Yıl:2019 Cilt3: Sayı:2 Year:2019 Vol:3 No:2

UYBİSBBD

ULUSLARARASI YÖNETİM BİLİŞİM SİSTEMLERİ
VE
BİLGİSAYAR BİLİMLERİ DERGİSİ

ULUSLARARASI YÖNETİM BİLİŞİM SİSTEMLERİ VE BİLGİSAYAR BİLİMLERİ DERGİSİ

INTERNATIONAL JOURNAL OF MANAGEMENT INFORMATION SYSTEMS AND COMPUTER SCIENCE

Cilt: 3 ● Sayı: 2 ● Aralık 2019
Vol: 3 ● No: 2 ● December 2019

ULUSLARARASI YÖNETİM BİLİŞİM SİSTEMLERİ VE BİLGİSAYAR BİLİMLERİ DERGİSİ

INTERNATIONAL JOURNAL OF MANAGEMENT INFORMATION SYSTEMS AND COMPUTER SCIENCE

Cilt: 3 ● Sayı: 2 ● Aralık 2019

Vol: 3 ● No: 2 ● December 2019

Adres (Address)
Kilis 7 Aralık Üniversitesi
Teknik Bilimler Meslek Yüksekokulu
79100 Kilis / TÜRKİYE

E-mail : ybsbb.info@gmail.com
Web : dergipark.gov.tr/uybisbbd

HAKEM KURULU	
Prof. Dr. Abdulkadir YILDIZ **(Kahramanmaraş Sütçü İmam Üniversitesi)**	**Dr. Öğr. Üyesi Zülfiye BIKMAZ** **(Kırklareli Üniversitesi)**
Prof. Dr. H. Mustafa PAKSOY **(Kilis 7 Aralık Üniversitesi)**	**Dr. Öğr. Üyesi Ö. Fatih KEÇECİOĞLU** **(Kahramanmaraş Sütçü İmam Üniversitesi)**
Prof. Dr. Mustafa AKSU **(İstanbul Üniversitesi)**	**Dr. Öğr. Üyesi Cuma ERCAN** **(Kilis 7 Aralık Üniversitesi)**
Prof. Dr. Sadettin PAKSOY **(Kilis 7 Aralık Üniversitesi)**	**Dr. Öğr. Üyesi Mustafa Oğuz GÖK** **(Kahramanmaraş Sütçü İmam Üniversitesi)**
Doç. Dr. Deniz Mertkan GEZGİN **(Trakya Üniversitesi)**	**Dr. Öğr. Üyesi Sinan UĞUZ** **(Isparta Uygulamalı Bilimler Üniversitesi)**
Doç. Dr. İlhan UMUT **(Trakya Üniversitesi)**	**Dr. Öğr. Üyesi Muhammet ATALAY** **(Kırklareli Üniversitesi)**
Doç. Dr. İrfan Deli **(Kilis 7 Aralık Üniversitesi)**	**Dr. Öğr. Üyesi Mustafa Mikail ÖZÇİLOĞLU** **(Kilis 7 Aralık Üniversitesi)**
Doç. Dr. Nursal ARICI **(Gazi Üniversitesi)**	**Dr. Öğr. Üyesi Hasan Hüseyin ÇAM** **(Kilis 7 Aralık Üniversitesi)**
Doç. Dr. Yusuf Ekrem AKBAŞ **(Adıyaman Üniversitesi)**	**Dr. Öğr. Üyesi Ebru KÜLEKÇİ AKYAVUZ** **(Kilis 7 Aralık Üniversitesi)**
Prof. Dr. Kemal Delihacıoğlu **(Kilis 7 Aralık Üniversitesi)**	**Dr. Öğr. Üyesi Halil ARSLAN** **(Cumhuriyet Üniversitesi)**
Doç. Dr. Bengü HIRLAK **(Kilis 7 Aralık Üniversitesi)**	**Dr. Öğr. Üyesi Emrah AYDEMİR** **(Ahi Evran Üniversitesi)**
Dr. Öğr. Üyesi Edip Serdar GÜNER **(Kırklareli Üniversitesi)**	**Dr. Öğr. Üyesi Ayşe ÇİÇEK KORKMAZ** **(Bandırma 17 Eylül Üniversitesi)**
Dr. Öğr. Üyesi Hüseyin KOÇARSLAN **(Selçuk Üniversitesi)**	**Dr. Öğr. Üyesi Hüseyin AKAR** **(Kilis 7 Aralık Üniversitesi)**
Dr. Öğr. Üyesi Yasin ORTAKCI **(Karabük Üniversitesi)**	**Dr. Nilüfer VATANSEVER TOYLAN** **(Kırklareli Üniversitesi)**
Dr. Öğr. Üyesi Mehmet ÖZÇALICI **(Kilis 7 Aralık Üniversitesi)**	**Dr. Murat GEZER** **(İstanbul Üniversitesi)**
Dr. Öğr. Üyesi Melda AKBABA **(Kilis 7 Aralık Üniversitesi)**	**Dr. Serra Çelik** **(İstanbul Üniversitesi)**
Dr. Öğretim Üyesi Hayrettin TOYLAN **(Kırklareli Üniversitesi)**	**Dr. Feyzi KAYSİ** **(İstanbul Üniversitesi)**
Dr. Öğr. Üyesi Yasin SÖNMEZ **(Dicle Üniversitesi)**	**Dr. Hakan AÇIKGÖZ** **(Kilis 7 Aralık Üniversitesi)**
Dr. Öğr. Üyesi Ramazan ASLAN **(Adıyaman Üniversitesi)**	**Dr. Fatma Önay KOÇOĞLU** **(İstanbul Üniversitesi)**
Dr. Öğr. Üyesi Sibel YAŞAR **(Kırklareli Üniversitesi)**	**Dr. Fatih AYDIN** **(Kırklareli Üniversitesi)**
Dr. Öğr. Üyesi Şebnem ÖZDEMİR **(Beykent Üniversitesi)**	**Dr. Cemal AKTÜRK** **(Kilis 7 Aralık Üniversitesi)**

Dr. Öğr. Üyesi ALİ DURDU **(Ankara Sosyal Bilimler Üniversitesi)**	**Dr. Tarık TALAN** **(Kilis 7 Aralık Üniversitesi)**
Dr. Öğr. Üyesi Hakan ÜSTÜNEL **(Kırklareli Üniversitesi)**	**Dr. Ahmet Çağdaş SEÇKİN** **(Uşak Üniversitesi)**
Dr. Öğr. Üyesi Mehmet BAKIR **(Bozok Üniversitesi)**	**Dr. Emre AKADAL** **(İstanbul Üniversitesi)**
Dr. Öğr. Üyesi Doğan ÜNAL **(Kırklareli Üniversitesi)**	**Dr. Feden KOÇ** **(Uşak Üniversitesi)**
Doç. Dr. Dilek AVCI **(Bandırma 17 Eylül Üniversitesi)**	
Dr. Öğr. Üyesi Kazım SARIÇOBAN **(Mehmet Akif Ersoy Üniversitesi)**	

YAYIN POLİTİKASI

Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi yılda iki kez Haziran ve Aralık aylarında yayınlanan uluslararası hakemli bir dergidir. Dergide yer alan yazılar kaynak gösterilmeksizin kısmen ya da tamamen iktibas edilemez. Bu dergide yayınlanan çalışmaların bilim ve dil sorumluluğu yazarlarına aittir.

Dergimize gönderilen çalışmalar, alanında uzman iki ayrı hakem tarafından incelendikten sonra uygun görülenler yayınlanmaktadır. Yazım kurallarına ilişkin bilgilere dergimizin web adresinde yer verilmiştir. Bu derginin tüm hakları saklıdır. Önceden yazılı izin almaksızın hiçbir iletişim ve kopyalama sistemi kullanılarak yeniden kopyalanamaz, çoğaltılamaz ve satılamaz.

International Journal of Management Information Systems and Computer Science is an international peer-reviewed journal which is published two times a year in June and December. The articles cannot be cited partly or entirely without showing resources. The responsibility about scientific and grammatical issues is belong to authors.

The papers sent to the journal are reviewed by two referees and after their approval, they will be sent to edit before being published. Writing & Publishing Policies can be found in the journal's website.

Makaleler / Articles

COMPUTATION OF SHORTEST PATH PROBLEM IN A NETWORK WITH SV-TRIANGULAR NEUTROSOPHIC NUMBERS

Said BROUMİ *
Florentin SMARANDACHE**
Mohamed TALEA***
Assai BAKALİ****

DOI: 10.33461/uybisbbd.588290

Abstract

In this article, we present an algorithm method for finding the shortest path length between a paired nodes on a network where the edge weights are characterized by single valued triangular neutrosophic numbers. The proposed algorithm gives the shortest path length from source node to destination node based on a ranking method. Finally, a numerical example is also presented to illustrate the efficiency of the proposed approach.

Keywords: *single valued triangular neutrosophic number, score function, network; shortest path problem*

* Laboratory of Information Processing, Faculty of Science Ben M'Sik, University Hassan II, B.P 7955, Sidi Othman, Casablanca, Morocco, broumisaid78@gmail.com ,s.broumi@flbenmsik.ma
** Department of Mathematics, University of New Mexico, 705 Gurley Avenue, Gallup, NM 87301, USA,fsmarandache@gmail.com
**** Laboratory of Information Processing, Faculty of Science Ben M'Sik, University Hassan II, B.P 7955, Sidi Othman, Casablanca, Morocco, taleamohamed@yahoo.fr
**** Ecole Royale Navale, Boulevard Sour Jdid, B.P 16303 Casablanca, Morocco, assiabakali@yahoo.fr

Geliş Tarihi / Received: 08.07.2019
Kabul Tarihi / Accepted: 18.12.2019

I. Introduction

In 1995, the concept of the neutrosophic sets (NS for short) and neutrosophic logic were introduced by Smarandache (2005, 2006) in order to efficiently handle the indeterminate and inconsistent information which exist in real world. Unlike fuzzy sets which associate to each member of the set a degree of membership T and intuitionistic fussy sets which associate a degree of membership T and a degree of non-membership F, T, F [0, 1], Neutrosophic sets characterize each member x of the set with a truth-membership function , an indeterminacy-membership function and a falsity- membership function each of which belongs to the non-standard unit interval]−0, 1+[. Thus, although in some case intuitionistic fuzzy sets consider a particular indeterminacy or hesitation margin, . Neutrosophic set has the ability of handling uncertainty in a better way since in case of neutrosophic set indeterminacy is taken care of separately. Neutrosophic sets is a generalization of the theory of fuzzy set (Zadeh, 1965), intuitionistic fuzzy sets (Atanassov 1986), interval-valued fuzzy sets (Turksen) and interval-valued intuitionistic fuzzy sets (Atanassov.and Gargov,1989). However, the neutrosophic theory is difficult to be directly applied in real scientific and engineering areas. To easily use it in science and engineering areas, in 2005, Wang et al. (2010)proposed the concept of SVNS, which differ from neutrosophic sets only in the fact that in the former's case, the of truth, indeterminacy and falsity membership functions belongs to [0, 1]. Recent research works on neutrosophic set theory and its applications in various fields are progressing rapidly (http://fs.gallup.unm.edu/NSS;Abdel-Basetetal,2019 ;2019a ;Broumi al,2017a,2017b,2018,2019b,2019c,2019d,2019e,2019f)]. Very recently Subas et al (2015)presented the concept of triangular and trapezoidal neutrosophic numbers and applied to multiple-attribute decision making problems. Then, Biswas et al(2014) presented a special case of trapezoidal neutrosophic numbers including triangular fuzzy numbers neutrosophic sets and applied to multiple-attribute decision making problems by introducing the cosine similarity measure. Deli and Subas (2016) presented the single valued triangular neutrosophic numbers (SVN-numbers) as a generalization of the intuitionistic triangular fuzzy numbers and proposed a methodology for solving multiple-attribute decision making problems with SVN-numbers.

The shortest path problem (SPP) which concentrates on finding a shortest path from a source node to other node, is a fundamental network optimization problem that has been appeared in many domain including, road networks application, transportation, routing in communication channels and scheduling problems and various fields. The main objective of the shortest path problem is to find a path with minimum length between starting node and terminal node which exist in a given network. The edge (arc) length (weight) of the network may represent the real life quantities such as, cost, time, etc. In conventional shortest path, the distances of the edge between different nodes of a network are assumed to be certain. In the literature, many algorithms have been developed with the weights on edges on network being fuzzy numbers, intuitionistic fuzzy numbers, type-2 fuzzy numbers vague numbers (Porchelvi and Sudha ,2013 ;.Jayagowri and Ramani,2014 ;Anuuya.and Sathya,2013; Kumar and Kaur,2011; Majumdaer and Pal,2013;Kumar and Kaur 2011a).

In more recent times, Broumi et al. (2016;2016a;2016b ;2016c ;2016d ;2016e) presented the concept of neutrosophic graphs, interval valued neutrosophic graphs and bipolar single valued neutrosophic graphs and studied some of their related properties. Also, Smarandache (2015;2015a) proposed another variant of neutrosophic graphs based on literal indeterminacy. Up to date, few papers dealing with shortest path problem in neutrosophic environment have been developed. The paper proposed by (Broumi et al, 2017) is one of the first on this subject. The authors proposed an algorithm for solving neutrosophic shortest path problem based on score function. The same authors (Broumi et al, 2016)proposed another algorithm for solving shortest path problem in a bipolar neutrosophic environment. Also, in (Broumi et al, 2019)they proposed the shortest path algorithm

in a network with its edge lengths as interval valued neutrosophic numbers. However, till now, single valued triangular neutrosophic numbers have not been applied to shortest path problem. The main objective of this paper is to propose an approach for solving shortest path problem in a network where the edge weights are represented by single valued triangular neutrosophic numbers.

In order to do, the paper is organized as follows: In Section 2, we firstly review some basic concepts about neutrosophic sets, single valued neutrosophic sets and single valued triangular neutrosophic sets. In Section 3, we propose some modified operations of single valued triangular neutrosophic numbers. In Section 5, we propose an algorithm for finding the shortest path and shortest distance in single valued triangular neutrosophic graph. In Section 6, we presented an hypothetical example which is solved by the proposed algorithm. Finally, some concluding remarks are presented in Section 7.

II. PRELIMINARIES

In this section, some basic concepts and definitions on neutrosophic sets, single valued neutrosophic sets and single valued triangular neutrosophic sets are reviewed from the literature.

Definition 2.1 (Smarandache,2005).. Let X be a space of points (objects) with generic elements in X denoted by x; then the neutrosophic set A (NS A) is an object having the form A = {< x: $T_A(x)$, $I_A(x)$, $F_A(x)$>, x ∈ X}, where the functions T, I, F: X→$]^{-}0,1^{+}[$define respectively the truth-membership function, an indeterminacy-membership function, and a falsity-membership function of the element x ∈ X to the set A with the condition:

$$^{-}0 \le T_A(x) + I_A(x) + F_A(x) \le 3^{+}. \qquad (1)$$

The functions $T_A(x)$, $I_A(x)$ and $F_A(x)$ are real standard or nonstandard subsets of $]^{-}0,1^{+}[$.

