneyimlerine göre sınıf içinde bekledikleri "*Trafikte ilk yardımı ilgilendiren müfredattaki temel konular*"

çerçevesinde yer alabilecek etkileşimleri anlamak olmuştur. Bu etkileşimlerin her biri uzmanların görüşleri alınarak bir teknolojik bileşen ile eşleştirilmiş ve ardından ürüne dönüştürülmüştür. Görüşmeleri yöneten araştırmacının hem ilgili teknolojilerde hem de görüşmeye-dayalı araştırma alanında sahip olduğu deneyimler bu araştırmanın şekillenmesinde etkili olmuştur (Sirris, 2022).

Bulgular

Çalışma kapsamında, öğretmenlerle yapılan görüşme analizinin sonuçları geliştirme yapılacak ürün bileşenlerini belirlemiştir. Geliştirilen ürün bileşenlerinin uygulama sonuçları ise gerçek ortamda ve öğretmenlerin gözetiminde test edilmiş, hedeflenen görevlerin tamamlanma durumları katılımcı bazlı raporlanmıştır. Bu kapsamda, bu bölümde çalışma sonunda elde edilen analiz sonuçları, geliştirilen ürün bileşenleri ve uygulama değerlendirme aşamasına ilişkin gözlem notlarından elde edilen çıkarımlar yer almaktadır.

Uygulamayı geliştirilmeye başlamadan önce otizmli çocukların özellikleri, öğrenme stilleri, bireysel ve sosyal özellikleri literatüre göre incelenmiş ardından katılımcılarla yapılan görüşmelerde verilen cevaplar birlikte değerlendirilmiştir. Bu amaçla yöneltilen "*Trafikte ilk yardımı ilgilendiren müfredattaki temel konular çerçevesinde hedef grubun ihtiyaç duyduğu öğretimi destekleyen bir materyal/uygulama nasıl olmalı?*" sorusu ve verilen cevaplara göre derinleşen konuşmalarda öğretmenlerden alınan cevaplar beş konu altında toplanmıştır. Bu bağlamda, ihtiyaç analizini ilgilendiren şu çıkarımlar yapılmıştır:

- Etkileşim eksikliği: Öğretmenler (*n*=4) trafikte ilk yardımı ilgilendiren temel konuların sadece basılı kartlarla anlatıldığını ve etkileşim eksikliğinin olduğunu belirtilmiştir. Buna örnek olarak, bir öğretmen "*... bu kartlardan konuyla ilgili resimleri (ilk yardım çantası kastediliyor) görüyorlar, ama onlarla bir uygulama yapmak her zaman mümkün olmuyor*" diyerek etkileşimli bir öğretim ortamının gerekliliğini vurgulamıştır. Tüm öğretmenler ders anında öğrencilerin ilgisini çekecek etkileşimli oyunlara ihtiyaç olduğunu düşünmektedir.
- Kavram kargaşası: Bazı öğretmenler (*n*=2) otizmli çocukların ambulans, polis ve itfaiye kavramlarını anlamada veya ayırt etmede zorluk yaşadıklarını ve bu türde kavramları gerçek ortamda göstermenin her zaman mümkün olmadığını dile getirilmiştir. Bir öğretmen "*çoğu zaman ambulans, polis ve itfaiye araçlarını (kartlarını) karıştırıyorlar veya tanıyamayabiliyorlar, … bazen pencereden bir ambulansın geçişini gösterebiliyoruz, ama bu elbette ders anına denk gelmeyebiliyor veya nadiren…*" diyerek kavramları karşılaştırarak gerçek ortamda gözlemlemenin zorluğunu belirtmiştir.
- Dijital materyal eksikliği: Öğretmenler (*n*=4) ders anında kullanabilecekleri dijital materyalleri bulmakta zorluk yaşadıklarını vurgulamıştır. Bir öğretmen "*İnternet üzerinden bir oyun seçsek dahi müfredata uygun olmayabiliyor veya özel eğitim için tasarlanmamış olabiliyor*" diyerek, uygun materyal bulmanın zorluğuna dikkat çekmiştir. Bu duruma ek olarak, başka bir öğretmen öğrenciye göre uygulamanın farklı olabileceğine değinirken "*… bu türde materyallerin hem dijital hem de basılı ortamda olması iyi olur*" diyerek somutlaştırmanın gerekliliğini vurgulamıştır.
- Veli katılımı: Öğretmenlerin bazılarına (*n*=3) göre, öğrencilerin evde de çeşitli sınıf-içi etkinliklere devam etmesi faydalı bulunmuştur. Örneğin, bir öğretmen, "*... çocuklar bir boyamanın benzerini veya aynısını evde de yapabilir*" demiştir. Benzer şekilde, bir başka öğretmen, "*Bazı materyalleri sağlarsak, veliler isteğe bağlı tekrar amaçlı yararlanabilir*" diyerek "*veli katkılarının*" yapılacak paylaşımlarla

öğretimi pekiştireceğini belirtmiştir. Özetle, velilerin eğitimin sürekliliğini sağlayacak konuyla ilgili materyallere sahip olması ve sürece katılımı önemli bulunmuştur.

İhtiyaç analizinin sonuçları, literatürdeki güncel uygulamalar ışığında değerlendirilmiştir. Öneri olarak, artırılmış gerçeklik-tabanlı hem hikâye anlatımı hem de üç boyutlu canlandırma ve etkileşim içeren bir materyal için uzman öğretim elemanlarının görüşleri alınmıştır. Bu görüşlere dayanarak uygulamada kullanılabilecek teknolojik bileşenler seçilmiştir. Kapsama dahil edilen konu başlıkları şunlardır: 1) İlk yardım çantasındaki malzemeler; 2) Acil durumda yapılması gereken müdahaleler; 3) Olaylara göre acilen aranması beklenen telefon numaralarıdır. Tüm konuların bir kitap üzerinden sunulması, bir etkileşim, hikâye ya da müzik ile birleştirilmesi düşünülmüştür. Bu kapsamda yapılan geliştirme sonucu ortaya çıkan bileşenler şunlardır:

- Etkileşimli kitap: Bu bileşende, vurgulanması istenen her bir kavram bir çizimle canlandırılmıştır. Öğrencinin objeleri sürükleyip tanımlı alana bırakarak veya doğru parçalarla eşleştirerek kavramları ayırt ettiğini göstermesi istenmiştir. Bu bileşen öğretmenler tarafından vurgulanan "Etkileşim eksikliği" ve "Kavram kargaşası" konularıyla ilişkilendirilmiştir.
- Artırılmış gerçeklik uygulaması: Etkileşimli kitaptaki kavramlar istenildiğinde bir barkod üzerinden harekete geçirilebilen video, ses veya animasyon-içerikli anlatımlarla desteklenmiştir. Bu bileşene yönelik, öğretmenin rehberliğinde kullanılması amaçlanan bir mobil uygulama geliştirilmiştir. Öğrencilerden duyduğunu gösterebilmesi ve dinlediğini tekrar edebilmesi beklenirken bazı yerlerde konuyu pekiştiren hikayeleri izlemesi istenmiştir. Bu bileşen başta "Dijital materyal eksikliği" olmak üzere "Etkileşim eksikliği" ve "Kavram kargaşası" konularıyla ilişkili görülmüştür.
- Veli katılım sistemi: Bileşenlerin dijital ortamda erişilebileceği bir Web tabanlı uygulama önerilmiştir (Ek-2). Uygulamada, öğretmenin izin verdiği konu etkinliklerine velilerin parça-parça (haftalık) veya bütün halde inceleyebilmesine ve materyalleri indirip kullanabilmesine olanak verilmiştir. Ayrıca, velilerin bu etkinlikler için çocuklarının tutumunu puanlayabilmesi ve öğretmene bilgi verebilmesi mümkün kılınmıştır. Önerilen bu sistem "Veli katılımı" ihtiyacına yönelik düşünülmüştür.