Since it is difficult to apply NSs to practical problems, Wang et al. [7] introduced the concept of a SVNS, which is an instance of a NS and can be used in real scientific and engineering applications.

Definition 2.2 (Wang et al,2010)**.** Let X be a space of points (objects) with generic elements in X denoted by x. A single valued neutrosophic set A (SVNS A) is characterized by truth-membership function $T_A(x)$, an indeterminacy-membership function $I_A(x)$, and a falsity-membership function $F_A(x)$. For each point x in X $T_A(x)$, $I_A(x)$, $F_A(x) \in$ [0, 1]. A SVNS A can be written as

$$A = \{< x: T_A(x), I_A(x), F_A(x) >, x \in X\} \qquad (2)$$

Definition 2.3 (Deli and Subas, 2016). A single valued triangular neutrosophic number (SVTrN-number) $\tilde{a} = <(a_1, b_1, c_1); T_a, I_a, F_a>$ is a special neutrosophic set on the real number set *R*, whose truth membership, indeterminacy-membership, and a falsity-membership are given as follows

$$T_a(x) = \begin{cases} (x - a_1)T_a / (b_1 - a_1) & (a_1 \le x \le b_1) \\ T_a & (x = b_1) \\ (c_1 - x)T_a / (c_1 - b_1) & (b_1 \le x \le c_1) \\ 0 \qquad otherwise \end{cases} \qquad (3)$$

$$I_a(x)=\begin{cases}(b_1-x+I_a(x-a_1))/(b_1-a_1) & (a_1\le x\le b_1)\\ I_a & (x=b_1)\\ (x-b_1+I_a(c_1-x))/(c_1-b_1) & (b_1\le x\le c_1)\\ 1 \quad otherwise\end{cases} \tag{4}$$

$$F_a(x)=\begin{cases}(b_1-x+F_a(x-a_1))/(b_1-a_1) & (a_1\le x\le b_1)\\ F_a & (x=b_1)\\ (x-c_1+F_a(c_1-x))/(c_1-b_1) & (b_1\le x\le c_1)\\ 1 \quad otherwise\end{cases} \tag{5}$$

Where $0\le T_a\le 1;\ 0\le I_a\le 1;\ 0\le F_a\le 1$ and $0\le T_a+I_a+F_a\le 3;\ a_1,b_1,c_1\in R$

Definition 2.4 (Deli and Subas, 2016). Let $\tilde{A}_1=<(a_1,a_2,a_3);T_1,I_1,F_1>$ and $\tilde{A}_2=<(b_1,b_2,b_3);T_2,I_2,F_2>$ be two single valued triangular neutrosophic numbers. Then, the operations for SVTrN-numbers are defined as follows.

(i) $\tilde{A}_1\oplus\tilde{A}_2=<(a_1+b_1,a_2+b_2,a_3+b_3);\min(T_1,T_2),\max(I_1,I_2),\max(F_1,F_2)>$ (6)

(ii) $\tilde{A}_1\otimes\tilde{A}_2=<(a_1b_1,a_2b_2,a_3b_3);\min(T_1,T_2),\max(I_1,I_2),\max(F_1,F_2))$ (7)

(iii) $\lambda\tilde{A}_1=<(\lambda a_1,\lambda a_2,\lambda a_3);\min(T_1,T_2),\max(I_1,I_2),\max(F_1,F_2)>$ (8)

A convenient method for comparing two single valued triangular neutrosophic numbers is by using of score function and accuracy function.

Definition 2.5(Deli and Subas, 2016). Let $\tilde{A}_1=<(a_1,a_2,a_3);T_1,I_1,F_1>$ be a single valued triangular neutrosophic number. Then, the score function $s(\tilde{A}_1)$ and accuracy function $a(\tilde{A}_1)$ of a SVTrN-numbers are defined as follows:

(i) $s(\tilde{A}_1)=\left(\frac{1}{12}\right)[a_1+2a_2+a_3]\times[2+T_1-I_1-F_1]$ (9)

(ii) $a(\tilde{A}_1)=\left(\frac{1}{12}\right)[a_1+2a_2+a_3]\times[2+T_1-I_1+F_1]$ (10)

Definition 2.6 (Deli and Subas, 2016). Let $\tilde{A}_1$ and $\tilde{A}_2$ be two SVTrN-numbers the ranking of $\tilde{A}_1$ and $\tilde{A}_2$ by score function and accuracy function are defined as follows :

(i) If $s(\tilde{A}_1)\prec s(\tilde{A}_2)$ then $\tilde{A}_1\prec\tilde{A}_2$

(ii) If $s(\tilde{A}_1)=s(\tilde{A}_2)$ and if

(1) $a(\tilde{A}_1)\prec a(\tilde{A}_2)$ then $\tilde{A}_1\prec\tilde{A}_2$

(2) $a(\tilde{A}_1)\succ a(\tilde{A}_2)$ then $\tilde{A}_1\succ\tilde{A}_2$

(3) $a(\tilde{A}_1)=a(\tilde{A}_2)$ then $\tilde{A}_1=\tilde{A}_2$

III. ARITHMETIC OPERATIONS BETWEEN TWO SV-TRIANGULAR NEUTROSOPHIC NUMBERS

In this subsection, a slight modification has been made on some operations between two single valued triangular neutrosophic numbers proposed by (Deli and Subas, 2016) required for the proposed algorithm.

Let $\tilde{A}_1 =< (a_1, a_2, a_3); T_1, I_1, F_1 >$ and $\tilde{A}_2 =< (b_1, b_2, b_3); T_2, I_2, F_2 >$ are two single valued triangular neutrosophic numbers,. Then the operations for SVTrNNs are defined ad below:

(i) $\tilde{A}_1 \oplus \tilde{A}_2 =< (a_1 + b_1, a_2 + b_2, a_3 + b_3); T_1 + T_2 - T_1T_2, I_1I_2, F_1F_2 >$ (11)

(ii) $\tilde{A}_1 \otimes \tilde{A}_2 =< (a_1 b_1, a_2 b_2, a_3 b_3); T_1T_2, I_1 + I_2 - I_1I_2, F_1 + F_2 - F_1F_2) >$ (12)

(iii) $\lambda\tilde{A}_1 =< (\lambda a_1, \lambda a_2, \lambda a_3); 1-(1-T_1)^{\lambda}), I_1^{\lambda}, F_1^{\lambda}) >$ (13)

IV. NETWORK TERMINOLOGY

Consider a directed network G = (V, E) consisting of a finite set of nodes V={1, 2,…,n} and a set of m directed edges $E \subseteq V \times V$. Each edge is denoted by an ordered pair (i, j) where i, j $\in$ V and $i \neq j$. In this network, we specify two nodes, denoted by s and t, which are the source node and the destination node, respectively. We define a path P_{ij} ={i= $i_1, (i_1, i_2), i_2, \ldots, i_{l-1}, (i_{l-1}, i_l), i_l$ =j}as sequence that joins two nodes of edges. The existence of at least one path P_{si} in G (V, E) is assumed for every i $\in$ V-{s}.

d_{ij} denotes a single valued triangular neutrosophic number associated with the edge (i ,j), corresponding to the length necessary to traverse (i, j) from i to j. In real problems, the lengths correspond to the cost, the time, the distance, etc. Then, neutrosophic distance along the path P is denoted as d(P) is defined as

$$d(P) = \sum_{(i,j \in P)} d_{ij} \qquad (14)$$

Remark1 : A node i is said to be predecessor node of node j if
(i) Node i is directly connected to node j.
(ii) The direction of path connecting node i and j from i to j.

V . SINGLE VALUED TRIANGULAR NEUTROSOPHIC PATH PROBLEM

In this section, motivated by the work of Kumar and Kaur (2011) an algorithm is presented for finding the shortest path between the source node (i) and the destination node (j) in a network where the edges weight are characterized by a single valued triangular neutrosophic numbers.

The steps of the algorithm are:

Step1: Assume $\tilde{d}_1 =< (0,0,0); 0,1,1 >$ and label the source node (say node1) as [$\tilde{d}_1 =< (0,0,0); 0,1,1 >$,-]. The label indicating that the node has no predecessor.

Step 2: Find $\tilde{d}_j$ = minimum{ $\tilde{d}_i \oplus \tilde{d}_{ij}$ };j=2,3,…,n.

Step 3: If minimum occurs corresponding to unique value of i i.e., i= r then label node j as [$\tilde{d}_j$, r]. If minimum occurs corresponding to more than one values of i then it represents that there are more

than one single valued triangular neutrosophic path between source node and node j but single valued triangular neutrosophic distance along path is $\tilde{d}_j$, so choose any value of i.

Step 4: Let the destination node (node n) be labeled as [$\tilde{d}_n$, *l*], then the single valued triangular neutrosophic shortest distance between source node and destination node is $\tilde{d}_n$.

Step 5: Since destination node is labeled as [$\tilde{d}_n$,*l*], to find the single valued triangular neutrosophic shortest path between source node and destination node, check the label of node *l*. Let it be [$\tilde{d}_l$, p], now check the label of node p and so on. Repeat the same procedure until node 1 is obtained.

Step 6: Now the single valued triangular neutrosophic shortest path can be obtained by combining all the nodes obtained by the step 5.

Remark 5.1 Let $\tilde{A}_i$; i =1, 2,…, n be a set of single valued triangular neutrosophic numbers, if S($\tilde{A}_k$) < S($\tilde{A}_i$), for all i, the single valued triangular neutrosophic number is the minimum of $\tilde{A}_k$.

After describing the proposed algorithm, in next section, an hypothetical example is presented and the proposed method is explained completely.

V. ILLUSTRATIVE EXAMPLE

In this section an hypothetical example is introduced to verify the proposed. Consider the network shown in Fig. 1; we want to obtain the shortest path from node 1 to node 6 where edges have a single valued triangular neutrosophic numbers. Let us now apply the proposed algorithm to the network given in Fig.1.

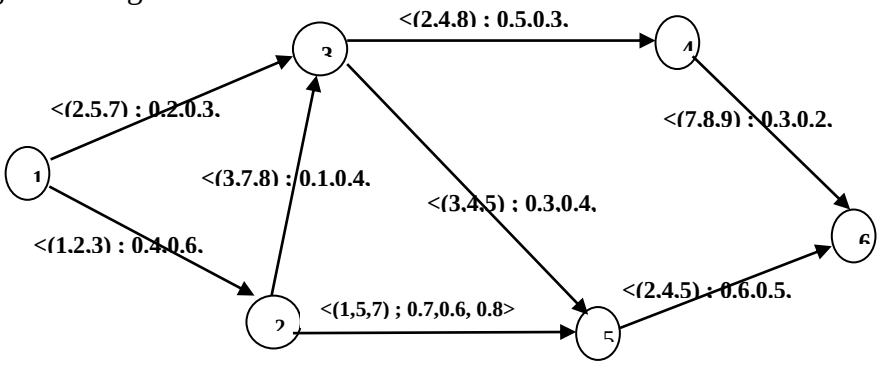


Fig. 1. A Network with single valued triangular neutrosophic edges.

In this network each edge have been assigned to single valued triangular neutrosophic number as follows:

Table 1: Weights of the graphs

Edges	Single Valued Triangular Neutrosophic Distance
1-2	<(1, 2,3);0.4,0.6,0.7>
1-3	<(2,5,7);0.2,0.3,0.4>
2-3	<(3,7,8);0.1,0.4,0.6>
2-5	<(1,5,7);0.7,0.6,0.8>
3-4	<(2,4,8);0.5,0.3,0.1>
3-5	<(3, 4,5);0.3,0.4,0.7>
4-6	<(7, 8,9);0.3,0.2,0.6>
5-6	<(2,4,5);0.6,0.5,0.3>

The calculations for this problem are as follows:

Node 6 is assumed to be the destination node,n= 6.

Assume $\tilde{d}_1 = <(0, 0, 0); 0, 1, 1>$ and label the source node (say node 1) as [$<(0, 0, 0); 0, 1, 1>$,-], the value of $\tilde{d}_j$; j= 2, 3, 4, 5 ,6 can be obtained as follows:

Iteration1: Since only node 1 is the predecessor node of node 2, so putting i=1 and j= 2 in step of the proposed algorithm, the value of $\tilde{d}_2$ is

$\tilde{d}_2 = \min\{\tilde{d}_1 \oplus \tilde{d}_{12}\}$=min{<(0, 0, 0); 0, 1, 1>$\oplus$ <(1, 2, 3); 0.4, 0.6, 0.7>= <(1, 2, 3); 0.4, 0.6, 0.7>

Since minimum occurs corresponding to i=1, so label node 2 as [<(1, 2, 3); 0.4, 0.6, 0.7>, 1]

$\tilde{d}_2$ = <(1, 2, 3); 0.4, 0.6, 0.7>

Iteration 2: The predecessor node of node 3 are node 1 and node 2, so putting i= 1, 2 and j= 3 in step 2 of the proposed algorithm, the value of $\tilde{d}_3$ is $\tilde{d}_3 = \min\{\tilde{d}_1 \oplus \tilde{d}_{13}, \tilde{d}_2 \oplus \tilde{d}_{23}\}$=min{<(0, 0, 0); 0, 1, 1>$\oplus$ <(2, 5, 7); 0.2, 0.3, 0.4>, <(1, 2, 3); 0.4, 0.6, 0.7>$\oplus$ <(3, 7, 8); 0.1, 0.4, 0.6>}= min<(2, 5, 7); 0.2, 0.3, 0.4> , <(4, 9, 11); 0.46, 0.24, 0.42>}

Using Eq.9, we have

S ({<(2, 5, 7); 0.2, 0.3, 0.4>) = $\left(\frac{1}{12}\right)\left[a_1 + 2a_2 + a_3\right] \times \left[2 + T_1 - I_1 - F_1\right]$=2.38

S (<(4, 9, 11); 0.46, 0.24, 0.42>) =4.95

Since S ({<(2, 5, 7); 0.2, 0.3, 0.4>) < S (<(4, 9, 11); 0.46, 0.24, 0.42>)

So min{<(2, 5, 7); 0.2, 0.3, 0.4> , <(4, 9, 11); 0.46, 0.24, 0.42>} = <(2, 5, 7); 0.2, 0.3, 0.4>

Since minimum occurs corresponding to i=1, so label node 3 as [<(2, 5, 7); 0.2, 0.3, 0.4>, 1]

$\tilde{d}_3$ =<(2, 5, 7); 0.2, 0.3, 0.4>

Iteration 3: The predecessor node of node 4 is node 3, so putting i= 3 and j= 4 in step 2 of the proposed algorithm, the value of $\tilde{d}_4$ is $\tilde{d}_4 = \min\{\tilde{d}_3 \oplus \tilde{d}_{34}\}$=min{<(2, 5, 7); 0.2, 0.3, 0.4> $\oplus$ <(2, 4, 8); 0.5, 0.3, 0.1> }=<(4, 9, 15,); 0.6, 0.09, 0.04>

So min {<(2, 5, 7); 0.2, 0.3, 0.4>, $\oplus$ <(2, 4, 8); 0.5, 0.3, 0.1> }= <(4, 9, 15); 0.6, 0.09, 0.04>

Since minimum occurs corresponding to i=3, so label node 4 as [<(4, 9, 15); 0.6, 0.09, 0.04>,3]