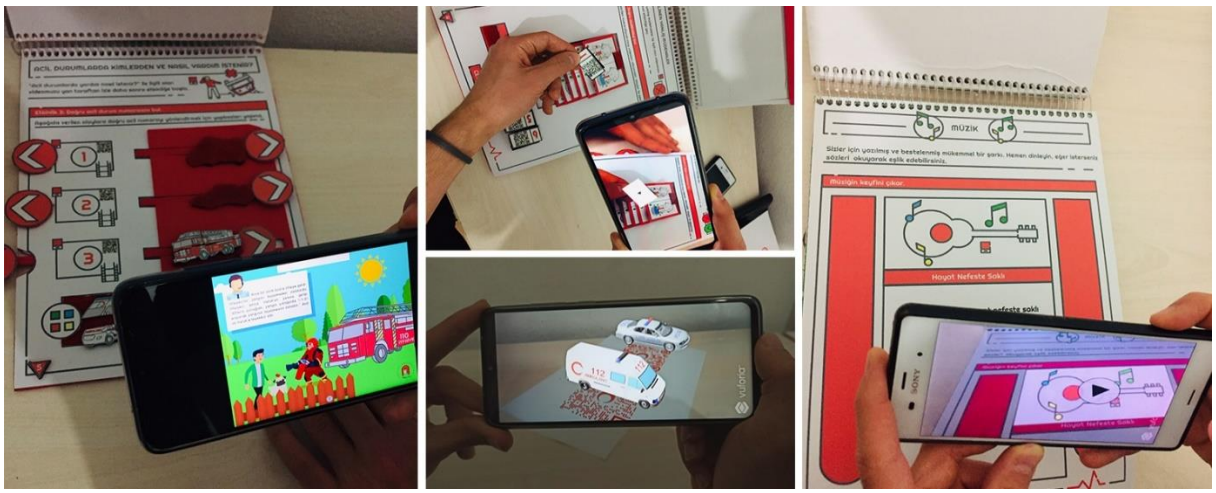
Mobil uygulama etkileşimlerinden örnek görüntüler Şekil 2'de, kitap etkileşimlerinden örnek görüntüler ise Şekil 3'te gösterilmektedir. Geliştirilen bileşenleri içeren bir uygulama otizm spektrum bozukluğu gösteren öğrencilerce ilgili öğretmenlerinin eşliğinde kullanılmıştır. Oturumlar bireysel gerçekleştirilmiştir. Bu süreçte, Öğretmen 1 tarafından hedef görevlerin tamamlanma düzeyleri not edilmiştir. Hiç tamamlanmayan görevler için 1 puan verilirken, tamamı gerçekleştirildiği düşünülen görevlere 5 puan verilmiştir. Hedef görevlerin her bir katılımcı öğrenci tarafından tamamlanma düzeyleri Tablo 4'te listelenmiştir.

Tablo 4. Hedef görev tamamlama raporu

No	Görev/Etkinlik	Katılımcı 1	Katılımcı 2	Katılımcı 3	Katılımcı 4	Toplam
1	Sayfaları dikine bir şekilde çevirir.	2	3	4	5	14
2	Dergide verilen yönergeleri öğretmen yardımı ile uygular.	2	3	3	4	12
3	Sayfalardaki "pop-up" bölümleri açar.	2	2	4	4	12
4	Araçları tanır.	2	1	2	4	9
5	Telefon uygulamasını öğretmen rehberliğinde elinde tutar.	1	2	3	5	11

6	Dergi içindeki şarkıyı dinler.	1	1	3	3	8
7	Dergi içindeki şarkıya eşlik eder.	1	1	1	2	5
8	Dergi içindeki animasyon ve videoları dikkatle izler.	3	2	4	4	13
9	Birinci etkinlikteki malzemeleri tanır.	3	2	3	5	13
10	Bağlantı bantlarını doğru yerlere yapıştırır.	2	3	3	4	12
11	Cevabının doğru veya yanlış olduğunu anlar. (Duyduğu veya gördüğü geri bildirimi anlar)	2	2	3	5	12
12	İkinci etkinlikteki ses kayıtlarını doğru bir şekilde resimleri ile eşleştirir.	1	2	2	3	8
13	Resim galerisindeki resimleri elleri ile çekerek değiştirir.	2	3	3	4	12
14	İkinci doğru ve yanlış müdahaleleri kavrar.	1	2	1	3	7
15	Üçüncü etkinlikteki hikayeleri sıkılmadan izler.	2	2	2	2	8
16	Hikayeleri doğru araba ile eşleştirir.	2	2	3	5	12
17	Karışık verilen araba parçalarını birleştirir.	1	1	2	3	7
18	Kaydırma oklarını kullanarak arabaları oynatır.	3	3	4	5	15
	Sütun toplamları:	33	37	50	70	190

Tablo 4'e göre toplamda en fazla alınabilecek puan 90 olabilmekteydi. Bu puana en çok yaklaşan öğrenci Katılıcı 4 olurken, en az puanı toplayan öğrenci Katılımcı 1 olmuştur. Katılımcıların genel olarak uygulamadaki objeleri kaydırma, çekme, yapıştırma gibi işlemlere daha yatkın oldukları, eşleştirme ve birleştirme işlemlerinde ise zorluk yaşadıkları görülmüştür. Öğrencilerin şarkıları ve hikayeleri genel olarak dinledikleri ama eşlik etmede kısmen daha çekingen kaldıkları görülmüştür. Uygulama anında aldığımız düzeltme notlarına göre, objelerin genel olarak daha büyük ve seçilebilir kılınması, birleştirme gerektiren nesnelerin ise daha az sayıda olması gerektiği anlaşılmıştır. Veli katılım sistemi tüm etkinliklere yönelik öğretmen ve ebeveynler için sınıf-içi uygulamadan önce erişilebilir hale geliştirilmiş, ancak bu çalışma kapsamında etkinliği değerlendirilememiştir.



Şekil 2. Mobil Uygulama Etkileşimlerinden Örnek Görüntüler

Şekil 3. Kitap Etkileşimlerinden Örnek Görüntüler

Tartışma ve Sonuç

Otizm spektrum bozukluğu gösteren öğrenciler için etkileşimli oyun ortamlarını şekillendirebilecek ihtiyaçlar bir durum çalışması kapsamında analiz edilmiştir. Sınıf-içi aktivitelerin etkileşim çeşitliliğinde, öğrenciler tarafından bazı kavramların anlaşılmasında ve ayırt edilmesinde, öğretimi destekleyecek uygun dijital materyallerin sayısında eksiklikler olduğu anlaşılmıştır. Bu durumlara ek olarak, ebeveynlerin öğretim faaliyetlerine destek sağlayabileceği ortamlara ihtiyaç olduğu görülmüştür. Bu kapsamda, bir etkileşimli kitap ve bu kitap ile bütünleşik çalışabilen artırılmış gerçeklik uygulaması ile veli katılımını destekleyecek bir web-tabanlı sistem önerilmiştir. Öğretmenler konuları hikâye tabanlı etkileşimli bir oyun kitabı üzerinden anlatmıştır. Etkileşimler bir cep telefonu yardımıyla öğrenciler tarafından öğretmenleri rehberliğinde gerçekleştirilmiştir. Bu süreçte, öğrencilerin yönergeleri eğlenerek takip ettikleri gözlemlenmiştir. Uygulamaya rehberlik eden öğretmenlerin görüşlerine göre, otizm spektrum bozukluğu gösteren öğrenciler için trafikte ilk yardımı ilgilendiren temel konular daha ilgi çekici hale gelmiştir.

Hedef görev tamamlama raporu (Tablo 4) bir bütün olarak incelendiğinde, görev zorluklarının anlaşılmasında yaş bilgisinin tek başına açıklayıcı olmadığı, özel eğitime ihtiyaç düzeyinin de dikkate alınması gerektiği ortaya çıkmıştır. Otizm spektrum bozukluğu gösteren öğrenciler, uygulamanın kullanımı sırasında kullanılabilirlik ile ilgili görevlerde (Ör. Görev 1, Görev 2, Görev 3, Görev 13, Görev 18) daha üst düzey performans gösterirken, entelektüel çaba gerektiren görevlerde (Ör. Görev 4, Görev 7, Görev 12, Görev 14, Görev 17) göreceli olarak daha alt düzey performans sergilemiştir. Bu sonuç, bir taraftan uygulamanın otizm spektrum bozukluğu gösteren öğrenciler için kullanılabilirliğinin yeterli düzeyde kabul edilebileceğini ima ederken, diğer taraftan uygulamada yer alan entelektüel görevler için veli veya öğretmen desteğinin gerekliliğine işaret etmektedir. Ayrıca, öğrenciler geliştirilen uygulamada yer alan Görev 8, Görev 9 ve Görev 13 gibi bazı görevleri benzer performansla yerine getirirken diğer görevlerde (Ör. Görev 4 ve Görev 5) farklı performanslar göstermiştir. Bu da öğrencilerin bireysel farklılıklarıyla ilişkili görülebilir ve bu tür uygulamaların kullanımında sunulacak öğretmen veya veli desteğinin öğrencinin bireysel özellikleri dikkate alınarak veya daha fazla bireyselleştirilerek sunulması için fikir verebilir.

Elde edilen bulgular, otizm spektrum bozukluğu gösteren öğrenciler için herkese uyan tek bir (“one-size-fits-all”) yaklaşımın uygun olmadığını göstermektedir. Bir uygulama tamamen otizm spektrum bozukluğu gösteren öğrencilerin özellikleri temel alınarak geliştirilmiş olsa bile bireyselleştirilmiş destek önemlidir. Otizmli

öğrencilerin eğitim olanaklarını iyileştirmek için artırılmış gerçeklik tabanlı uygulamaların diğer konu alanlarında da araştırılması ve diğer akademik kazanımlar için genişletilmesi önerilmektedir.

Bu çalışma, bir örnek durum incelemesi ile sınırlıdır. Çalışmada raporlanan literatür, geliştirilen uygulama ve elde edilen bulgular tüm popülasyon için gerçek bir temsil olmayabilir. Görüşülen kişilerin, soruları mümkün olan en iyi şekilde cevapladıkları varsayılmıştır. Bulguları tekrarlamak ve otizmli öğrencilere yönelik tasarım ve uygulama gereksinimlerini açıklığa kavuşturmak için daha büyük gruplarla yürütülecek daha fazla çalışmaya ihtiyaç vardır.

Teşekkür ve Bilgilendirme / Acknowledgements

Çalışmanın gerçekleşmesinde katkılarından dolayı özel eğitim kurumuna, öğretmenlere, öğrencilere ve öğretim teknolojileri uzmanlarına teşekkür ederiz. Çalışmanın bir bölümü TÜBİTAK-2242 araştırma projeleri kapsamında "Can Kurtarın" ismiyle sunulmuş ve Ankara Bölge Birinciliği ve Türkiye Geneli Teşvik ödüllerine değer bulunmuştur.

Yayın Etiği Bildirimi / Research Ethics

Yazarlar çalışmanın etik dışı bir sorunu olmadığını, araştırma ve yayın etiği konularının gözlemlediklerini beyan etmektedir. / The authors declare that the research does not have an unethical problem and that they observe the topic of research and publication ethics.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Makalenin yazımı ve metodun geliştirilmesi birinci yazar tarafından yapılmıştır. Tüm yazarlar uygulama, analiz ve sonuçların ortaya çıkarılmasında görev almıştır. Tüm yazarlar makaleyi okudu ve onayladı. / The first author developed the method and wrote the manuscript. All authors are involved in the implementation, analysis and revealing of the results. All authors read the manuscript and approved it.

Çıkar Çatışması / Conflict of Interest

Yazarlar herhangi bir çıkar çatışması olmadığını beyan etmektedir. / The authors declare no conflict of interest.

Fon Bilgileri / Funding

Bu çalışma için herhangi bir fondan yararlanılmamıştır. / No funding was used for this study.

Etik Kurul Onayı / The Ethical Commitee Approval

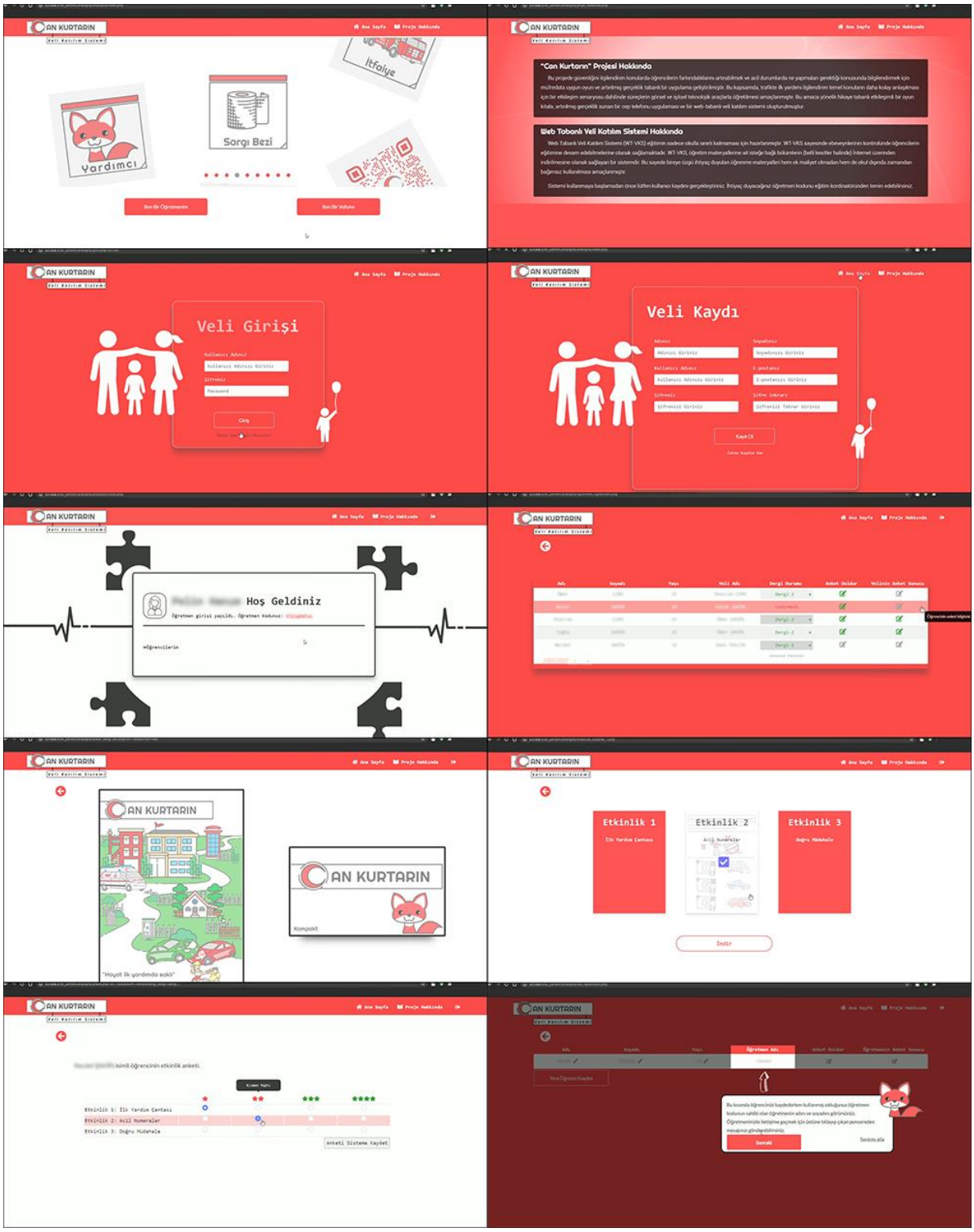
Bu çalışma yürütülmeye başlamadan önce etik kurul onayı alınmıştır. / Ethics committee approval was obtained before the study was conducted.