$\tilde{d}_4$ =<(4, 9, 15); 0.6, 0.09, 0.04>

Iteration 4: The predecessor node of node 5 are node 2 and node 3, so putting i= 2, 3and j= 5 in step 2 of the proposed algorithm, the value of $\tilde{d}_5$ is $\tilde{d}_5 = \min\{\tilde{d}_2 \oplus \tilde{d}_{25}, \tilde{d}_3 \oplus \tilde{d}_{35}\}$=min{<(1, 2, 3); 0.4, 0.6, 0.7>$\oplus$ <(1, 5, 7); 0.7, 0.6, 0.8>, <(2, 5, 7); 0.2, 0.3, 0.4>$\oplus$ <(3, 4, 5); 0.3, 0.4, 0.7>}= min{<(2, 7, 10); 0.82, 0.36, 0.56>, <(5, 9, 12); 0.44, 0.12, 0.28>}

Using Eq.9, we have

S (<(2, 7, 10); 0.82, 0.36, 0.56>) =4.12

S (<(5, 9, 12); 0.44, 0.12, 0.28>) =5.13

Since S (<(2, 7, 10); 0.82, 0.36, 0.56>) < S (<(5, 9, 12); 0.44, 0.12, 0.28>)

minimum{<(2, 7, 10); 0.82, 0.36, 0.56>, <(5, 9, 12); 0.44, 0.12, 0.28>}

= <(2, 7, 10); 0.82, 0.36, 0.56>

$\tilde{d}_5$ = <(2, 7, 10); 0.82, 0.36, 0.56>

Since minimum occurs corresponding to i=2, so label node 5 as [<(2, 7, 10); 0.82, 0.36, 0.56>, 2]

Iteration 5: The predecessor node of node 6 are node 4 and node 5, so putting i= 4, 5and j= 6 in step 2 of the proposed algorithm, the value of $\tilde{d}_6$ is $\tilde{d}_6$ =min{ $\tilde{d}_4 \oplus \tilde{d}_{46}, \tilde{d}_5 \oplus \tilde{d}_{56}$ }=min{<(4, 9, 15); 0.6, 0.09, 0.04> $\oplus$ <(7, 8, 9); 0.3, 0.2, 0.6>, <(2, 7, 10); 0.82, 0.36, 0.56> $\oplus$ <(2, 4, 5); 0.6, 0.5, 0.3>}= min{<(11, 17, 24); 0.72, 0.018, 0.024>, <(4, 11, 15); 0.93, 0.18, 0.17>}

Using Eq.9, we have

S (<(11, 17, 24); 0.72, 0.018, 0.024>) =15.40

S (<(4, 11, 15); 0.93, 0.18, 0.17>) =8.82

Since S (<(4, 11, 15); 0.93, 0.18, 0.17>) < S (<(11, 17, 24); 0.72, 0.018, 0.024>)

So min{<(11, 17, 24); 0.72, 0.018, 0.024>, <(4, 11, 15); 0.93, 0.18, 0.17>}

= <(4, 11, 15); 0.93, 0.18, 0.17>

$\tilde{d}_6$ =<(4, 11, 15); 0.93, 0.18, 0.17>

Since minimum occurs corresponding to i= 5, so label node 6 as [<(4, 11, 15); 0.93, 0.18, 0.17>, 5]

Since node 6 is the destination node of the given network, so the single valued triangular neutrosophic shortest distance between node 1 and node 6 is <(4, 11, 15); 0.93, 0.18, 0.17>. Now the single valued triangular neutrosophic shortest path between node 1 and node 6 can be founded by using the following procedure:

Since node 6 is labeled by [<(4, 11, 15); 0.93, 0.18, 0.17>, 5], which represents that we are coming from node 5. Node 5 is labeled by [<(2, 7, 10); 0.82, 0.36, 0.56>, 2], which represent that we are coming from node 2. Node 2 is labeled by [<(1, 2, 3); 0.4, 0.6, 0.7>, 1], which represents that we are coming from node 1. Now the single valued triangular neutrosophic shortest path between node 1 and node 6 is obtaining by joining all the obtained nodes. Hence the single valued triangular neutrosophic shortest path $1 \to 2 \to 5 \to 6$.

The single valued triangular neutrosophic shortest distance and the single valued triangular neutrosophic shortest path of all nodes from node 1 is depicted in the table 2 and the labeling of each node is shown in Fig.2.

TABLE 2: Tabular representation of different single valued triangular neutrosophic shortest paths

Node No.(j)	$\tilde{d}_i$	**Single Valued Triangular Neutrosophic Shortest Path Between jth and 1st node**
2	<(1, 2, 3); 0.4, 0.6, 0.7>	$1 \rightarrow 2$
3	<(2, 5, 7); 0.2, 0.3, 0.4>	$1 \rightarrow 3$
4	<(4, 9, 15); 0.6, 0.09, 0.04>	$1 \rightarrow 3 \rightarrow 4$
5	<(2, 7, 10); 0.82, 0.36, 0.56>	$1 \rightarrow 2 \rightarrow 5$
6	<(4, 11, 15); 0.93, 0.18, 0.17>	$1 \rightarrow 2 \rightarrow 5 \rightarrow 6$

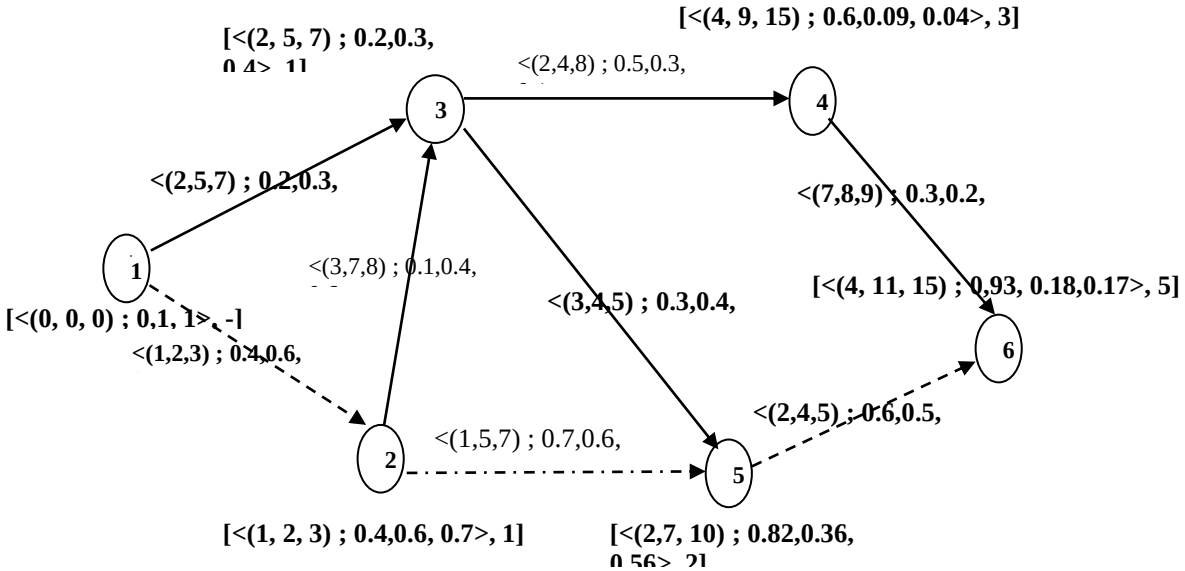


Fig.2.Network with single valued triangular neutrosophic shortest distance of each node from node 1

VI. CONCLUSION

In this article, an algorithm has been developed for solving the shortest path problem on a network where the edges weight are characterized by a neutrosophic numbers called single valued triangular neutrosophic numbers. To show the performance of the proposed methodology for the shortest path problem, an hypothetical example was introduced. In future works, we studied the shortest path problem in complex neutrosophic environment and we will research the application of this algorithm.

REFERENCES

Abdel-Baset M., Chang V., & Gamal A. (2019). "Evaluation of the green supply chain management practices: A novel neutrosophic approach". Computers in Industry 108, 210-220

Abdel-Basset M., Saleh M., Gamal A., & Smarandache F. (2019a).”An approach of TOPSIS technique for developing supplier selection with group decision making under type-2 neutrosophic number”. Applied Soft Computing 77, 438-452.

Anuuya V.and Sathya R. (2013). “Shortest Path with Complement of Type -2 Fuzzy Number”. Malya Journal of Matematik, S(1), 71-76.

Atanassov K. (1986). “Intuitionistic Fuzzy Sets”. Fuzzy Sets and Systems 20, 87-96.

Atanassov K. and Gargov G. (1989). “Interval Valued Intuitionisitic Fuzzy Sets”. Fuzzy Sets and Systems 31, 343-349.

Biswas P., Parmanik S. and Giri B. C. (2014). “Cosine Similarity Measure Based Multi-attribute Decision- Making With Trapezoidal Fuzzy Neutrosophic Numbers”.Neutrosophic sets and systems 8, 47-57.

Broumi S. and Talea M. and Bakali A. and Smarandache F. and Khan M. (2017). “A Bipolar Single Valued Neutrosophic Isolated Graphs: Revisited”. International Journal of New Computer Architectures and their Applications (IJNCAA) 7(3), 89-94

Broumi S. , Talea M., Bakali A. , Smarandache F. , Nagarajan D., Lathamaheswari M. and Parimala M. (2019e). “Shortest path problem in fuzzy, intuitionistic fuzzy and neutrosophic environment: an overview”. Complex & Intelligent Systems , ,1-8, https://doi.org/10.1007/s40747-019-0098-z

Broumi S., Bakali A., Talea M., Smarandache F., Ali M. (2016f). “Shortest Path Problem Under Bipolar Neutrosophic Setting”.Applied Mechanics and Materials 859, 59-66

Broumi S., A. Dey, M. Talea, A. Bakali, F. Smarandache, D. Nagarajan, M. Lathamaheswari and Ranjan Kumar (2019d), “Shortest Path Problem using Bellman Algorithm under Neutrosophic Environment”.Complex & Intelligent Systems ,1-8, https://doi.org/10.1007/s40747-019-0101-8,

Broumi S., Bakali A., Talea M. and Smarandache F. (2016b). “Isolated Single Valued Neutrosophic Graphs”. Neutrosophic Sets and Systems 11, 74-78.

Broumi S., Bakali A., Talea M. and Smarandache F., “Shortest Path Problem on Single Valued Neutrosophic Graphs”, 2017 International Symposium on Networks, Computers and Communications (ISNCC): Wireless and Mobile Communications and Networking - Wireless and Mobile Communications and Networking, 978-1-5090-4260-9/17/$31.00 ©2017 IEEE .

Broumi S., Bakali A., Talea M. and Smarandache F., Şahin R., Krishnan Kishore K. P., (2019a).”Shortest Path Problem Under Interval Valued Neutrosophic Setting” .International Journal of Advanced Trends in Computer Science and Engineering 8, No.1.1, 216-222.

Broumi S., Bakali A., Talea M., Smarandache F. (2017a). “A Matlab Toolbox for interval valued neutrosophic matrices for computer applications”. Uluslararası Yönetim Bilişim Sistemlerive Bilgisayar Bilimleri Dergisi, 1(1),1-21

Broumi S., Bakali A., Talea M., Smarandache F., and Singh P. K.(2019b). “Properties of Interval-Valued Neutrosophic Graphs”, in :C. Kahraman and ˙ I. Otay (eds.), Fuzzy Multicriteria Decision MakingUsingNeutrosophic Sets, Studies in Fuzziness and Soft Computing 369,https://doi.org/10.1007/978-3-030-00045-5_8

Broumi S., Bakali A., Talea M., Smarandache F., Uluçay V., Sahin M., Dey A., Dhar M., Tan R.P., Bahnasse A., Pramanik S. (2018). “Neutrosophic Sets: An Overview”, In book: New Trends in Neutrosophic Theory and Applications, Edition: Volume 2, Publisher: pons edition, Editors: FlorentinSmarandache, SurapatiPramanik, 403-434

Broumi S., Nagarajan D. , Bakali A. , Talea M. , Smarandache F. , Lathamaheswari M.(2019f).”The shortest path problem in interval valued trapezoidal and triangular neutrosophic environment”. Complex & Intelligent Systems,1-12, https://doi.org/10.1007/s40747-019-0092-5.

Broumi S., Smarandache F., Talea M. and Bakali A. (2016b).”An Introduction to Bipolar Single Valued Neutrosophic Graph Theory”. Applied Mechanics and Materials 841, 184-191.

Broumi S., Smarandache F., Talea M. and Bakali A. (2016d). "Decision-Making Method Based On the Interval Valued Neutrosophic Graph". Future Technologie, IEEE, 44-50.

Broumi S., Son L.H., Bakali A., Talea M., Smarandache F., Selvachandran G. (2017b). "Computing Operational Matrices in Neutrosophic Environments: A Matlab Toolbox".Neutrosophic Sets and Systems18, 58-66

Broumi S., Talea M., Bakali A. and Smarandache F. (2016a).On Bipolar Single Valued Neutrosophic Graphs".Journal Of New Theory 11, 84-102.

Broumi S., Talea M., Bakali A., Smarandache F. (2016). "Single Valued Neutrosophic Graphs. Journal of New Theory 10, 86-101.

Broumi S., Talea M., Bakali A., Singh P. K., Smarandache F. (2019c). "Energy and Spectrum Analysis of Interval Valued Neutrosophic Graph using MATLAB". Neutrosophic Sets and Systems 24, 46-60.

Broumi S., Talea M., Smarandache F. and Bakali A.(2016e)."Single Valued Neutrosophic Graphs: Degree, Order and Size". IEEE International Conference on Fuzzy Systems (FUZZ), 2444-2451.

Deli I. and Subas Y. (2016). "A Ranking methods of single valued neutrosophic numbers and its application to multi-attribute decision making problems". International Journal of Machine Learning and Cybernetics, 1-14.

http://fs.gallup.unm.edu/NSS.

Jayagowri P. and Ramani G.G(2014). "Using Trapezoidal Intuitionistic Fuzzy Number to Find Optimized Path in a Network", Volume 2014. Advances in Fuzzy Systems, 6 pages.

Kumar A. and Kaur M. (2011a). "Solution of fuzzy maximal flow problems using fuzzy linear programming". World Academy of Science and Technology87, 28-31.

Kumar A. and Kaur M. (2011). "A New Algorithm for Solving Shortest Path Problem on a Network with Imprecise Edge Weight". Applications and Applied Mathematics 6(2), 602-619.

Majumdaer S. and Pal A. (2013). "Shortest Path Problem on Intuitionistic Fuzzy Network". Annals of Pure and Applied Mathematics 5, No.1, 26-36.

Nagarajan D., Lathamaheswari M., Broumi S., Kavikumar J. (2019). "A new perspective on traffic control management using triangular interval type-2 fuzzy sets and interval neutrosophic sets". Operations Research Perspectives, https://doi.org/10.1016/j.orp.2019.100099.

Porchelvi R. S. and Sudha G. (2013). "A modified a algorithm for solving shortest path problem with intuitionistic fuzzy arc length".International Journal and Engineering Research 4,issue 10, 884-847.