Ekler / Appendices

Ek 1. Hedef görev tamamlama çizelgesi

Tarih:						
Uygulanan Okul:						
Uygulama No:						
	Görevler/Etkinlikler	Çok Zor (1)	Zor (2)	Orta (3)	İyi (4)	Çok İyi (5)
1	Sayfaları dikine bir şekilde çevirir.					
2	Dergide verilen yönergeleri öğretmen yardımı ile uygular.					
3	Sayfalardaki pop-up bölümleri açar.					
4	Araçları tanır.					
5	Telefon uygulamasını öğretmen rehberliğinde elinde tutar.					
6	Dergi içindeki şarkıyı dinler.					
7	Dergi içindeki şarkıya eşlik eder.					
8	Dergi içindeki animasyon ve videoları dikkatle izler.					
9	Birinci etkinlikteki malzemeleri tanır.					
10	Bağlantı bantlarını doğru yerlere yapıştırır.					
11	Cevabının doğru veya yanlış olduğunu anlar. (Duyduğu veya gördüğü geri bildirimi anlar)					
12	İkinci etkinlikteki ses kayıtlarını doğru bir şekilde resimleri ile eşleştirir.					
13	Resim galerisindeki resimleri elleri ile çekerek değiştirir.					
14	İkinci doğru ve yanlış müdahaleleri kavrar.					
15	Üçüncü etkinlikteki hikayeleri sıkılmadan izler.					
16	Hikayeleri doğru araba ile eşleştirir.					
17	Karışık verilen araba parçalarını birleştirir.					
18	Kaydırma oklarını kullanarak arabaları oynatır.					
Karşılaşılan zorluklar nelerdi? (Gözlem notları)						

Ek 2. Veli Katılım Sisteminden Örnek Görüntüler



Kaynakça / References

Álvarez-Guerrero, G., López de Aguileta, A., Racionero-Plaza, S., & Flores-Moncada, L. G. (2021). Beyond the school walls: Keeping interactive learning environments alive in confinement for students in special education. *Frontiers in Psychology*, *12*, 662646. https://doi.org/10.3389/fpsyg.2021.662646

Avcı, Ş. K., Çoklar, A. N., & İstanbullu, A. (2019). Üç boyutlu sanal ortamlar ve artırılmış gerçeklik uygulamalarının öğrenme başarısı üzerindeki etkisi: Bir meta-analiz çalışması. *Eğitim ve Bilim*, *44*(198). http://dx.doi.org/10.15390/EB.2019.7969

Baron-Cohen, S., Ashwin, E., Ashwin, C., Tavassoli, T., & Chakrabarti, B. (2009). Talent in autism: Hyper-systemizing, hyper-attention to detail and sensory hypersensitivity. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *364*(1522), 1377–1383. https://doi.org/10.1098/rstb.2008.0337

Bozkurt, S. S. (2017). Özel eğitimde dijital destek: Yardımcı teknolojiler. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, *3*(2), 37–60.

Branch, R. M. (2009). *Instructional design: The ADDIE approach*. Springer US. https://doi.org/10.1007/978-0-387-09506-6

Cakir, R., & Korkmaz, O. (2019). The effectiveness of augmented reality environments on individuals with special education needs. *Education and Information Technologies*, *24*(2), 1631–1659. https://doi.org/10.1007/s10639-018-9848-6

Çakir, R., Solak, E., & Tan, S. S. (2015). Artırılmış gerçeklik teknolojisi ile ingilizce kelime öğretiminin öğrenci performansına etkisi. *Gazi Eğitim Bilimleri Dergisi*, *1*(1), Article 1.

Chen, Y., Wang, Q., Chen, H., Song, X., Tang, H., & Tian, M. (2019). An overview of augmented reality technology. *Journal of Physics: Conference Series*, *1237*(2), 022082. https://doi.org/10.1088/1742-6596/1237/2/022082

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications, Inc.

Davis, M., Dautenhahn, K., Powell, S., & Nehaniv, C. (2010). Guidelines for researchers and practitioners designing software and software trials for children with autism. *Journal of Assistive Technologies*, *4*(1), 38–48. https://doi.org/10.5042/jat.2010.0043

Demirer, V., & Erbaş, Ç. (2015). Mobil artırılmış gerçeklik uygulamalarının incelenmesi ve eğitimsel açıdan değerlendirilmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, *11*(3). https://doi.org/10.17860/efd.29928

Eliçin, Ö., & Yıkmış, A. (2015). Otizmi olan öğrencilere okuma-yazma öğretme konusunda sınıf öğretmenlerinin görüş ve önerileri. *Abant İzzet Baysal Üniversitesi Eğitim Fakültesi Dergisi*, *15*(0). https://doi.org/10.17240/aibuefd.2015.15.0-5000128655

Erişti, S. D. B., Fırat, M., İzmirli, S., & Ceylan, B. (2017). Otizm spektrum bozukluğu olan çocuklar için tasarım tabanlı araştırma yaklaşımına dayalı eğitsel oyun tasarımı. *Uludağ Üniversitesi Eğitim Fakültesi Dergisi*, *30*(1), 73–99. https://doi.org/10.19171/uefad.323387

F. Antonak, R., & Livneh, H. (2000). Measurement of attitudes towards persons with disabilities. *Disability and Rehabilitation*, *22*(5), 211–224. https://doi.org/10.1080/096382800296782

Ginsburg, K. R., and the Committee on Communications, & and the Committee on Psychosocial Aspects of Child and Family Health. (2007). The Importance of Play in Promoting Healthy Child Development and Maintaining Strong Parent-Child Bonds. *Pediatrics*, *119*(1), 182–191. https://doi.org/10.1542/peds.2006-2697

Jiménez-Muñoz, L., Peñuelas-Calvo, I., Calvo-Rivera, P., Díaz-Oliván, I., Moreno, M., Baca-García, E., & Porras-Segovia, A. (2022). Video games for the treatment of autism spectrum disorder: A systematic review. *Journal of Autism and Developmental Disorders*, *52*(1), 169–188. https://doi.org/10.1007/s10803-021-04934-9

Kandalaft, M., Didehbani, N., Krawczyk, D., Allen, T., & Chapman, S. (2012). Virtual reality social cognition training for young adults with high-functioning autism. *Journal of Autism and Developmental Disorders*, *43*. https://doi.org/10.1007/s10803-012-1544-6

Kaytez, N., & Durualp, E. (2014). Türkiye'de okul öncesinde oyun ile ilgili yapılan lisansüstü tezlerin incelenmesi. *Uluslararası Türk Eğitim Bilimleri Dergisi*, *2014*(2), 110–122.

Kim, S. L., Suk, H. J., Kang, J. H., Jung, J. M., Laine, T. H., & Westlin, J. (2014). Using Unity 3D to facilitate mobile augmented reality game development. *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 21–26. https://doi.org/10.1109/WF-IoT.2014.6803110

Korkmaz, B. (2010). Otizm: Klinik ve nörobiyolojik özellikleri, erken tanı, tedavi ve bazı güncel gelişmeler. *Turkish Pediatrics Archive/Turk Pediatri Arsivi*, *45*.

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, *22*(140), 1–55.

Mazon, C., Etchegoyhen, K., Saint-Supery, I., Amestoy, A., Bouvard, M., Consel, C., & Sauzéon, H. (2022). Fostering parents-professional collaboration for facilitating the school inclusion of students with ASD: Design of the "ToGather" web-based prototype. *Educational Technology Research and Development*, *70*(1), 231–262. https://doi.org/10.1007/s11423-021-10073-w

Ökcün-Akçamuş, M. Ç. (2016). Otizm spektrum bozukluğu olan çocukların sosyal iletişim becerileri ve dil gelişim özellikleri. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Özel Eğitim Dergisi*. https://doi.org/10.21565/ozelegitimdergisi.246293

Öncül, N., & Çifci Tekinarslan, İ. (2021). Otizm spektrum bozukluğu olan çocuklara sembolik oyunların öğretiminde canlı ve video modelle öğretimin karşılaştırılması. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Özel Eğitim Dergisi*, 1–27. https://doi.org/10.21565/ozelegitimdergisi.783396

Pan, X., & Hamilton, A. F. de C. (2018). Why and how to use virtual reality to study human social interaction: The challenges of exploring a new research landscape. *British Journal of Psychology*, *109*(3), 395–417. https://doi.org/10.1111/bjop.12290

Pişkin, Ü. (1993). Otlstik çocuklarda oyun. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Özel Eğitim Dergisi*, *1*(3). https://doi.org/10.1501/Ozlegt_0000000016

Rosenberg, M. J. (1982). The ABCs of ISD (instructional systems design). *Training and Development Journal*, *36*(9), 44–50.

Sedgwick, P. (2013). Convenience sampling. *BMJ*, *347*(oct25 2), f6304–f6304. https://doi.org/10.1136/bmj.f6304

Serin, E., Novica, D. R., & Hidayat, I. K. (2021). The importance of design elements in special education of individuals with autism and learning disabilities. *KnE Social Sciences*, 32–40. https://doi.org/10.18502/kss.v5i6.9174

Shamir, A., & Lifshitz, I. (2013). E-Books for supporting the emergent literacy and emergent math of children at risk for learning disabilities: Can metacognitive guidance make a difference? *European Journal of Special Needs Education*, *28*(1), 33–48.