Smarandache F. (2005). A unifying field in logic. Neutrosophy: Neutrosophic probability, set, logic, American Research Press, Rehoboth, fourth edition,

Smarandache F., Neutrosophic set- a generalization of the intuitionistic fuzzy set, Granular Computing. 2006 IEEE International Conference, 2006, 38-42.

Smarandache F., (2015a) "symbolic Neutrosophic Theory", Europanova asbl, Brussels, , 195p.

Smarandache F., "Types of Neutrosophic Graphs and neutrosophic Algebraic Structures together with their Applications in Technology," seminar, Universitatea Transilvania din Brasov, Facultatea de Design de Produs si Mediu, Brasov, Romania 06 June 2015

Subas Y., "Neutrosophic numbers and their application to multi-attribute decision making problems",(in Turkish) (master Thesis, 7 Aralk university. Graduate School of Natural and Applied Science, 2015.

ŞAHİN R., Peide Liu, "Maximizing deviation method for neutrosophic multiple attribute decision making with incomplete weight information", Neural Computing and Applications

Turksen I., "Interval Valued Fuzzy Sets based on Normal Forms". Fuzzy Sets and Systems20, 191-210.

Wang H., Smarandache F., Zhang Y.and Sunderraman R. (2010). "Single Valued Neutrosophic Sets". Multispace and Multisrtucture 4, pp.410-413.

Zadeh L. (1965). "Fuzzy Sets". Information and Control 8, 338-353.

DİJİTAL VERİLERİN İMHA SÜREÇLERİNİN TANIMLANMASI VE UYGULAMA YÖNÜNDEN DEĞERLENDİRİLMESİ

***

IDENTIFICATION OF THE DATA DESTRUCTION PROCESS OF DIGITAL DATA AND CONSIDERING IN TERMS OF APPLICATION

DOI: 10.33461/uybisbbd.598590

İlker KARA*

Öz

Gelişen teknolojiyle toplumun her sektörünün dijitalleşme ve iş modellerinin değişmesiyle birlikte düzenli veya düzensiz büyük miktarda veri çıktıları oluşmaktadır. Elde edilen bu verilerin analitik yöntemlerle işlenmesi sonucunda depolanabilmekte, uygun şifreleme yöntemleriyle saklanabilmekte ya da ihtiyaç doğrultusunda kullanılabilmektedir. Dijital verilerin sağladığı bu kolaylıkların yanı sıra büyük miktardaki verilerin yetkisiz kişilerin eline geçmemesi için imha edilmesi son zamanlarda büyük bir sorun haline gelmiştir. Literatürde yapılan çalışmalar genellikle verilerin korunmasına yönelik yapılmış olup, verilerin güvenli imha süreçlerine çok fazla değinilmemiştir. Bu çalışmada dijital verilerin imha süreçleri uygulama yönünden detaylı olarak incelenmiştir.

***Anahtar Kelimeler**: dijital veriler, kişisel veriler, imha.*

Abstract

With the digitalization of every sector, the society and the change of business models, a large amount of data outputs are formed regularly or irregularly. Obtained materials becomes storable as a result of analytical processing and it can be stored with appropriate encryption method or it can be used according to requirements. In adition to the ease of digital data,the destruction of large amounts of data to prevent unauthorized access has become a growing problem lately. Stuides in literature were generally done to protect data but the safe destruction of data has not been addressed much. In this study, the destruction of the processes of digital data was examined in detail.

***Keywords:** digital data, personal data, destruction.*

* Dr. Öğretim Üyesi Çankırı Karatekin Üniversitesi Sağlık Meslek Yüksek Okulu, karaikab@gmail.com
ORCID: 0000-0003-3700-4825

Geliş Tarihi / Received: 30.07.2019
Kabul Tarihi / Accepted: 17.10.2019

1. GİRİŞ

Veri (ing: data); incelenen konu hakkında yapılan araştırma, incelenme, analiz, veya öneriler sonucunda meydana gelen işlenmemiş, farklı kullanıcılar tarafından üzerinde yorum yapmaya imkan sağlayan işlenmemiş ham bilgilere denilmektedir (Yıldız, 2006:157). Dijital veri ise bilişim sistemleri ya da internet ortamında vasıtasıyla oluşturulmuş bilgi paketleri olarak bilinmektedir (Şengül, 2014:17). Dijital veriler, üretici tarafından uzak erişime açılabilir, farklı kullanıcılar tarafından değişiklik yapılarak farklı formatlar ile kaydedilebilmektedir (Jensen, 1986:266). Dijital veriler sahip oldukları bu avantajları nedeniyle kişisel kullanıcılar ya da resmi kuruluşlar tarafından yaygın olarak kullanılmakta birçok uygulama ve hizmetler dijital platformlara taşınmaktadır (Schroeder, 2016:15). Bu durum getirdiği kolaylıkların yanı sıra bazı problemlere de yol açmaktadır.

Bilişim ve iletişimin teknolojinin büyük bir hızla ilerlediği günümüzde birçok veri işleme ve depolama cihazları sayesinde düzenli veya düzensiz büyük miktarda veri elde edilmektedir. Her geçen gün çok hızlı bir şekilde üretilen veriler; iletişim, bankacılık, pazarlama veya kamusal alanda kullanılabilmektedir (Doğan, 2016:56). Bu verilerin türü, kapasitesine ve kullanım alanına göre farklı teknolojiler ile kullanılmakla birlikte güvenlik, erişilebilirlik veya istenmediği durumlarda güvenli olarak imha edilmesi için yeni yöntemler geliştirmeye ihtiyaç duyulmaktadır (Gantz, 2012:5). Bu gelişmelere gerekli önlemleri alamayan kurumlar veya bireysel kullanıcılar için büyük bir sorun haline gelmiştir. Bu amaçla geliştirilen yöntemler etkili olmakla beraber özellikle verilerin güvenli imhası alanında yapılan çalışmalar yetersiz kalmıştır.

2. VERİ KAVRAMI

Veri, bilginin yapılandırılarak depolanabilen hale getirilmesidir (Çetin, 2014:86, Canber, 2006:165). Anlamlı hale getirilen veriler istenilen amaç doğrultusunda bütünleştirilerek kolay analiz edilebilir hale getirilebilir. Veri, "Gizlilik, Bütünlük, Erişilebilirlik, Doğrulama, Yetkilendirme ve İnkâr Edememe" gibi temeller doğrultusunda oluşturulmalıdır (Baykara vd., 2013:231). Elde edilen verilerin belirli bir formatta işlenebilmesi ve gerektiğinde ulaşılabilmesi için veri tabanları oluşturulmuştur. Veri tabanları kullanıcılara verileri kullanarak işlem yapmalarına olanak tanımaktadırlar. Veri tabanı oluşturulması ve etkin şekilde kullanılabilmesi için özel yazılımlara ihtiyaç duyulmaktadır. (Sağıroğlu, 2008:23). Bu amaçla birçok veri tabanı sistemi oluşturulmuştur (Günümüzde en popülerleri; MySQL, Oracle, SQLite, PostgreSQL, Firebird vb.).

Dijital veriler uygun ortamlarda depolanabilme özeliklerine sahiptirler. Herman Hollerith'in geliştirildiği delikli kartlardan günümüz bulut teknolojisine (Online depolama) kadar depolama alanında birçok yöntem geliştirilmiştir (Biles, 1989:604). Depolan verilerin güvenli şekilde silinebilmesi veya yetkisiz kişilerin eline geçmemesi için doğru imhası süreçleri yürütülmesi hem kurumların hem de kullanıcılar için büyük bir sorun haline gelmiştir. Depolanan dijital veriler için literatürde herkes tarafından kabul gören bir imha yöntemi bulunmamakla beraber karşılaşılan problemlere geçici çözüm yolları bulunmuştur (Hughes, 2009:32). Bu sonuç depolanan verilerin kapasitesi büyüklüğü ve depolama cihaz alanlarının sayılarının artması çözülmesi zor bir hale neden olmaktadır (Şişkin, 2018:343). Bu çalışmanın amacı dijital verilerin imha süreçleri içeren pratik imha yöntemleri sunmaktır. Çalışma sonucunda dijital verilerin imhalarının uygulama yönünden karşılaşılabilecek sorunlara karşı çözüm önerileri sunulmuştur.

3. DİJİTAL VERİLERİN İMHA EDİLMESİNİN HUKUKİ BOYUTU

Hukuki kurallara göre uygun olarak oluşturulmuş dijital veriler çeşitli nedenlerle silinmesi gerektiğinde (İşlenmesi gereken sebepler ortadan kalktığında, kanuni zorunluluk veya kişinin rızası

gibi durumlarda) resen veya ilgili kurumun talebi doğrultusunda uygun yöntemlerle silinebilmektedir (Henkoğlu, 2017:243).

3.1. Avrupa İnsan Hakları Sözleşmesi

4 Kasım 1950'de Roma'da imzalanarak 3 Eylül 1953'te yürürlüğe giren "Avrupa İnsan Hakları Sözleşmesi" nin "Özel ve aile hayatına saygı hakkı" başlıklı 8. maddesinin 1. fıkrasına göre, "Herkes, özel ve aile hayatına, konutuna ve yazışmalarına saygı gösterilmesi hakkına sahiptir" hükümde değinilen "özel hayata saygı hakkı", kişisel verileri de içermektedir (Gölcüklü, 1994:49). İlgili 8. maddenin 2. fıkrasında; "Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasa ile öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin iktisadi refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve hürriyetlerinin korunması için alınması gereken tedbirler bakımından mümkün olabilir." hükmünü öngörülmektedir. Bu bağlamda kişisel verilere kişinin rızasının olmadığı durumlarda yapılan müdahaleler suç kapsamında değerlendirilmektedir.

3.2. Türkiye Cumhuriyeti Anayasası

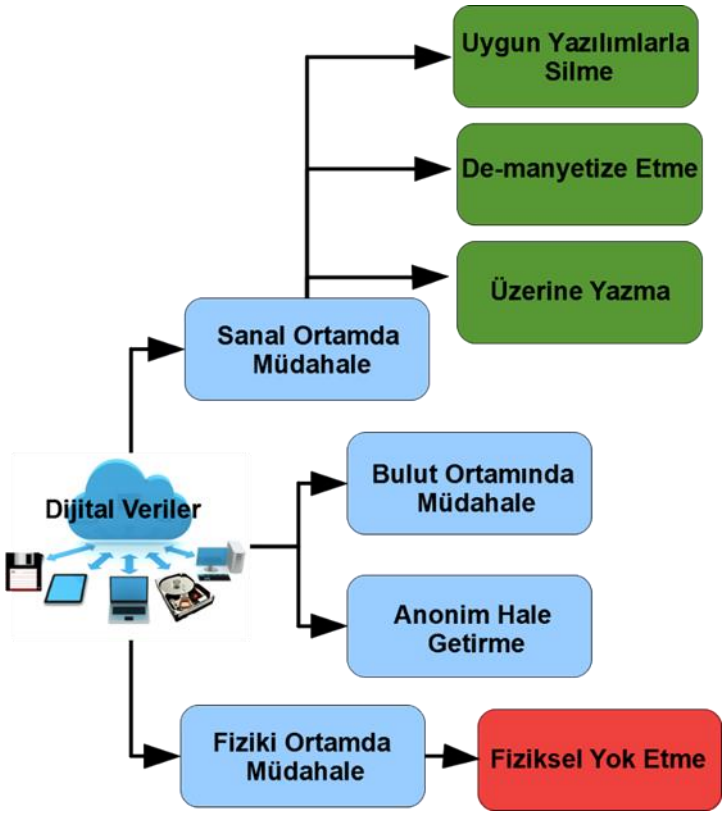
7 Kasım 1982'de yürüklüğe giren 2709 numaralı Türkiye Cumhuriyeti Anayasasının 20. Maddesinin 3 fıkrasında "Herkes, kendisi ile ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığı öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızası ile düzenlenir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü ile düzenlenmiştir (Göztepe, 2011:15). İlgili hükümde kişisel verilerin mutlak korunmasını gerekliliği vurgulanmıştır. Bu bağlamda kişisel verilerin yalnızca kişinin açık rızasıyla işlenebileceği ve kişisel verilerin nasıl korunacağına dair esas ve usullerin ilgili kanunla düzenleneceği öngörülmüştür.

3.3. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

7 Nisan 2016 tarihinde yürürlüğe giren "6698 Sayılı Kişisel Verilerin Korunması Kanunu", kişisel verilerin işlenmesi, özel hayatın gizliliğinin korunması ve temel hak ve özgürlükleri korumak için verilerin işlenmesi ya da silinmesi kurallarını düzenleme amaçlamaktadır (Henkoğlu, 2015:16). Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi ilgili kanun gereğince uygun şartlar altında yapılabilmektedir. Dijital verilerin kişinin rızasını içermeyecek durumlar ve üçüncü şahıslara aktarılmaması için yasal zemini oluşturulmaktadır. 6698 sayılı Kişisel Verilerin Korunması Kanununa aykırı şekilde verilerin işlenmesi durumunda 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde uyarınca bir yıldan üç yıla kadar hapis cezası verilebilmektedir.

4. DİJİTAL VERİLERİ İMHA SÜREÇLERİ

Dijital verilerin silinmesi kullanıcıların hiçbir suretle tekrar erişilemez ve kullanılamaz hale getirilmesi işlemini tanımlamaktadır (Winter, 2013:12). Bu işlemi yapan sorumlu verinin tekrar erişilemez ve kullanılamaz hale getirilmesi için gerekli tüm teknik ve yasal tedbirleri almakla mükelleftir. Dijital verilerin güvenli imhası için pratikte uygulanan ve herkes tarafından kabul gören standart bir yöntem bulunmamaktadır (Chen, 2012:648). Verilerin çeşitliliği, kapasitesi ve depolama alanlarının teknolojik altyapılarının farklılıkları imha yöntemini doğrudan etkilemektedir. Pratik ve güvenli bir imha yöntemin bilinerek doğru şekilde uygulanması dijital verilerin güvenli imhası için gereklidir. Bu amaçla uygulanabilir bir dijital veri imha yöntemi Şekil 1'de verilmiştir.



Şekil 1: Dijital Verileri İmha Yöntemleri.

Dijital verilerin kayıt ortamlarında depolanabildiklerinden kayıt ortamlarına uygun yöntemlerle imha edilmesi gerekir. Bu nedenle imha süreçleri verilerin bulunduğu ortamlara göre müdahale edilmelidir. Dijital verilerin imhası dört başlık altında toplanabilir. Bunlar;

4.1. Sanal Ortamda Müdahale

Sanal ortam, veriler ile elektronik olarak iletişim kurulabilen bir ortamı açıklamaktadır. Veriler uygun depolama cihazlarında tutulduğundan imha edilebilmesi için; Uygun yazılımlarla silme, De-manyetize etme, Üzerine yazma, Bulut (cloud) ortamında müdahale, Anonim hale getirme, Fiziki ortamda müdahale, Fiziksel yok etme adımları uygulanabilir.

4.1.1. Uygun yazılımlarla silme: Hard disk, hafıza kartları, Taşınabilir bellekler, disketler ve CD-DVD'lerde depolana verilerin kalıcı ve güvenli olarak program vasıtasıyla silinme işlemidir. Bu işlemlerde verilerin tam olarak ve güvenli bir şekilde silindiği kullanılan program vasıtasıyla doğrulanabilir. En çok kullanılan yazılımsal silme programları; Moo0 Anti-Recovery, Disk Redactor, Eraser, SDelete, FileShredder, Turbo Shredder vb.