Sirris, S. (2022). Researchers' Role Reflexivity When Studying Values Work. In G. Espedal, B. Jelstad Løvaas, S. Sirris, & A. Wæraas (Eds.), *Researching Values* (pp. 205–224). Springer International Publishing. https://doi.org/10.1007/978-3-030-90769-3_12

Somyürek, S. (2014). Öğretim sürecinde z kuşağının dikkatini çekme: Artırılmış gerçeklik. *Eğitim Teknolojisi Kuram ve Uygulama*, *4*(1), 63–80. https://doi.org/10.17943/etku.88319

Stoeva, M. (2014). Interactive multimedia tool for dynamic generation of web interfaces with html5/php/mysql and javascript. *International Journal of Emerging Technology & Advanced Engineering*, *4*(9), 412–418.

Subaşı, M., & Okumuş, K. (2017). Bir araştırma yöntemi olarak durum çalışması. *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *21*(2), 419–426.

T.C. Aile, Çalışma ve Sosyal Hizmetler Bakanlığı. (2019). *Engelliler için bilgilendirme rehberi*. T.C. Aile, Çalışma ve Sosyal Hizmetler Bakanlığı. https://www.ailevecalisma.gov.tr/media/17688/engelli-bilgilendirme-27-09.pdf

TOV. (2008). *Otizm tarama projesi sonuç raporu*. TC Sağlık Bakanlığı Tohum Otizm Vakfı [TOV]. https://www.tohumotizm.org.tr/wp-content/uploads/2018/07/taramaprojesi.pdf

Ünal, M. (2009). Çocuk gelişiminde oyun alanlarının yeri ve önemi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi*, *10*(2), 95–110.

Xiao, C., & Lifeng, Z. (2014). Implementation of mobile augmented reality based on Vuforia and Rawajali. *2014 IEEE 5th International Conference on Software Engineering and Service Science*, 912–915. https://doi.org/10.1109/ICSESS.2014.6933713

Yakubova, G., Defayette, M. A., Chen, B. B., & Proulx, A. L. (2021). The use of augmented reality interventions to provide academic instruction for children with autism, intellectual, and developmental disabilities: An evidence-based systematic review. *Review Journal of Autism and Developmental Disorders*. https://doi.org/10.1007/s40489-021-00287-2

Yang, D., Zhu, S., & Lu, W. (2004). Realization of 3D simulation by openGL and 3D studio MAX [J]. *Applied Science and Technology*, *2*, 13.

2022

4(2), 247-259

Duygu Analizinde Aşırı Öğrenme Algoritması ve Uygulamaları: Sistematik Literatür Taraması

Rumeysa Erdoğan*[1], Baha Şen[2]

Anahtar Sözcükler

Duygu analizi
Aşırı öğrenme makinesi
Makine öğrenmesi

Makale Hakkında

Gönderim Tarihi
04 Aralık 2022
Kabul Tarihi
24 Aralık 2022
Yayın Tarihi
28 Aralık 2022

Makale Türü
Derleme Makalesi

Öz

Duygu Analizi, yapılandırılmamış metin aracılığıyla insan duygularını tanımlama ve özellik çıkarma tekniği olarak kabul edilir ve Doğal Dil İşleme ve Makine Öğrenimi yoluyla yapılır. Günümüzde birçok kurum ve şirketler bunu kullanarak müşteri veya kullanıcının özelliklerini tanımak ve ona uygun şekilde hareket etmek istemektedir. Böylece duygu analizinin önemi ve etkinliği ve kullanılan algoritmaların çeşitliliği günden güne artmaktadır. Bu algoritmalardan biri de Aşırı Öğrenme Makinesi (Extreme Learning Machine)dir. Extreme Learning Machine (ELM) algoritması, duygu analizi ve sınıflandırması için önemli bir makine öğrenimi algoritmasıdır. Bu çalışma, ELM'nin duygu analizinde kullanımına ilişkin seçilen çalışmaların kullanılan yöntem, bağlam ve uygulamaları yönünden incelendiğini gösteren sistematik bir araştırmadır. 2020 ile 2022 yılları arasında yayınlanan çalışmaların sistematik bir incelemesi, Web of Science ve Google Scholar veri tabanları kullanılarak gerçekleştirilmiştir. Literatürün ilk ve derinlemesine taranmasından sonra inceleme sürecinden 28 makaleden 10'u seçilmiştir. Makaleler, çalışmanın amacına ve araştırma sorularına göre incelenmiştir. Araştırma kapsamında yapılan inceleme sonuçlarına göre, duygu analizinde çoğunlukla ELM ile birlikte farklı metotlar kullanılmış, ELM' nin performansı iyileştirilmeye çalışılmıştır. Tedavi özetlerinin kalite analizi, sağlık, eğitim, website ürün değerlendirmeleri gibi farklı alanlarda kullanılmaktadır. ELM'nin duygu analizinde kullanımında kapsam olarak en çok sosyal medya verisi ve özellikle de Twitter platformunun kullanıldığı sonucuna ulaşılmıştır.

Extreme Learning Machine Algorithm in Sentiment Analysis and Its Applications: Systematic Literature Review

Keywords

Sentiment analysis
Extreme learning machine
Machine learning

Article Info

Received
December 04, 2022
Accepted
December 24, 2022
Published
December 28, 2022

Article Type
Review Article

Abstract

Natural language processing and machine learning are used to define and extract human emotions from unstructured text using a technique called sentiment analysis. Today, many organizations and companies want to use this to recognize and act accordingly on the customer or user's features. This increases the importance and effectiveness of emotion analysis and the diversity of algorithms used day by day. One of these algorithms is the Extreme Learning machine. The Extreme Learning machine (ELM) algorithm is an important machine learning algorithm for emotion analysis and classification. In this study, the method used in the ELM's emotional analysis is systematic research that shows that the context and its applications have been studied. A systematic review of the works published between 2020 and 2022 was carried out using the Web of Science and Google Scholar databases. After the first and in-depth screening of the literature, 10 of the 28 articles were selected from the review process. The articles have been reviewed based on the purpose of the study and research questions. According to the research results, different methods were used in the emotional analysis, mostly with the ELM, and ELM's performance was improved. Quality analysis of treatment summaries is used in different areas, such as health care, education, and website product assessments. ELM's use of emotion analysis has resulted in most social media data as a scope, especially the Twitter platform.

Atıf: Erdoğan, R. & Şen, B. (2022). Duygu analizinde aşırı öğrenme algoritması ve uygulamaları: sistematik literatür taraması. *Bilgi ve İletişim Teknolojileri Dergisi*, *4*(2), 247-259. https://doi.org/10.53694/bited.1214454

***Cite*:** Erdogan, R. & Sen, B. (2022). Extreme learning machine algorithm in sentiment analysis and its applications: systematic literature review. *Journal of Information and Communication Technologies*, *4*(2), 247-259. https://doi.org/10.53694/bited.1214454

* **Sorumlu Yazar/Corresponding Author:** erdogannrumeysaa@gmail.com
[1] MSc Student., Ankara Yıldırım Beyazıt University, Institute of Science, Ankara/Turkey, erdogannrumeysaa@gmail.com, https://orcid.org/ 0000-0002-6218-7072
[2] Assoc. Prof. Dr., Ankara Yıldırım Beyazıt University, Faculty of Engineering and Natural Sciences, Ankara/Turkey, bsen@ybu.edu.tr, https://orcid.org/0000-0003-3577-2548

Introduction

With the beginning of digital and web technologies, expressing and sharing ideas over the Internet has become inevitable today. Twitter, Instagram, YouTube, etc. social networking sites, have become increasingly important to users. Various users, including consumers, government, and brands, use these platforms to share promotional agreements, exchange ideas, run campaigns, raise awareness of social issues, and promote products and services. With data transmitted through such platforms, it is aimed at applying algorithms to understand consumer emotions and thoughts, analyze the views and emotions of businesses, and analyze the views and emotions of people. There are various mechanisms that are monitored to review content on social media for business analytics and emotional analysis of consumer feedback. Sentiment analysis is related to strategies that use machine learning and Natural Language Processing tools to identify and remove human emotions from unstructured text (Jindal & Aron, 2021). Any organization that intends to base choices on consumer behavior must consider emotional analysis. Learning-based and non-learning techniques can be used to categorize emotions. Compared to non-learning-based methods, machine learning-based techniques can produce better categorization results. One of the most widely used machine learning-based techniques is the Extreme Learning Machine (ELM), which consistently outperforms other gradient-based learning algorithms successfully used in a range of applications in the real world.