4.1.2. De-manyetize etme: Hemen hemen tüm depolama cihazları manyetik alana duyarlı malzemelerden üretilmiştir. Bu nedenle istenmeden yüksek bir manyetik alana maruz kalması cihazın tekrar kullanılamaz hale getirebilmektedir. Bu durumdan yola çıkarak verilerin imha edilmesi istenilen cihazların çok yüksek bir manyetik değere sahip özel cihazlara uzun süreli (ortalama 1 saat) maruz kalması üzerindeki verilerin tekrar okunamayacak biçimde bozulmasına neden olmaktadır.

4.1.3. Üzerine yazma: Dijital veriler bulunduğu depolama cihazlarında 0 ve 1'lerden oluşan düzenli yapılardan oluşmaktadır. Bu yapılar üzerine rasgele 0 ve 1'lerden oluşan rasgele yazılırsa verinin kurtarılması engel olunur. Bu işlem en az yedi kez tekrarlanması gereklidir. Bu işlemler için kullanılan en yaygın programlar; Disk-Wipe, R-Wipe & Clean, HDD Data Wiping vb.

4.2. Bulut (cloud) ortamında müdahale: Bilgisayar ve benzeri internet tabanlı cihazların kullanıcılar için verilerini depolayabilen istenildiği zaman ulaşılabilenini sağlayan hizmette bulut ortamı denilmektedir. Bulut sistemindeki verilerin imhası özel programlar vasıtasıyla yapılabilmektedir. Bu programlardan en yaygın kullanılanları Office 365, Dropbox'lar, Salesforce vb. Bu tedbirlere ek olarak eğer bir bulut sisteminden hizmet alınıyorsa kullanıcılar için ayrı ayrı şifreleme anahtarı oluşturularak istenilen kullanıcının kaynak erişimi hizmet sağlayıcılara erişim anahtarı iptal edilmesi gereklidir.

4.3. Anonim hale getirme: Anonim hale getirme işlemi, verilerin tüm ya da bir kısmını silerek ya da tanınmayacak şekilde değiştirilerek verinin tanımlayıcı ve kişiselleştirici özelliklerini yok etme işlemine denilmektedir. Bu işlem sonucunda hedef veriler tamamen bağımsız hale gelerek ilgili kişiyle bağını ortadan kaldırılır. Üçüncü bir kişinin bu verilere ulaşması mevcut hali ile kişiler ile bağlantı kuramayacağında sakıncasız hale gelmektedir. Verilerin anonim hale getirmek için hedef veriler bir kısmı veya tamamı uygun yazılımlarla silme, maskeleme, gürültü ekleme gibi yöntemler uygulanmaktadır.

4.4. Fiziki ortamda müdahale: Fiziki ortamda müdahaleler, verilerin depolandığı cihazların fiziki olarak kullanılmaz hale getirilmesi için yapılan tüm işlemleri (kırma, parçalama, eritme vb.) kapsamaktadır.

4.4.1. Fiziksek yok etme: Fiziksek yok etme, depolama cihazların kimyasallar ile eritilmesi, yakılması veya öğütücülerle parçalanmasını içermektedir. Bu işlemler sonucunda veriler tam anlamıyla imha edilmiş olmaktadır. Fiziki olarak yok etme işlemi diğer süreçlere göre daha maliyetli ve zaman alıcıdır. Bu nedenle diğer süreçler ile imhası olmadığı zaman son seçenek olarak kullanılması uygun olacaktır.

Literatüre de en yaygın olarak kullanılan dijital verileri imha süreci kurumlar tarafından dijital ortamlarda tutulan kişisel verilerin silinerek bulunduğu bilişim sistemde geri getiremeyecek şekilde formatlanması üzerinedir (Oğuz,. 2018:124). Bu yöntemin kamu kurumlarda kullanılan kurum bilgisayarlarında uygulanması bazı durumlarda sakıncalar içermektedir. Olası disiplin, idari veya adli soruşturmalarda tek delillin dijital materyallerin olması halinde delilerin incelenememesi ve soruşturmanın selameti doğrudan etkilemektedir.

5. SONUÇ

Dijital verilerin oluşturulması, gizliliği, korunması veya güvenli olarak erişilebilir olması kadar önemli bir diğer husus da güvenli bir şekilde imha edilebilmesidir. Dijital verilerin imha süreçlerinde dikkat edilmesi gereken birçok önemli hususlar bulunmaktadır. Bu hususlar veri depolama şekline göre doğru imha sürecinin seçiminden verilerin geri getirilemez olarak imha edildiğinden emin olunmasına kadar çok çeşitli süreçleri içermektedir.

Veri imhası süreçleri verilerin diğer özellikleri (güvenlik, gizlilik vb.) yanında genellikle ikinci planda kalan ve önemsiz olarak görülmektedir. Bu algı geri dönülmesi zor ve çok önemli güvenlik zafiyetleri oluşturmaktadır. Bu nedenle veri imha süreçlerinin her aşamasında çok dikkatli yapılarak maksimum özen göstermek gereklidir. İmha edilecek verilerin çeşitliliği ve miktarda büyük bir sorundur. İmha edilecek verilerin türlerine ve uygun yöntemlerinin önceden belirlenmesi güvenli veri imhası ve zaman kazandırması açısından önemlidir. Bu amaçla çalışmada uygulanabilir bir dijital verileri imha yöntemi detaylı olarak incelenmiştir.

Dijital verilerin imha süreçlerinde alınabilecek önlemler iki gruba ayrılabilir;

Bunlar;

i) Fiziki tedbirler,

ii) İmha personelinin farkındalıkları,

i) Fiziki tedbirler; güvenli olarak veri imha edilecek materyallerin nerede, hangi koşullarda, nasıl, kim tarafından imha edileceğini kapsamaktadır.

ii) İmha personelinin farkındalıkları; dijital verileri imha edecek personellin teknik ve hukuki boyutuna hâkim olması için gerekli eğitimleri kapsamaktadır.

Türkiye'de dijital verilerin imha süreçleri kurumlara göre farklılıklar göstermekle birlikte birçok sorunlarla karşılaşılmaktadır. Bu alanda yapılan çalışmalarda kişisel verilerin imhasında yoğunlaşmış olup diğer veri türleri için uygulamada detaylı bir çalışma bulunmamaktadır. Bu çalışmada verilen veri imha yöntemleriyle karşılaşabilecek veri tür ve çeşitlerine göre imha süreçleri detaylı olarak tanımlanmıştır. Çalışma bu boyutuyla literatüre sağlayacağı katkının yanı sıra uygulama imha süreçlerinde kullanılmasında yol gösterici olacaktır.

KAYNAKÇA

Baykara, M., Daş, R., & Karadoğan, İ. (2013). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. In 1st International Symposium on Digital Forensics and Security (ISDFS'13) (pp. 231-239).

Biles, G. E., Bolton, A. A., & DiRe, B. M. (1989). Herman Hollerith: Inventor, manager, entrepreneur-a centennial remembrance. Journal of Management, 15(4), 603-615.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. Politeknik Dergisi, 9(3), 165-174.

Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In 2012 International Conference on Computer Science and Electronics Engineering (Vol. 1, pp. 647-651). IEEE.

Çetin, H. (2014). Kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi. Akdeniz Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 14(29), 86-105.

Doğan, K., & Arslantekin, S (2016). Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum. Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi, 56(1).

Gantz, J., & Reinsel, D. (2012). The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east. IDC iView: IDC Analyze the future, 2007(2012), 1-16.

Gölcüklü, F. (1994). Avrupa İnsan Hakları Sözleşmesi'nde" Adil Yargılama". Ankara Üniversitesi SBF Dergisi, 49(01).

Göztepe, E. (2011). Türkiye'de Anayasa Mahkemesi'ne bireysel başvuru hakkının (Anayasa Şikâyeti) 6216 sayılı kanun kapsamında değerlendirilmesi. Türkiye Barolar Birliği Dergisi, (95), 13-40.

Henkoğlu, T. (2017). Veri Koruma Kanununun Getirdikleri. Journal of Current Researches on Social Sciences, 7(2), 241-250.

Henkoğlu, T., & Uçak, N. Ö. (2015). Üniversite Kütüphanelerinde Kişisel Verilerin Korunması. Bilgi Dünyası, 16(1).

Hughes, G. F., Coughlin, T., & Commins, D. M. (2009). Disposal of disk and tape data by secure sanitization. IEEE Security & Privacy, 7(4), 29-34.

Jensen, J. R., & Christensen, E. J. (1986). Solid and hazardous waste disposal site selection using digital geographic information system techniques. Science of the total environment, 56, 265-276.

Oğuz, S. (2018). Kişisel verilerin korunması hukukunun genel ilkeleri. Bilgi Ekonomisi ve Yönetimi Dergisi, 13(2), 121-138.

Schroeder, G. N., Steinmetz, C., Pereira, C. E., & Espindola, D. B. (2016). Digital twin data modeling with automationml and a communication methodology for data exchange. IFAC-PapersOnLine, 49(30), 12-17.

Şengül, G., Atsan, F. K., & Bostan, A. (2014). Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri. 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 17-18.

Şişkin, D. Ş. (2018). Bilgi güvenliği ve kişisel verilerin korunması. Türk Kütüphaneciliği, 32(4), 342-345.

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 23(2).

Winter, R. (2013). SSD vs HDD-data recovery and destruction. Network Security, 2013(3), 12-14.

Yıldız, A. K. (2006). Dijital Belge Yönetimi: Dijital Belgelerin Üretimi, Yönetimi ve Korunması için Rehber. Bilgi Dünyası, 7(1), 157-158.

ISO27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ STANDARDININ KAMU KURUMLARINA UYGULANABİLİRLİĞİNİN ARAŞTIRILMASI: ANKARA İLİ ÖRNEĞİ

***

INVESTIGATION OF THE IMPLEMENTATION OF ISO27001 INFORMATION SECURITY MANAGEMENT SYSTEM STANDARD ON PUBLIC INSTITUTIONS: CASE OF ANKARA PROVINCE, TURKEY

Hüseyin ÇAKIR[*]
Mehmet TUYGUN[**]

DOI: 10.33461/uybisbbd.598989

Öz

Bu araştırmada, ISO27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) sertifikasyon sürecinin tamamlamış kamu kurumlarında kurum personelinin sistem hakkındaki düşüncelerinin incelenmesi amaçlanmıştır. Bu sebeple araştırma kapsamında, "Yönetim Kadrosu", "BGYS Ekip Üyeleri", "Kurum Teknik Personeli" ve "Kurum Personeli" gibi dört farklı odak grup üzerinde ilgili gruplar için hazırlanmış farklı anketler uygulanmıştır. Hazırlanan anketlerde 5'li likert ölçeği kullanılmıştır. Likert tipi ölçek sorularında güvenilirlik analizi uygulanmıştır. Yapılan ön çalışmanın analizleri sonucunda anketin güvenilirlik katsayısının kabul edilebilir düzeyde olduğu görülmüştür. Elde edilen verilerde odak gruplarının görüşlerinin belirlenmesi amacıyla frekans ve yüzdelik dağılımları belirlenerek yorumlanmıştır. Elde edilen veriler ışığında, yönetim kadrosunun ISO27001 sertifikasyon sürecini olumlu karşıladığı, kurumsal süreçlerin ve bilgi güvenliğinin sağlanması açısından olumlu katkı sağladığı yönünde görüş birliği olduğu görülmüştür. Diğer taraftan BGYS ekip üyelerinin, ISO27001 süreçlerinin etkin bir şekilde yönetilebilmesi için gereken teknik yeterlilik, eğitim ve sayısal çokluk noktasında takviye ihtiyaçları olduğu yönünde görüş bildirdikleri görülmüştür. Teknik ekip üyelerinin ise ISO27001 süreçlerinin işlerini kolaylaştırdığı ve etkin çalışma yürütülmesine katkı sağladığı yönünde olumlu görüş bildirdikleri fakat teknik yeterlilikler ve sayısal yeterlilik konusunda görüş birliği olmadığı görülmüştür. Kurum personelinin ise ISO27001 kapsamında alınan farkındalık eğitimlerini faydalı olduğu ve BGYS süreçlerinin kurumsal bilgi güvenliği açısından gerekli olduğu yönünde olumlu görüş bildirdikleri görülmüştür.

Kurumsal bir BGYS kurmak, kurulan sitemin sürekliliğini sağlamak, sürekli izlemek ve aksayan yönlerini tespit ederek iyileştirmeler yapmak, bilgi güvenliği farkındalığı oluşturmak, kısacası canlı bir BGYS kurmak ISO27001 belgesi sahibi olmanın olmazsa olmaz şartlarındandır. Bu çalışmanın, kamu kurumlarının kurmuş oldukları BGYS'lerin etkinlik seviyelerine, sahiplenme durumlarına ve teknik yeterliliklerine ışık tutması açısından önemli olduğu düşünülmektedir.

Anahtar Kelimeler: *e-devlet, Bilgi Güvenliği, ISO27001.*

Abstract

The aim of this research is to examine the opinions of the personnel of the institution in the public institutions that have completed the ISO27001 Information Security Management System (ISMS) certification process. For this reason, in the scope of the research, different questionnaires were

[*] Dr. Öğr. Üyesi, Gazi Üniversitesi, Gazi Eğitim Fakültesi Bil. ve Öğr. Tek. Eğitimi Bölümü, hcakir@gazi.edu.tr
ORCID: 0000-0001-9424-2323
[**] Gazi Üniversitesi, Bilişim Enstitüsü, Bilişim Sistemleri Anabilim Dalı, mehmettygn@gmail.com
ORCID: 0000-0000-0000-0000

Geliş Tarihi / Received: 31.07.2019
Kabul Tarihi / Accepted: 24.11.2019

prepared for the related groups on four different focus groups such as "Management Staff", "ISMS Team Members", "Institution Technical Staff", "Institution Staff". The 5-point Likert scale was used in the surveys. Reliability analysis was applied in Likert type scale questions. As a result of the analysis of the preliminary study, it was found that the reliability coefficient of the questionnaire was acceptable. In order to determine the opinions of the focus groups, frequency and percentage distributions were determined and interpreted. In light of the data obtained, it is seen that the management team has a positive attitude towards the ISO27001 certification process and in terms of ensuring institutional processes and information security. On the other hand, it has been observed that ISMS team members have expressed their opinion on the need for technical qualification, training and numerical multiplicity in order to manage the ISO27001 processes effectively. It was observed that the technical team members gave a positive opinion that the ISO27001 processes facilitated their work and contributed to the effective execution of the work, but there was no consensus on technical qualifications and numerical competence. It has been observed that the staff of the institution have been positive about the awareness trainings taken within the scope of ISO27001 and that ISMS processes are required for enterprise information security.

Establishing a corporate ISMS, ensuring the continuity of the established system, continuously monitoring and identifying the deficiencies, making improvements, creating information security awareness, in short, establishing a live ISMS is an indispensable condition of having ISO27001 certificate. This study is thought to be important in terms of shedding light on the efficiency levels, ownership and technical competence of ISMS established by public institutions.

Keywords: *e-government, Informatıon Security, ISO27001.*

1. GİRİŞ

Son yıllarda elektronik sistemlerin günlük yaşantının ve iş hayatının vazgeçilmez bir parçası haline gelmiştir. Sunulan kurumsal hizmetlerin ve kişisel bilgilerin bu sistemler üzerinde paylaşımı, bilgiye erişim yöntemlerinde gelişmeler, bu sistemler üzerinde bulunan zafiyetlerin kötü niyetli saldırıların odağı haline gelmesine sebep olmuştur. Kötü niyetli saldırılar sonucunda kişisel ve kurumsal veri kayıplarının her geçen gün artıyor olması bilgi güvenliğinin öneminin artmasındaki en büyük etkenler arasında yer almaktadır. Kurumsal veya kişisel bilgi varlıklarına yapılan saldırılar ile birlikte gerek kişisel gerekse kurumsal bilgi güvenliğine verilen önem artmıştır ve yeni yaklaşımların ve bilgi güvenliği standartlarının kurumlar bünyesinde benimsenmesine ve uygulanmasına sebep olmuştur.

Kurumsal bilgi güvenliği, bilginin üretilmesi, işlenmesi, erişimi ve saklanması aşamalarının her birinde sağlanmak zorundadır. Bunun için kurumlar bünyesinde kullanılan veya geliştirilen yazılımlar, donanımsal sistemler ve bilgi güvenliğinin vazgeçilmez bir parçası olan insan kaynakları dikkate alınmalıdır. Kurumsal bilgi varlıklarının korunmaya çalışıldığı bilgi güvenliği yaklaşımlarında güvenlik zincirinin en zayıf halkasının her zaman insanlar olduğu kabul edilmiştir (Colwill, 2009). Bunun sebebi, kurumsal sistemlerde uygulanan birçok teknik veya teknik olmayan güvenlik önlemleri saldırganlar tarafından insanlar kullanılarak çeşitli yöntemlerle aşılabilmektedir (Arce, 2003).

Bilgi güvenliğinin sağlanabilmesi amacıyla, kurumların kendi ihtiyaçları ve süreçleri doğrultusunda bir dizi güvenlik politikalarını ve prosedürlerini belirlemesi ve uygulanması gerekmektedir (Asosheh, Hajinazari, & Khodkari, 2013). Bu politikalar, kurumsal faaliyetlerin gözden geçirilmesi, sistemlere erişimlerin izlenmesi, değişiklik kayıtlarının tutularak gerekli değerlendirmelerin yapılması, silme yetkisinin kısıtlanması gibi bazı kullanıcı işlemlerine indirgenebilmektedir (Canbek & Sağıroğlu, 2006).

En temel ifadesiyle bilgi güvenliği, kurumsal bilgi güvenliği risklerini tanımlamak ve bu risklerin etkilerinin kabul edilebilir seviyelere indirgenebilmesi amacıyla yürütülen süreçlerdir. Bu bağlamda, bir BGYS'nin benimsenmesi bir kurum için stratejik bir karar olmalıdır, çünkü BGYS'nin tasarımı ve uygulanması, kurumsal ihtiyaçlar ve amaçlar, güvenlik gereksinimleri, kullanılan süreçler kurumun büyüklüğü ve yapısı ile doğrudan ilgilidir (Asosheh et al., 2013).

Bilgi güvenliği kurumun faaliyetlerini desteklemede çok önemli bir rol oynadığından, bilgi güvenliği konusundaki yönetişimi düzenleyen bir standart veya ölçüte sahip olmak gerekmektedir. Bilgi güvenliği uygulamalarını standartlaştırmak ve düzene koymak için, dünya üzerinde gerek devlet eliyle enstitüler kurularak gerekse özel sektörde organizasyonlar eliyle bilgi güvenliği uygulamalarını, süreçlerini ve prosedürlerini "bilgi teknolojisi sistemlerini ve bilgilerini korumak için" çeşitli standartlar geliştirilmiştir (Gikas, 2010).

Bu standartlardan birisi olan ISO27001 standardı dünya üzerinde bilgi güvenliği alanından oluşturulmuş birçok standart içerisinde geçerliliği olması ve sektör bağımsız yapısıyla her türlü kurum veya kuruluş üzerinde uygulanabilir esnek yapıda olması sebebiyle her geçen gün birçok alanda zorunlu hale getirilmeye başlanan bir standarttır. ISO27001, kurum süreçlerine uygun bir şekilde belirlenmiş bir takım kontroller yardımıyla, bilgi güvenliğinin etkin bir şekilde yönetebileceği ve etkinliğinin ölçebileceği bir yaklaşım sunmaktadır (Rhodes-Ousley, 2013).

Türkiye'de ise siber güvenlik ve bilgi güvenliği alanlarında yapılan çalışmalar kapsamında yayınlanan "2016 – 2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ile hız kazanmıştır. Bu çalışmalar kapsamında özellikle kamu kurumların bilgi güvenliği yönetim sistemlerinin kurulması ve kurulan bilgi güvenliği yönetim sistemlerinin ISO27001 sertifikası ile sürdürülebilir ve sürekli geliştirilebilir dinamik bir yapıya kavuşturulması istenmiştir. Özellikle kamu kurumları arasında iletişimin sağlandığı, güvenli hat olarak tabir edilen KamuNet ağının kurulması çalışmalarında tüm kamu kurumlarına ISO27001 kurulması zorunlu hale getirilmiştir (UDHB, 2017).

1.1. Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliğinin sağlanabilmesi için öncelikle bilgi kavramı ve bu bilginin güvenliğinin sağlanabilmesi ile doğrudan ilişkili olan temel unsurları göz önünde bulundurmak gerekmektedir.

Bilgi (Information), gelecekte alınması muhtemel kararların şekillenmesinde ve güncel kararların alınmasında kullanılan, belli bir düzende işlenmiş veri (data) olarak da tanımlanabilir. Eğer veri davranışları etkiliyorsa bilgi olarak ifade edilebilir. Bilgi her zaman anlamlı olmayabilir. Belli bir kararın alınmasında önemli bir rol oynayan bilgi, başka bir kararın alınması noktasında sadece bir veri olabilir. Bu noktada bilginin güvenilirliği, konu ile ne kadar ilgili olduğu, eksiksiz olması, erişim kolaylığı, ihtiyaçları karşılaması gibi ölçütler o bilgisinin kalitesini belirlemektedir (Demirtaş, 2013).

Sahip olunan bilginin önemi her geçen gün artmaya devam etmektedir. Sahibi olunan daha fazla bilgi, etrafınızdaki dünyaya daha iyi uyum sağlamanız açısından önemli bir araçtır. Kurum veya kuruluşlarda, bilgi genellikle bir şirketin sahip olduğu en önemli varlıklardan biridir. Bilgiyi aynı zamanda şirketleri birbirinden ayıran ve birinin diğerinden daha başarılı olmasına yardımcı olan kaldıraç gibi de düşünebiliriz (Rhodes-Ousley, 2013). Bilgi güvenliği, kurumsal bilgi güvenliği risklerini tanımlamak ve bu risklerin etkilerinin kabul edilebilir seviyelere indirgenebilmesi amacıyla yürütülen süreçlerdir (Asosheh et al., 2013).

Bilgi güvenliği yönetimi ise, bilginin korunması ile güvenli erişimi arasında kurulan bir denge hali olarak nitelendirilebilir. Bunu sağlamak için işletmeler üst yönetim tarafından desteklenen bir çerçeve dâhilinde, çeşitli politikalarla sınırları çizilen bir güvenlik yönetimi yaparlar.

Kurumlarda bilgi güvenliğinin sağlanması sadece teknoloji ile mümkün değildir. Teknolojik çözümlerin yeterli olacağı algısı tamamen yanlış bir algıdır. Bilgi güvenliği teknoloji, süreç ve insan faktörlerinin beraber değerlendirilmesi gereken ve bu üç faktöre göre oluşturulması gereken bir kavramdır. Bilgi güvenliği yönetim sistemi bu noktada teknoloji süreç insan faktörlerine göre oluşturulmuş bir sistemdir.

BGYS; bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ilkelerini sağlamak üzere sistemli, kuralları konulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, yönetimce kabul edilmiş ve desteklenmiş, uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününe denmektedir. Başka bir değişle BGYS, kuruluşların güvenlik olaylarını bütüncül ve sistematik bir biçimde yönetmelerini sağlayan bir çerçevedir.

Aynı zamanda BGYS, kuruluşun bilgi güvenliğini yönetmeye, izlemeye, denetlemeye ve geliştirmeye yardımcı olan süreçler, teknoloji ve insanlar sistemidir. BGYS bünyesinde, insan kaynaklarını, kurumsal politikaları, prosedürleri ve aynı zamanda teknolojinin bir parçası olarak yazılımsal ve donanımsal varlıkları içerir. BGYS'yi uygulayan bir kurum, bilgi varlıklarını çeşitli bilgi güvenliği tehditlerine karşı korunması sağlanabilir. Diğer taraftan BGYS'nin önemli bir parçası risk yönetimidir. Risk yönetimi, riskin belirlenmesi, değerlendirilmesi ve sonrasında işlenerek kabul edilebilir bir düzeye düşürmek veya tamamen ortadan kaldırmak için adımlar atılması sürecidir. Risk değerlendirmesi yapılırken, gizlilik, bütünlük ve erişilebilirlik temel ilkeler doğrultusunda ilgili potansiyel riskler belirlenmeli ve zayıf yönleri tanımlanmalıdır. BGYS'nin doğru bir şekilde yönetilmesi kurumun, riskleri doğru bir şekilde azaltmasına ve yönetmek için uygun kontrolü tanımasına yardımcı olacaktır. Aynı zamanda felaket / olay sırasında maddi kayıpları ve etkileri en aza indirecektir. Ayrıca, kurumun bilgi güvenliği yönetimine bakış açısını da önemli ölçüde geliştirebilir. Kuruluşun tüm bileşenlerinde bilgi güvenliği bilincini artırabilir (Achmadi, Suryanto, & Ramli, 2018).

1.1.1. ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardı

ISO (International Organization for Standardization), 25 ülkeden delegeler, 1946 yılında Londra'daki İnşaat Mühendisleri Enstitüsünde buluşması ile başladı ve endüstriyel koordinasyonu ve endüstriyel standartların birleştirilmesini kolaylaştırmak için yeni bir uluslararası organizasyon oluşturulmasına karar verildi. 23 Şubat 1947'de ISO yeni organizasyonu resmen faaliyete geçti.

Kuruluşundan bu yana, teknoloji ve imalatın neredeyse tüm yönlerini kapsayan 21616'dan fazla Uluslararası Standart yayımlandı. Günümüzde ise, standartların geliştirilmesi amacıyla 163 ülkeden ve 779 teknik makamdan üyeleri bulunmaktadır (ISO, 2019).

ISO / IEC 27000 ailesi standartları, kuruluşların bilgi varlıklarını güvence altına almalarına amacıyla oluşturulmuştur. Bu standartlar ailesini kullanmak, kuruluşların mali bilgiler, fikri mülkiyet hakları, çalışan bilgileri veya üçüncü kişilere ait bilgiler gibi varlıkların güvenliğinin yönetilmesine yardımcı olmaktadır. ISO27001 bilgi güvenliği yönetim sistemi bu ailenin en iyi bilinen standardıdır.

ISO27001 standardının ilgili kurumun faaliyet gösterdiği sektörden bağımsız olarak bir bilgi güvenliği yönetim sisteminin gereksinimlerini tanımlaması, denetlenebilir olması ve diğer yönetim sistemleri ile uyum sağlayabilmesi sebebiyle uluslararası kabul görmüş en önemli standartlardan bir tanesidir. ISO organizasyonu tarafından yayınlanan istatistiklere göre, 2590 tanesi 2017 yılı içerisinde alınmış olan dünya çapında toplam 39501 adet kurumun ISO27001 belgesi sahibi olduğu belirtilmiştir (ISO, 2017).

Türkiye'de siber güvenlik alanında Ulaştırma ve Altyapı Bakanlığı tarafından kamu bilişim sistemlerine, kamu veya özel sektör tarafından yürütülen kritik altyapılara ait bilişim sistemlerinde ve küçük ve orta ölçekli tüzel kişilikleri kapsayacak 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı yayınlanmıştır (UHDB, 2016). Eylem planı çerçevesinde yürütülen çalışmalardan biri de kamu kurumlarının birbirleri olan iletişimlerinin sağlandığı KamuNet ağı kurulumudur. Resmi gazetede yayınlanan 21.07.2016 tarih ve 30103 sayılı "KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ" ile KamuNet ağı hakkında usul ve esaslar belirlenmiştir. Tebliğin, Kamu Kurumu yükümlülükleri ve asgari gereksinimlerin yer aldığı ikinci bölümü 4.maddesi a bendi uyarınca KamuNet bağlantısı yapacak tüm kamu kurumlarının birimleri ve sistemlerini kapsayacak şekilde Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmasını ve işletmesini zorunlu kılınmıştır. Yine aynı maddenin b bendi uyarınca ise kurumlar tarafından kurulan BGYS için ISO27001 standardı uyumluluğunun sağlanması ve belgelendirme işlemlerinin bağımsız belgelendirme kuruluşları tarafından yapılması zorunluluğu getirilmiştir (UDHB, 2017). Kamu kurumları ve kamu kurumları ile iş yapan özel sektör kuruluşlarına getirilen bu zorunluluk ile birlikte Türkiye'de ISO27001 sertifikası sahibi kurum sayılarında artış olduğu gözlemlenmiştir.

ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardı üzerine yapılmış çalışmalar şunlardır;

Çek (2017) tarafından yayınlanan yüksek lisans tezinde kurumsal bilgi güvenliği yönetişiminde insan faktörünün önemi üzerinde durmuştur. Bilgi güvenliği yönetişiminin kurumlarda sağlıklı bir şekilde yönetilebilmesi için yönetim desteğinin şart olduğu vurgulanmış ve bu desteğin en üst yönetimin tarafından verilmesi gerektiği belirtilmiştir.

King (2017) tarafından yayınlanan doktora tezinde kurumsal bilgi güvenliği yönetişimi ile bilgi güvenliği yönetim standartları arasında doğrusal bir ilişki olup olmadığının araştırılması amaçlanmıştır.

Güldüren (2015) tarafından yayınlanan doktora tezinde, yükseköğretim kurumlarında görevli öğretim üyeleri üzerinde bilgi güvenliği farkındalığı oluşturmaya yönelik, çoklu ortam materyalleri ile birlikte bir web sitesi geliştirilmesi ve bu geliştirilen web sitesinin farkındalık kazandırılması noktasındaki etkinliğinin ölçülmesi amaçlanmıştır.

Gencer (2015) tarafından yürütülmüş olan araştırma kapsamında, ISO27001 süreçlerinin ve gerekliliklerinin dinamik bir yapı kazandırılarak, kurumlarda günlük yaşantının bir parçası haline getirilmesi amaçlanmıştır. İlgili araştırmada kurumsal ve uluslararası saygınlık ve kabul görmek için ISO27001 standardının gerekliliği dile getirilmiştir.