ELM is used in many different areas, such as medicine, robotics, and geography, due to high learning speed, providing good accuracy value, and good generalization performance. In medicine, Hu et al. (2022), propose a new model for early diagnosis and determination of the disease severity of COVID-19. In this study, a combination of kernel extreme learning machine algorithm and improved binary Harris hawk optimization (HHO) algorithm is used for prediction. The results indicate that this new model can achieve good performance. In robotics, Alcin et al. (2016), applied ELM to the operation of the robotic arm. When they compare the accuracy of the model with the Artificial Neural Network (ANN), the experimental results demonstrate that the proposed model is suitable. In geography, Hua et al. (2020), propose an optimized ELM-based model that aims to predict wind speed. Compared to other models, this new model appears to provide superior performance in predicting wind speed.

For specific classification applications, other machine learning classifiers like the Support Vector Machine (SVM) and Random Forest (RF) are also utilized. These machine-learning classifiers are utilized for binary classification issues, and it is unknown how well they perform while processing nonlinear sensitivity classification (Shafqat-Ul-Ahsaan et al., 2019).

Extreme Learning Machine

Single hidden layered forward-feed boundary networks (SLFNs) can be modeled using the ELM, which chooses hidden nodes at random and calculates the output weights of SLFNs analytically. Theoretically, this method often demonstrates high generalization performance at a very quick learning rate. Experimental results based on a few real-world and synthetic benchmarking functions approaches and classification problems, including very large complex applications, show that the new algorithm can learn thousands of times faster than traditional popular learning algorithms for forward-feeding neural networks and can produce a good generalization performance in the most cases (Huang et al., 2006).

Purpose of the Research and Research Questions

The aim of this study is to investigate how the ELM algorithm is implemented in sentiment analysis applications. Within the scope of this research, the following research questions were addressed:

RQ1: What is the application context of sentiment analysis with the ELM algorithm?

RQ2: Is there a performance difference between ELM and other machine learning algorithms in sentiment analysis?

RQ3: What are the methods used in sentiment analysis?

Method

Design of the Research

To systematically present the synthesis and interpretation of pertinent and quality work, three research questions that served as the basis for this study's design were addressed through a systematic literature review. A systematic review is a procedure that involves choosing, locating, and synthesizing pertinent research studies to present a clearer and more complete representation of the collected studies than any one study can (Gough et al., 2012). Following the detailed steps of the investigation, a systematic literature review is carried out to answer the research questions.

Selection of Relevant Literature

Web of Science, a website that provides comprehensive citation information for several databases with subscription-based access for a variety of academic studies, and Scholar, a search engine and database that searches academic articles and topics, were used for this assessment. The search keywords used for these online databases are "Sentiment Analysis" and "Extreme Learning Machine". The total number of articles identified from the database search is 16 articles on the Web of Science. The search made on Scholar yielded 1, 620 results. When searching for articles, inclusion and exclusion criteria, and searching resulted in 13 articles on the Web of Science and 15 articles on Scholar. As a result, full-text reading and analysis of each article were made depending on the purpose of the study, research questions, and whether the ELM algorithm was applied, and accordingly, a total of 10 final articles were obtained, 4 from Web of Science and 6 from Scholar.

Data Analysis

The studies that were identified and included in the research were examined in a way to seek answers to the research questions. In the research, the results related to the year of the study, keyword, method, application area, and dataset were determined as criteria. The data obtained from these criteria are entered in the table. When all assessments were completed, the data were analyzed.

Findings

In this section, the data of 10 studies examined within the scope of the research are presented for the research questions. The reviewed studies were published between 2020-2022. There are a total of 10 articles selected for the purpose of this review. The studies examined were analyzed according to the “Author”, “Year”, “Title”, “Method/Tools”, “Application/Result” and “Context/Dataset" features, and the findings are given in Table 1.

Table 1. Information of reviewed articles.

Author	Year	Paper Type	Title	Method	Application	Dataset
Samer Abdulateef Waheeb, Naseer Ahmed Khan, Bolin Chen, & Xuequn Shang.	2020	Article	Machine Learning Based Sentiment Text Classification for Evaluating Treatment Quality of Discharge Summary	Lexicon-based, extreme learning machine with autoencoder	Analyzing the quality of treatment	health and medical records
Bei Pan, Kaoru Hirota, Zhiyang Jia, Linhui Zhao, Xiaoming Jin, & Yaping Dai.	2021	Article	Multimodal emotion recognition based on feature selection and extreme learning machine in video clip	Genetic Algorithm and Extreme Learning Machine	Prediction of categorical emotions where visual and auditory signals are used as multimodal input	Emotional visual and audio dataset
Samer Abdulateef Waheeb, Naseer Ahmed Khan, & Xuequn Shang.	2022	Article	Topic Modeling and Sentiment Analysis of Online Education in the COVID-19 Era Using Social Networks Based Datasets	Extreme Learning Machine AutoEncoder (ELM-AE) and Long Short-Term Memory(LSTM)	Elimination of noise in the information	Twitter dataset
Anwer Mustafa Hilal, Badria Sulaiman Alfurhood, Fahd N. Al-Wesabi, Manar Ahmed Hamza, Mesfer Al Duhayyim, & Huda G. Iskandar.	2021	Article	Artificial Intelligence Based Sentiment Analysis for Health Crisis Management in Smart Cities	Beetle Antenna Search with Extreme Learning Machine (BAS-ELM)	Management of healthcare crisis in smart cities	Twitter dataset
Shafqat-Ul-Ahsaan, Ashish Kumar Mourya, & Parvinder Singh.	2019	Book Chapter	Predictive Modeling and Sentiment Classification of Social Media Through Extreme Learning Machine	Extreme Learning Machine	Multiclass sentiment classification of social media	Facebook dataset
P. Menakadevi & J. Ramkumar.	2022	Conference paper	Robust Optimization Based Extreme Learning Machine for Sentiment Analysis in Big Data	Robust Optimization-based Extreme Learning Machine (ROELM)	Sentiment classification in big data	Amazon product review datasets

Aijing Sun, Fan Wei, Guoqing Wang, & Yijia Li.	2022	Conference paper	Chinese Sentiment Analysis Using Regularized Extreme Learning Machine and Stochastic Optimization	Regularized Extreme Learning Machine	Chinese Sentiment Analysis	Chinese text dataset
Heyam H. Al-Baity, Hala J. Alshahrani, Mohamed K. Nour, Ayman Yafoz, Omar Alghushairy, Raed Alsini, & Mahmoud Othman.	2022	Article	Computational Linguistics Based Emotion Detection and Classification Model on Social Networking Data	Shuffled Frog Leaping Optimization (SFLO) Algorithm with Extreme Learning Machine	Recognition and classification of emotions in social networking data	Social media dataset
Mustafa Abdul Salam & Mahmoud Ali.	2020	Article	Optimizing Extreme Learning Machine using GWO Algorithm for Sentiment Analysis	Grey Wolf Optimization (GWO) with Extreme Learning Machine	Sentiment analysis of Twitter	Twitter dataset
Dr. V Chandra Sekhar, Chintalapati Sindhu Sri.	2021	Article	Predicting Cyber Bullying On Social Media In The Big Data Era Using Extreme Learning Machine	Extreme Learning Machine	Cyberbullying detection on social media	Twitter dataset

When the distribution of studies by years is examined in Table 1, it is seen that the most studies are 4 scientific studies in 2022. This is followed by 2021 with 3 scientific studies and 2019 with 3 scientific studies. Considering the number of scientific studies, it is seen that there is no regular increase in the number of studies on the application of ELM in sentiment analysis, but there are studies on this subject every year.

When the keywords used in the reviewed articles are examined, it is seen that "sentiment analysis" and "extreme learning machine" are frequently used. In addition to these keywords, similar keywords such as "emotion recognition", "emotion classification", "machine learning" and "classification" are also used in the studies.
In this study, the articles were analyzed according to the methods used. In the articles reviewed, not only the ELM algorithm but also the ELM algorithm in 8 out of 10 studies were implemented using machine learning methods such as the Lexicon-based method and optimization methods.

According to the studies examined, it is seen that 4 studies used a Twitter dataset, 1 study used a Facebook dataset, and 1 study used a social media dataset as a dataset for sentiment analysis. In the studies examined based on this, it is seen that social media is mostly used in the sentiment analysis implemented in the ELM.

Waheeb et al. (2020) developed a new sentiment analysis system using a natural language processing feature extraction method of patient discharge documents to analyze and classify treatment and diagnostic quality. In this study, the ELM method uses a metric in Eq. 1:

$$y_j = \sum_{i=1}^{\varphi} \beta_i g(w_i.x_i + b_i),\ j = 1,2,\ldots,N$$

Eq. 1. Formula of ELM

In this formula, w_i connects the input neuron and the hidden neuron in ELM and b_i is the bias of the hidden neuron. β_i provides the connection between the hidden neuron and the output neuron. This formula can be expressed as in Eq. 2:

$$y = \mathrm{H}\beta$$

Eq. 2. Expression of y with the matrix form H

Here, Moore–Penrose popularize matrix H can be represented in Eq. 3:

$$H = \begin{bmatrix} g(w_1x_1 + b_1) & \ldots. & g\left(w_\varphi x_1 + b_\varphi\right) \\ \vdots & & \vdots \\ g(w_1x_1 + b_1) & \ldots. & g\left(w_\varphi x_N + b_\varphi\right) \end{bmatrix}_{N\times\varphi}$$

Eq. 3. Moore–Penrose popularize matrix H

Statistical methods, vector space models, association rule, and Extreme Learning Machine Autoencoder (ELM-AE) are included in this system. Experimental results show that this new method is an effective technique in analyzing the quality of treatment.

This study, in which visual and auditory signals are used as input, presents a new emotion analysis system to predict categorical emotions. ELM classifiers optimized for emotion recognition are utilized. The aim here is to give different weights to the auditory modality and the visual modality based on their importance for sentiment analysis, formulated as in Eq. 4:

$$C\left(y_v, y_a\right) = \max_i \left(\beta p_v(i) + (1-\beta)p_a(i)\right)$$

Eq. 4. Formula of sentiment classification

In this formula, y_v represents the classification results of the visual modality, and y_a the auditory modality. β is the weight indicating the importance of the visual modality. $p_v(i)$ and $p_a(i)$ are implicit probability values of visual and auditory modality. This developed system was applied to three general datasets and the results were compared. Accordingly, emotion recognition results obtained by combining visual and auditory predicted emotions are superior to both the recognition of unimodality and the ranking of individual characteristics (Pan et al., 2021).

Menakadevi and Ramkumar (2022) proposed the Robust Optimization-based Extreme Learning Machine (ROELM) classifier for sentiment analysis of the large Amazon product evaluation dataset. ROELM uses natural wolf-like behavior to analyze an enormous database of reviews. ELM's single-layer hidden layer acts to improve classification performance. Indicating that classifiers trained for a particular dataset may perform poorly for other large datasets, (Menakadevi & Ramkumar, 2022) evaluated the accuracy and f-measurement performance of the proposed classifier. According to the results obtained, the proposed classifier performs better in classification than other classifiers.

In the study of Sun et al. (2022), a model with high accuracy and fast performance is developed for sentiment analysis of short Chinese texts. In this model, regularized ELM algorithm is used for classification, and the Particle Swarm Optimization algorithm is used. The extreme learning machine model used in this study is as in Eq. 5:

$$Y_m = \sum_{i=1}^{L} \beta_i G(w_i, b_i, x_j); \;\; j = 1,2, \ldots, n$$

Eq. 5. The formula of ELM

In this formula, Y_m is the output, β is the link weight matrix of the output layer and the hidden layer, and G(wi, bi, xj) is the output matrix of the hidden layer neurons. When this proposed model is compared with other models, it is seen that it has a high accuracy value and execution speed.

In Al-Baity et al. (2022) study, it is proposed a linguistic-based sentiment analysis model for sentiment recognition and classification on social network data. This model uses the ELM algorithm for sentiment analysis after making the necessary preprocessing. Then the shuffled frog leaping optimization algorithm (SFLO) is used, which changes the parameters of the ELM algorithm accordingly. In this study, the ELM formula given in Eq. 6 was used as a model:

$$\sum_{i=1}^{L} \beta_i g(w_j \cdot x_j + b_i) = t_j, j = 1,2, \ldots, N$$

Eq. 6. Formula of ELM

In this formula, w_i connects the input neuron and the hidden neuron in ELM and b_i is the bias of the hidden neuron. β_i provides the connection between the hidden neuron and the output neuron. When the experimental results are examined, it is seen that this new model outperforms other models (Al-Baity et al., 2022).

In Shafqat-Ul-Ahsaan et al. (2019) study, the ELM algorithm, which outperforms the SVM classifier and is widely preferred in classification, is used to apply sentiment analysis on the Facebook dataset. The ELM algorithm, which can present the results in categorical form, has been analyzed for the multi-class sentiment. ELM algorithm Single Layer Feed Forward Networks with activation function λ(x) and N hidden nodes can be modeled as in Eq. 7:

$$\sum_{i=1}^{\check{N}} \beta_i \lambda_i(x_j) = \sum_{j=1}^{\check{N}} \beta_i \lambda_i(W_j, b_j, x_j)$$

Eq. 7. The formula of ELM

In this equation, wj is the vector form input weight between the various input layer nodes and the jth hidden layer node, and it has the values (wj_1, wj_2,..., wj_m). β_j is the weight matrix of the jth hidden layer nodes, and $\lambda(\cdot)$ is the activation function which is a continuous nonlinear function. The ELM has the capability to approach any predicted value by minimizing the error, the expression can be edited as in Eq. 8:

$$H\beta = \tau$$

Eq. 8. Expression of the output with the matrix form H

where *H* is the output matrix of the hidden layer

$$\begin{bmatrix} h(x_1) \\ h(x_2) \\ \vdots \\ h(x_n) \end{bmatrix} = \begin{bmatrix} \lambda(w_1, b_1, x_1) & \dots & \lambda(w_m, b_m, x_1) \\ \lambda(w_1, b_1, x_2) & \dots & \lambda(w_m, b_m, x_2) \\ \vdots & \dots & \vdots \\ \lambda(w_1, b_1, x_n) & \dots & \lambda(w_m, b_m, x_n) \end{bmatrix}$$

Eq. 9. Expression of the resultant output

where β is the weight of the hidden layer and τ is the target matrix of the ELM. Experimental results show that ELM obtains better performance and accuracy compared to other machine learning classifiers.

Sekhar and Sri (2021) develop a system to predict whether there is cyberbullying in social media. In addition, (Shafqat-Ul-Ahsaan et al., 2019), the study also uses the Twitter dataset. They apply deep learning-based models, thinking that they can improve their prediction ability by using ELM techniques. As a result, it has been reached that it makes a better prediction and classification than other methods.

In the model proposed in Waheeb et al. (2022) study, the ELM algorithm and Autoencoder are used together to eliminate the noise in the Twitter data, and LSTM (Long Short-Term Memory) is included in the application in classification. In this study, the ELM method uses a metric in Eq. 10:

$$y_j = \sum_{i=1}^{\varphi} \beta_i g(w_i.x_i + b_i),\ j = 1, 2, \dots, N$$

Eq. 10. Formula of ELM

In this formula, w_i connects the input neuron and the hidden neuron in ELM and b_i is the bias of the hidden neuron. β_i provides the connection between the hidden neuron and the output neuron. This formula can be expressed as in Eq. 11:

$$y = \mathrm{H}\beta$$

Eq. 11. Expression of y with the matrix form H

Here, Moore–Penrose popularize matrix H can be represented in Eq. 12:

$$H = \begin{bmatrix} g(w_1 x_1 + b_1) & \cdots & g(w_\varphi x_1 + b_\varphi) \\ \vdots & & \vdots \\ g(w_1 x_1 + b_1) & \cdots & g(w_\varphi x_N + b_\varphi) \end{bmatrix}_{N \times \varphi}$$

Eq. 12. Moore–Penrose popularize matrix H

When the results are examined, it is seen that this proposed model achieves higher performance when compared with training test sets of different sizes (Waheeb et al., 2022).