Akay (2014) tarafından ISO27001 standardının tarihsel gelişimi ve sürümler arasındaki farklılıklara yer verilmiştir. İlgili çalışmada, ISO27001 sertifikasyon sürecini tamamlamış ve isimleri gizili tutulmuş iki kuruluş ile yapılan mülakatlara yer verilmiş ve elde edilen bulgular ele alınmıştır.

Gürcan (2014) tarafından yapılan çalışmada, finans kurumlarının bilgi güvenliği ihtiyaçlarının ISO27001 çatısı altında incelenerek belirlenmesi üzerinde durulmuştur.

Ganbat (2013) tarafından, ISO27001 ve ISO27005 standartlarının uygulanması konulu çalışmasında ISO27001'in nasıl uygulanması gerektiği ve ISO27005 Risk Yönetimi standardı ile ilişkisi üzerinde durulmuştur.

Demirtaş (2013) tarafından yapılan çalışmada kamu ve özel sektör kuruluşları tarafından yürütülen BGYS'lerin başarı dayanakları değerlendirilmiş ve sistemi olumlu ya da oluşu yönde etkileyen unsurlar irdelenmiştir. Diğer taraftan ISO27001 sertifikasyon süreçlerinin etkin bir şekilde uygulanabilmesini teminen bir model önerisinde bulunulmuştur.

Haklı (2012) tarafından "*Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi*" başlıklı çalışmasında kamu kurumlarına özel olarak tasarlanmış ve ISO27001 kurulum süreçlerinin tamamının yönetilebileceği bir uygulama geliştirilmesi üzerinde durulmuştur.

Shoraka (2011) tarafından yürütülmüş olan tez çalışmasında ISO BGYS sertifikasyon sürecini tamamlanmış kuruluşlar arasında yaptığı bir araştırma ile sertifika sahibi olmanın ilgili kuruluşlara herhangi ekonomik değer kazandırıp kazandırmadığını araştırmıştır.

Mete (2010) tarafından yürütülen çalışmada ISO27001 standardının bilgi işlem merkezlerine uygulanması araştırılmıştır. Çalışma kapsamında BGYS kurulumu yapmak isteyen bilgi işlem merkezlerine rehber niteliği taşıyan Türkçe bir kaynak oluşturulması amaçlanmıştır.

Aydoğmuş (2010) tarafından hazırlanmış olan "*Türkiye'deki Organizasyonların Bilgi Güvenliği Olgunluk Seviyelerinin Belirlenmesi ve ISO/IEC 27001:2005 Standardına Uyumluluklarının Değerlendirilmesi*" başlıklı tez çalışması kapsamında kurumların bilgi güvenliği olgunluk seviyelerinin belirlenmesi amaçlanmıştır.

Bilgi güvenliği yönetim sistemleri ve ISO27001 standartları ile ilgili yapılan çalışmalar incelendiğinde kurulan sistemin etkinliği ve insan faktörünün öneminin özellikle vurgulandığı görülmektedir. Diğer taraftan yapılan araştırmalarda etkin bir BGYS kurulumu ve yönetimi için kurumsal üst yönetim desteğinin önemi de ayrıca vurgulanmıştır. Aynı zamanda bilgi güvenliği yönetiminde, yönetim, BGYS ekibi, kurum teknik personeli ve kurum personeli gibi çeşitli roller olduğu dile getirilmiş ve bu roller arasındaki uyumlu çalışmanın önemi vurgulanmıştır. Bahse konu roller arasındaki çalışmanın uyumu ve olgunluk seviyeleri ile ilgili çeşitli araştırmalar yapılmış ve kurumsal bilgi güvenliğinin olgunluk düzeyinin ölçülmesi amacıyla çeşitli modeller geliştirilmiştir.

İlgili olgunluk seviyelerinin belirli bir düzeye çıkarılması ve kurumsal bilgi güvenliği yönetim sisteminin daha etkin bir şekilde yönetilmesi amacıyla çeşitli uygulamalar geliştirilmiş ve bu kapsamda çeşitli yüksek lisans ve doktora tez çalışmaları yapıldığı görülmüştür. Yapılan tüm çalışmalar ve geliştirilen tüm uygulamaların temelinde insan faktörü olduğu ve yapılan tüm çalışmalarda kurum personellerinin tüm kademelerde katılımcı rol almaları gerektiği yönünde çıkarımlar olduğu görülmektedir. Özellikle ISO27001 sertifikasyon sürecinin ve BGYS kurulumunun en önemli çalışması olarak risk belirleme ve işleme süreçleri olduğu vurgulanmıştır.

Yapılan bazı araştırmalar kapsamında sertifikasyon sürecinin ilgili kuruluşlara her ne kadar ekonomik bir değer katmıyor olsa da marka ve imaj değeri açısından olumlu yönde katkı sağladığı sonucuna varıldığı görülmektedir. Diğer taraftan BGYS süreçler kapsamında yapılan çalışmaların sadece teknik personeller ile ilgili olmadığı kurum personelinin bu süreci günlük yaşantının bir parçası haline getirmesi gerektiği sonucuna varıldığı görülmektedir.

Araştırmaların sertifikasyon süreçlerinden ziyade BGYS ve siber güvenlik alanında yapıldığı, personelin bilgi güvenliği farkındalığı ve kurulan BGYS'nin olgunluk seviyesinin değerlendirildiği görülmektedir. Diğer taraftan Türkiye'de 2017 yılında yayınlanan KamuNet tebliği (UDHB, 2017) kapsamında kamu kurumlarına BGYS kurulumu ve ISO27001 sertifikasyon süreçlerinin tamamlanması zorunluluğu getirilmiştir. Bu kapsamda Türkiye'de kamu kurumları ve kamu kurumları ile ortak çalışma yürüten özel sektör kuruluşlarının da ISO27001sertifikası sahibi olmaları ile birlikte bazı temel yeterliliklere sahip olmaları beklenmektedir. Bu sebeple birçok kamu kuruma bahse konu tebliğde yer alan asgari güvenlik kriterleri ve ISO27001 sertifikasyon sürecinin tamamlamaları için belirli süreler tanınmıştır. Tanınan bu süreler içerisinde kamu kurumları gerekli çalışmaları tamamlamış ve BGYS ile birlikte ISO27001 sertifikası sahibi olmuşlardır. Bu çalışmada sertifikasyon sürecini tamamlamış olan ve bu güne kadar yapılan çalışmalarda dile getirilerek önemi vurgulanan üst yönetim, BGYS ekip üyeleri, teknik ekipler ve kurum personeli açısından kurumlarında çalışmaları tamamlanmış BGYS süreçleri hakkındaki görüşlerinin araştırılması planlanmıştır.

1.1. Araştırmanın Amacı

Kamu kurumlarına getirilen BGYS kurma ve bunu ISO27001 standardı ile belgelendirme zorunluluğunun getirilmesi ile Türkiye'de bulunan kamu kurumlarının ISO27001 sertifikasının alınması ve işletilmesi sürecinde ISO27001 BGYS'nin kamu kurumlarına uygulanabilirliğinin araştırılması amaçlanmıştır. Bu amaç kapsamında belirlenmiş olan alt amaçlar ise şunlardır.

ISO27001 BGYS standardının kamu kurumlarına uygulanabilirliğine ilişkin;

1. ISO/IEC sertifikasyon sürecinin tamamlamış ve aktif BGYS'ye sahip olan kamu kurumlarında görevli yönetim kademesinde olan kişilerin görüşleri nelerdir?

2. Kurumsal bilgi güvenliği yönetim sisteminin kurulumu ve etkin bir şekilde yönetiminden sorumlu olan ve üst yönetim tarafından görevlendirilmiş kamu kurumlarında görevli BGYS ekip üyelerinin görüşleri nelerdir?

3. ISO27001 sahibi kamu kurumlarında görevli BGYS ekip üyeliği dışında, bilgi güvenliğinden dolaylı olarak sorumlu olan diğer teknik personelin görüşleri nelerdir?

4. ISO27001 sertifikasyon sürecini tamamlamış ve etkin bir şekilde BGYS yürütülen kamu kurumlarında görevli ve teknik olmayan personelin görüşleri nelerdir?

2. YÖNTEM

Bu bölümde araştırmanın nasıl yapılacağı, evren ve örneklem ve verilerin toplanması ile ilgili çalışmalar üzerinde durulmuştur.

2.1. Araştırma Modeli

Bilgi güvenliği yönetim sistemine sahip ve sertifikalandırmış olan kamu kurumlarının bu süreci ne ölçüde sahiplendikleri, sertifika sahibi olmanın bilgi güvenliğinin sağlanmasında yeterli olup olmadığı, bilgi güvenliği farkındalık seviyelerindeki gelişme gibi konuların belirlenmesi amacıyla betimsel çalışma uygulanmıştır. Bu çalışmanın örnekleri üzerinde anket çalışmaları yürütülmüş ve alınan cevaplar doğrultusunda ana problem ve alt problemlere cevap verilmeye çalışılmıştır.

2.2. Evren ve Örneklem

Araştırmanın evreni Ankara da bulunan ve ISO27001 sertifikası sahibi kamu kurum ve kuruluşlarından oluşmaktadır. Evrenin büyük olması ve bazı ISO27001 sahibi kurum ve kuruluşlar tarafından kurum personeline anket uygulanmasına izin verilmemesi, izin verilen kurumlarda ise katılımın tam olarak sağlanmaması sebebiyle örneklem alma yoluna gidilmiştir. Resmi yollardan alınan izinler neticesinde Ankara ili genelinde 6 kamu kurumuna anket uygulanabilmiştir. Bu sebeple araştırmanın örneklemini Ankara'da bulunan 6 kamu kurumu ve bu kurumlarda görevli 539 kişi oluşturmaktadır.

2.3. Veri Toplama Araçları

Araştırmada Türkiye'de bulunan ISO27001 sertifika sahibi kurumların hâlihazırda çalışan dört farklı personel grubuna (Üst Yönetim, BGYS Ekibi, Teknik Ekip ve Personel) uygulanmak üzere hazırlanmış dört ayrı anketten oluşmaktadır. Anketlerde yer alan sorularda 5'li likert ölçeği kullanılmıştır. Ölçeğin dereceleri ise "Kesinlikle Katılmıyorum", "Katılmıyorum", "Kararsızım", "Katılıyorum", "Kesinlikle Katılıyorum" şeklindedir. Anket soruları, bilgi güvenliği ve istatistik alanlarında uzmanların görüşleri alınarak oluşturulmuştur. Sorular hazırlanırken anlaşılır olması ve katılımcılar arasında farklı anlaşılmalara sebebiyet vermemesi için özen gösterilmiştir.

Likert tipi ölçek sorularında Cronbach Alpha (α) güvenilirlik analizi uygulanmış ve alınan güvenilirlik analizi sonuçlarının ardından, hazırlanan soruların güvenilirlik düzeylerinin yeterli olduğu sonucuna varılmıştır. Hazırlanan sorular son olarak Türk Dili uzmanları tarafından yazım yanlışı ve dilbilgisi hataları açısından incelenmiştir.

Anket sorularının oluşturulması esnasında ISO27001 standardında yer alan "*Bir kuruluşun bu standarda uyumluluk iddiasında bulunması durumunda, Madde 4 ila Madde 10 arasında belirtilen şartların herhangi birinin hariç tutulması kabul edilebilir değildir."* ifadesinde belirtilen ilgili maddelerden ve bilgi güvenliği konusunda daha önce hazırlanmış olan çeşitli tez çalışmalarından faydalanılmıştır. Oluşturulan anketler ve uygulanan analizlere ilişkin veriler şu şekildedir:

Yönetici

Kurum yöneticileri için hazırlanmış olan anket 16 adet sorudan oluşmaktadır. Anket soruları ile ISO27001 in olmazsa olmaz unsurlarından biri olan ve aynı zamanda ilgili standardın 5. Liderlik maddesi altında yer alan ve "Liderlik" rolüne olan yaklaşımlarının ve sistemin sahiplenilmesi ve işletilmesi konusunda göstermiş oldukları iradenin incelenmesi amaçlanmıştır. Yapılan ön çalışmanın analizleri sonucunda yönetim anketinin güvenilirlik katsayısı 0,932 olarak hesaplanmıştır.

BGYS Ekip Üyeleri

Kurumlarda ISO27001 in işletilmesi ve gerekli kontrollerinin sağlanmasından sorunlu olan ve üst yönetim tarafından atanan BGSY ekip üyelerinin çalışmaları esnasında yaşadıkları problemler üzerinde durulmaya çalışılmış ve yeterlilik seviyeleri sorgulanmaya çalışılmıştır. BGYS ekip üyeleri için hazırlanan anket 18 sorudan oluşmaktadır. Uzman görüşlerinin ardından 2 soru çıkarılmıştır. Ardından yapılan ön çalışmanın analizleri sonucunda yönetim anketinin güvenilirlik katsayısı 0,876 olarak hesaplanmıştır.

Teknik Ekip

Kurumların teknik ekipleri için hazırlanan soru setinde ise ekibin ISO27001 in gerekliliklerini yerine getirme noktasında göstermiş oldukları irade ve yeterliliklerin sorgulanması amaçlanmıştır. Teknik ekip için hazırlanan anket 17 sorudan oluşmaktadır. Uzman görüşlerinin ardından 1 soru çıkarılmıştır. Ardından yapılan ön çalışmanın analizleri sonucunda yönetim anketinin güvenilirlik katsayısı 0,932 olarak hesaplanmıştır.

Personel

Personel için hazırlanan soru setinde ise ISO27001 tarafından zorunlu kılınan personel tarafının farkındalığı ile ilgili gerçekleştirilmesi gereken farkındalığın geliştirilmesi sürecine ilişkin personelin yaklaşımı ve süreçten memnuniyet düzeyleri sorgulanmaya çalışılmıştır. Personel için hazırlanan anket 16 sorudan oluşmaktadır. Uzman görüşlerinin ardından 3 soru çıkarılmıştır. Ardından yapılan ön çalışmanın analizleri sonucunda yönetim anketinin güvenilirlik katsayısı 0,845 olarak hesaplanmıştır.

2.4. Verilerin Toplanması

Hazırlanan anketler, hem ankete özel hazırlanmış web sitesi hem de alınan çıktılara altı adet kamu kurumuna uygulanmıştır. Toplam 573 adet anket cevaplanmış, cevaplanan bu anketlerden 34 tanesinin eksik cevaplanmış olması sebebiyle değerlendirmeye alınmamıştır.

Tablo 1: Anketlerin kurumlara göre dağılımı

Kurumlar	**A**	**B**	**C**	**D**	**E**	**F**	**Toplam**
Yönetim	11	9	15	19	16	8	**78**
BGYS Ekip Üyeleri	5	7	8	9	6	7	**42**
Teknik Ekip	12	15	11	14	12	26	**90**
Personel	45	47	43	124	31	39	**329**
Toplam	**73**	**78**	**77**	**166**	**65**	**80**	**539**

Değerlendirmeye alınan 539 adet anketin; 78 adedi üst yönetim ve birim yöneticileri, 42 adedi BGYS ekip üyeleri, 90 adedi kurum teknik ekipleri, 329 adedi kurum personelleri tarafından cevaplanmıştır. Anketlerin kurumlara göre dağılımı Tablo 1'de verilmiştir. Kurum isimleri güvenlik nedeniyle ve kurumlardan alınan izinler doğrultusunda gizli tutulmuştur.