Hilal et al. (2022) presented an artificial intelligence-based sentiment analysis system for health services crisis management in smart cities. Validation and tests are performed on the Twitter dataset. Brainstorm Optimization Algorithm (BSO) and Deep Belief Network Algorithm (DBN) are used together for feature extraction. For classification, the Beetle Antenna Search algorithm is used together with the ELM in various classes. In this study, the ELM formula given in Eq. 13 was used as a model:

$$h_j = g(W_j^i x_i^T + b_j)$$

Eq. 13. The formula of ELM

where g is the activation function, W_j^i indicates the input weight vector and b is the bias. When this formula is remodeled with the matrix below:

$$Y = H\beta$$

$$\text{where } H = \begin{bmatrix} g(W_1 x_1^T + b_1) & \cdots & g(W_L x_1^T + b_L) \\ \vdots & \ddots & \vdots \\ g(W_1 x_N^T + b_1) & \cdots & g(W_L x_N^T + b_L) \end{bmatrix}_{N \times L}, \beta = \begin{bmatrix} \beta^1 \\ \vdots \\ \beta^L \end{bmatrix}_{L \times m}, Y = \begin{bmatrix} y^1 \\ \vdots \\ y^m \end{bmatrix}_{N \times m}$$

Eq. 14. The equation of the matrix H

The resultant expression can be obtained as in Eq. 14. Experimental results show that measurements such as high classification performance and accuracy value have been achieved.

In this study, it is aimed to make a sentiment analysis on the Twitter dataset, which is one of the big social media forums where people share their feelings and thoughts. A new approach that optimizes the ELM algorithm with the Grey Wolf Optimization algorithm is presented. According to the results, it has been noted that the new hybrid model can cope with the problems of the classical ELM models and outperforms the other models compared (Salam & Ali, 2020).

Discussion and Conclusion

In this systematic literature review, the use of the ELM algorithm in sentiment analysis has been investigated in terms of the methods used and the context. In the reviewed articles, it is stated that the combination of the results with pure ELM or some other algorithms shows high performance and accuracy when compared to other algorithms. In 8 of the 10 selected scientific studies, the ELM algorithm is either modified or used in a hybrid way with other algorithms to improve its performance.

When the studies examined within the scope of the research are examined in the context of the method used, it is seen that algorithms such as Genetic Algorithms (Pan et al., 2021), Beetle Antennae Search Algorithm (Hilal et al., 2022), Shuffled Frog Leaping Optimization Algorithm (Al-Baity et al., 2022), Grey Wolf Optimization Algorithm (Salam & Ali, 2020) and Particle Swarm Optimization Algorithm (Sun et al., 2022) are also used in addition to the ELM algorithm.

When the studies are examined in the context of the scope and the dataset used, it is seen that the ELM algorithm is used in sentiment analysis in different research areas. 4 of the analyzed studies use the Twitter dataset (Salam & Ali, 2020; Salam & Ali, 2020; Sekhar & Sri, 2021; Waheeb et al., 2022), 1 of them use the Facebook dataset (Shafqat-Ul-Ahsaan et al., 2019) and 1 of them uses the social network dataset (Al-Baity et al., 2022). Based on these data, it is seen that social media, and especially Twitter, is the context frequently used in sentiment analysis.

Another finding from this research is that the basic formula of ELM was used in most of the studies. In these studies, the basic ELM model was either simply used or developed and applied. In addition, these models show successful performance in the studies examined. In addition to these, Waheeb et al. (2020) and Waheeb et al. (2022) used the same ELM model on different topics in their studies.

Wang et al. (2022), also reviewed ELM with different aspects and topics. Theoretical analysis, various improvements in the performance of ELM, and applications of ELM in different fields are given and discussed.

This study has some limitations that should be considered along with its contribution to the literature. It can be stated that there is a limitation in comparing the use of ELM in sentiment analysis, as 10 studies are suitable to be included in the study. As the ELM algorithm is applied to different topics in sentiment analysis, different results will be obtained. In addition, this study covers the years 2020-2022. This limitation can be removed if the scope year of the studies is extended, and future studies are included.

Research Ethics

The authors declare that the research does not have an unethical problem.

Contribution Rate of Researchers

The authors contributed equally to each part of this study.

Conflict of Interest

The authors declare that this study has no conflicts of interest.

Funding

The authors declare that there is no funding for this study.

The Ethical Committee Approval

This study does not require an ethics committee decision, since data in an international database open to all researchers is used, no experimental procedures have been performed on any living species, and there is no need for a data collection process.

Kaynakça / References

Al-Baity, H. H., Alshahrani, H. J., Nour, M. K., Yafoz, A., Alghushairy, O., Alsini, R., & Othman, M. (2022). Computational linguistics based emotion detection and classification model on social networking data. *Applied Sciences*, *12*(19), 9680. https://doi.org/10.3390/app12199680

Alcin, O. F., Ucar, F., & Korkmaz, D. (2016, August). Extreme learning machine based robotic arm modeling. In *2016 21st International Conference on Methods and Models in Automation and Robotics (MMAR)* (pp. 1160-1163). IEEE.

Gough, D., Thomas, J., & Oliver, S. (2012). Clarifying differences between review designs and methods. *Systematic Reviews*, *1*(1). https://doi.org/10.1186/2046-4053-1-28

Hilal, A. M., Alfurhood, B. S., Al-Wesabi, F. N., Hamza, M. A., al Duhayyim, M., & Iskandar, H. G. (2022). Artificial intelligence based sentiment analysis for health crisis management in smart cities. *Computers, Materials and Continua*, *71*(1), 143–157. https://doi.org/10.32604/cmc.2022.021502

Hu, J., Heidari, A. A., Shou, Y., Ye, H., Wang, L., Huang, X., ... & Wu, P. (2022). Detection of COVID-19 severity using blood gas analysis parameters and Harris hawks optimized extreme learning machine. *Computers in Biology and Medicine*, *142*, 105166.

Hua, L., Zhang, C., Peng, T., Ji, C., & Nazir, M. S. (2022). Integrated framework of extreme learning machine (ELM) based on improved atom search optimization for short-term wind speed prediction. *Energy Conversion and Management*, *252*, 115102.

Huang, G. B., Zhu, Q. Y., & Siew, C. K. (2006). Extreme learning machine: theory and applications. *Neurocomputing*, *70*(1-3), 489-501.

Jindal, K., & Aron, R. (2021). A systematic study of sentiment analysis for social media data. *Materials Today: Proceedings*. https://doi.org/10.1016/J.MATPR.2021.01.048

Menakadevi, P., & Ramkumar, J. (2022). Robust optimization based extreme learning machine for sentiment analysis in big data. *2022 International Conference on Advanced Computing Technologies and Applications, ICACTA 2022*. https://doi.org/10.1109/ICACTA54488.2022.9753203

Pan, B., Hirota, K., Jia, Z., Zhao, L., Jin, X., & Dai, Y. (2021). Multimodal emotion recognition based on feature selection and extreme learning machine in video clips. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-021-03407-2

Salam, M. A., & Ali, M. (2020). Optimizing extreme learning machine using GWO algorithm for sentiment analysis. *International Journal of Computer Applications*, *176*(38), 22-28.

Sekhar, C., & Sri, C. S. (2021). Predicting cyber bullying on social media in the big data era using extreme learning machine *11*(10).

Shafqat-Ul-Ahsaan, Mourya A. K, & Singh, P. (2019). Predictive modeling and sentiment classification of social media through extreme learning machine. *Proceedings of ICETIT 2019: Emerging Trends in Information Technology*, 605, 356.

Sun, A., Wei, F., Wang, G., & Li, Y. (2022). Chinese sentiment analysis using regularized extreme learning machine and stochastic optimization. *2022 4th International Conference on Natural Language Processing (ICNLP)*, 525–529. https://doi.org/10.1109/ICNLP55136.2022.00096

Waheeb, S. A., Khan, N. A., Chen, B., & Shang, X. (2020). Machine learning based sentiment text classification for evaluating treatment quality of discharge summary. *Information (Switzerland)*, *11*(5). https://doi.org/10.3390/INFO11050281

Waheeb, S. A., Khan, N. A., & Shang, X. (2022). Topic modeling and sentiment analysis of online education in the COVID-19 era using social networks-based datasets. *Electronics (Switzerland)*, *11(*5). https://doi.org/10.3390/electronics11050715

Wang, J., Lu, S., Wang, S. H., & Zhang, Y. D. (2022). A review on extreme learning machine. *Multimedia Tools and Applications*, *81*(29), 41611-41660.