2.5. Verilerin Çözümü ve Yorumlanması

Araştırma ile ilgili elde edilen veriler uygun istatistik teknikler kullanılarak analiz edilmiş, daha sonra çizelgeler ve tablolar oluşturularak açıklanmış ve yorumlanmıştır.

Bu kapsamda, ISO/IEC sertifikasyon sürecinin tamamlamış ve aktif BGYS'ye sahip olan kamu kurumlarında görevli yönetim kademesi, kurumsal BGYS'nin yönetiminden sorumlu olan BGYS ekip üyelerinin, kurumda görevli diğer teknik personelin ve teknik olmayan personel görüşlerinin belirlenmesi amacı için frekans ve yüzde dağılımları kullanılmıştır.

3. ARAŞTIRMA BULGULARI

Bu bölümde, yapılan araştırma kapsamında uygulanmış olan anket verilerine ilişkin elde edilen bulgular ve bu bulgular doğrultusunda yapılan yorumlara yer verilmiştir. Her anket ayrı bir alt başlık altında incelenmiştir.

3.1. Yönetim Kademesinin Bilgi Güvenliği Yönetim Sistemi Hakkındaki Görüşleri

Bu bölümde araştırmaya katılan ve ISO27001 sahibi kamu kurumlarında görevli üst yönetici veya birim yöneticileri tarafından elde edilen veriler incelenmiştir. Altı kamu kurumunda görevli toplan 78 yöneticinin ankete katılım sağladığı görülmektedir. Anket 12 sorudan oluşmaktadır. Yöneticilerin anketlere vermiş olduğu cevaplara ilişkin veriler soru bazlı olarak incelenmiştir.

Tablo 2: Yönetim Kademesinin Bilgi Güvenliği Yönetim Sistemi Hakkındaki Görüşleri

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	N	$\overline{X}$
ISO27001 Standardının kurumlar için gerekliliği olduğunu düşünüyorum	3	3,8	4	5,1	1	1,3	23	29,5	47	60,3	78	4,37
ISO27001 Sertifika sahibi olmanın kazandırdığı ulusal ve uluslararası saygınlık kazandırdığını düşünüyorum	2	2,6	4	5,1	8	10,3	27	34,6	37	47,4	78	4,19
ISO27001 Bilgi Güvenliği alanındaki kurumsal hedeflerime de sağladığı kolaylık sağladığını düşünüyorum	6	7,7	1	1,3	4	5,1	32	41,0	35	44,9	78	4,14
ISO27001 Bilgi Güvenliği politikalarının kurumsal süreçlerin uygulanması konusunda kolaylık sağladığını düşünüyorum	1	1,3	7	9,0	3	3,8	31	39,7	36	46,2	78	4,21
ISO27001'in kurum yöneticilerinin Bilgi Güvenliği farkındalığına katkı sağladığını düşünüyorum	1	1,3	6	7,7	3	3,8	25	32,1	43	55,1	78	4,32
Bilgi Güvenliği Yönetim Sisteminin sürdürülebilir olmasına yönetim desteğinin katkısının önemli olduğunu düşünüyorum	3	3,8	3	3,8	4	5,1	11	14,1	57	73,1	78	4,49
ISO27001 Bilgi Güvenliği Yönetim Sisteminde yer alan, yönetimin üzerine düşen görevlerin uygulanabilir olduğunu düşünüyorum	4	5,1	3	3,8	9	11,5	36	46,2	26	33,3	78	3,99
ISO27001 standartlarının uygulanmasının kurumsal süreçlerin uygulanması sırasında ek iş yükü getirdiğini düşünüyorum	10	12,8	20	25,6	22	28,2	12	15,4	14	17,9	78	3,00
ISO27001 Bilgi Güvenliği ve Yönetim Sistemi üst yönetim olarak bu sistem içerisindeki ayrıcalıklı olmam gerektiğini düşünüyorum	13	16,7	16	20,5	15	19,2	20	25,6	14	17,9	78	3,08
ISO27001 in kurum dışı ve kurum içi güvenliğe katkı sağladığını düşünüyorum	1	1,3	6	7,7	9	11,5	47	60,3	15	19,2	78	3,88
ISO27001 kapsamında genelde veya yerelde gerçekleşecek kritik bir güvenlik probleminde sistemin bizi koruyacağını düşünüyorum.	1	1,3	8	10,3	9	11,5	49	62,8	11	14,1	78	3,78
ISO27001 sertifikasyonu sağlanmadan bilgi güvenliği yönetim sisteminin verimli olarak yönetilemeyeceğini düşünüyorum.	4	5,1	12	15,4	14	17,9	32	41,0	16	20,5	78	3,56

Tablo 2'den de anlaşılacağı üzere Kurum yöneticileri, ISO/IEC 27001 standardının kurumları için gerekli olduğu yönündeki ağırlıklı görüş bildirmektedir. Bununla birlikte kurum yönetiminin tamamına yakınının ISO/IEC 27001 sertifika sahibi olmanın kuruma saygınlık kazandırdığı ve kurumsal süreçlerin işletilmesine olumlu yönde katkı sağladığı noktasında görüş birliğinde oldukları görülmektedir. Kurum yönetim kademesinin ISO/IEC 27001 standardının bilgi güvenliği farkındalığına olumlu yönde katkı sağladığı ve standardın sürdürülebilir olması için üst yönetim desteğinin gerekliği olduğu görüşünün hâkim olduğu da verilen cevaplardan anlaşılmaktadır. Diğer taraftan ISO/IEC 27001 standardının kurumsal süreçlerin uygulanması esnasında ek iş yükü getirdiği noktasında bir görüş birliği olmadığı görülüyor. Ortalamanın 3.00 olarak görüldüğü bu soruda; katılımcıların %33,3'ünün standardın ek iş yükü getirdiği, %28,2'sinin bu konuda karasız

olduğu ve geri kalan %38,5'lik kısmının da ek iş yükü getirmediği yönünde görüş bildirdikleri görülmektedir. Aynı zamanda yönetim kademesinin sistem içerisinde ayrıcalıklı olup olmamaları yönünde sorulan soruya verilen cevaplarda da bu konuda bir görüş birliği sağlanamadığını görülmüştür. Yönetim kadrosunun %43,5'lik bir bölümünün ayrıcalıklı olmaları gerektiği yönünde görüş bildirdikleri, %19,2'lik bölümünün bu konuda kararsız oldukları, geri kalan %37,3'lük bölümün ise ayrıcalık tanınmaması gerektiği yönünde görüş bildirdikleri görülmektedir. Kurum yönetiminin %76,9 gibi yüksek bir bölümünün kurum tarafından yönetilen bilgi güvenliği yönetim sisteminin ISO/IEC27001 sertifikasyonu olmadan verimliği bir şekilde yönetilemeyeceği yönünde görüş bildirdikleri görülmektedir.

3.2. Bilgi Güvenliği Yönetim Sistemi Ekip Üyelerinin Bilgi Güvenliği Yönetim Sistemi Hakkındaki Düşünceleri

Bu bölümde ISO27001 sahibi kamu kurumlarının BGYS kurulumu ve işletilmesinden sorumlu personellerden elde edilen veriler incelenmiştir. Altı kamu kurumundan toplam 42 ekip üyesi yapılan ankete katılım sağlamıştır. Sorulan sorularda BGYS ekip üyelerin kurumlarında yürüttükleri görevler ve BGYS hakkındaki görüşlerinin alınması planlanmıştır. Katılımcıların anket sorularına vermiş oldukları cevaplar soru bazlı olarak incelenmiştir.

Tablo 3 incelendiğinde ekip üyelerinin BGYS süreçlerinin yönetimi ve ISO27001 süreçlerinin etkin bir şekilde yönetilebilmesi için kurulmuş olan ekibin, eğitim ihtiyacı olduğu, sayısal anlamda yeteriz kaldığı ve bu sebeple danışmanlık hizmetlerinin gerekli olduğu yönünde görüş bildirdikleri görülmektedir. Ekip üyelerinin %84,1'inin eğitime ihtiyaç duydukları yönünde görüş bildirdikleri görülmüştür. Süreçlerin yönetilmesi noktasında personel yeterli olup olmadığı konusunda %43,2'lik bir çoğunluğun kararsız kaldığı görülmektedir. Diğer taraftan kurum personeli ile uyumlu bir çalışma yürütülüp yürütülmediği konusunda %43,2'sinin olumlu görüş bildirdiği %34,1'lik bölümünün ise kararsız kaldığı görülmektedir. Diğer taraftan kurum personeli ile yürütülen risk çalışmalarında ise uyumlu bir çalışma yapılıp yapılamadığı yönünde %43,2'lik bölümünün olumsuz görüş bildirdiği görülmüştür. BGYS kapsamında yapılan çalışmaların ve kurumsal BGYS süreçlerinin sağlıklı bir şekilde uygulanıp uygulanamadığı yönündeki soruya ilişkin cevaplar incelendiğinde, katılımcıların %29,6'sinin olumsuz görüş bildirdiği, %38,6'lık bölümünün bu konuda kararsız kaldığı ve geri kalan %31,8'lik bölümünün ise kurumsal BGYS süreçlerinin sağlıklı bir şekilde işletilebildiği yönünde görüş bildirdikleri görülmektedir. Diğer taraftan kurum personelinin %65,9'luk bölümünün ise BGYS kapsamında alınan önlemler kapsamından yapılan değişiklikler ile birlikte alışkanlıklarını değiştirme konusunda zorlandıkları yönünde görüş bildirdikleri görülmüştür. Son olarak, ISO27001 sertifikasyon süreci tamamlanmış ve etkin bir şekilde BGYS süreçlerini kapsamında uygulanan politika ve prosedürlerin kurumsal süreçlere sağladığı katkılara ilişkin sorulan soruya katılımcıların toplam %27,3'lük bölümünün olumsuz görüş bildirdiği, %36,4'lük bölümünün kararsız kaldığı ve %36,9'unun olumlu yönde görüş bildirdikleri görülmüştür.

Tablo 3: BGYS Ekip Üyelerinin Bilgi Güvenliği Yönetim Sistemi Hakkındaki Düşünceleri

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	N	$\overline{X}$
Bilgi Güvenliği Yönetim Sistemi süreçlerinin yönetilmesi amacıyla mutlaka danışmanlık hizmeti alınması gerektiğini düşünüyorum.	3	6,8	5	11,4	6	13,6	15	34,1	15	34,1	44	3,77
Bilgi Güvenliği Yönetim Sistemi süreçlerinin yönetilebilmesi için kurumumuz personelinin yeterli olduğunu düşünüyorum.	4	9,1	8	18,2	19	43,2	11	25,0	2	4,5	44	2,98
Bilgi Güvenliği yönetim Sistemi süreçlerinin yönetilmesi için ekip üyelerinin eğitim alması gerektiğini düşünüyorum.	3	6,8	2	4,5	2	4,5	9	20,5	28	63,6	44	4,30
Kurulacak olan ekibin bilişim personellerinden oluşması gerektiğini düşünüyorum.	3	6,8	11	25,0	11	25,0	13	29,5	6	13,6	44	3,18
Kurumumuz Bilgi Güvenliği yönetimi ekip üyelerinin sayısının ISO27001 süreçlerinin sağlıklı bir şekilde yönetilebilmesi için yeterli olduğunu düşünüyorum.	5	11,4	12	27,3	12	27,3	12	27,3	3	6,8	44	2,91
ISO/IEC 27001 süreçlerinin yönetimi esnasında kurum personeli ile sağlıklı bir çalışma yürütülebileceğini düşünüyorum.	2	4,5	8	18,2	15	34,1	15	34,1	4	9,1	44	3,25
Kurumsal risk çalışmaları sırasında kurum personelinden yeterince destek alınabileceğini düşünüyorum.	4	9,1	15	34,1	10	22,7	14	31,8	1	2,3	44	2,84
ISO/IEC 27001 süreçlerinin kurumumuzda sağlıklı bir şekilde uygulanabildiğini düşünüyorum.	5	11,4	8	18,2	17	38,6	10	22,7	4	9,1	44	3,00
ISO/IEC 27001 standardının kurumsal bilgi güvenliği açısından gerekli olduğunu düşünüyorum.	4	9,1	3	6,8	5	11,4	18	40,9	14	31,8	44	3,80
ISO27001 kurum dışı olduğu kadar kurum içi güvenliği de tam olarak sağladığını düşünüyorum	4	9,1	6	13,6	16	36,4	13	29,5	5	11,4	44	3,20
ISO27001 kapsamında alınan önlemlerin, kurum içinden veya dışından gelecek kritik bilgi güvenliği problemlerine karşı bizi koruyacağına inanıyorum.	3	6,8	8	18,2	9	20,5	21	47,7	3	6,8	44	3,30
ISO27001 sistemine geçiş sürecinde insanların alışkanlıklarını terk etmelerinin zor olduğunu düşünüyorum.	3	6,8	6	13,6	6	13,6	14	31,8	15	34,1	44	3,73
ISO/IEC 27001 sistemine geçişin ardından bilişim personeli üzerindeki iş yükünün azaldığını düşünüyorum.	15	34,1	13	29,5	8	18,2	5	11,4	3	6,8	44	2,27
ISO/IEC 27001 çerçevesinde belirlenen politika ve prosedürlerin tıkanan kurumsal süreçlerini açtığını düşünüyorum.	3	6,8	9	20,5	16	36,4	11	25,0	5	11,4	44	3,14

3.3. Teknik Personelin Bilgi Güvenliği Yönetim Sistemi ve Yeterlilikler Hakkındaki Görüşleri

Bu bölümde ISO27001 sahibi kamu kurumlarında görevli, ağ uzmanı, sistem uzmanı yazılım uzmanı vb. teknik personellerden elde edilen veriler incelenmiştir. Altı kamu kurumunda görevli toplam 90 teknik personel yapılan ankete katılım sağlamıştır. Sorulan sorularda kurumsal BGYS ve ISO27001 süreçleri hakkında teknik personellerin görüşlerinin alınması planlanmıştır. Katılımcıların anket sorularına vermiş oldukları cevaplar soru bazlı olarak incelenmiştir.

Tablo 4: Teknik Personelin Bilgi Güvenliği Yönetim Sistemi ve Yeterlilikler Hakkındaki Görüşleri

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	N	$\overline{X}$
Bilgi Güvenliği Yönetim Sistemi süreçlerinin sağlıklı bir şekilde yürütülmesi için teknik personelin yeterli olduğunu düşünüyorum.	8	8,9%	28	31,1%	8	8,9%	34	37,8%	12	13,3%	90	3,16
ISO/IEC 27001 standardının kurumsal bilişim süreçlerinde uygulanabilir olduğunu düşünüyorum.	2	2,2%	7	7,8%	18	20,0%	51	56,7%	12	13,3%	90	3,71
ISO/IEC 27001 ile ilgili eğitim/eğitimler almamız gerektiğini düşünüyorum.	4	4,4%	5	5,6%	5	5,6%	42	46,7%	34	37,8%	90	4,08
ISO/IEC 27001 görevimle ilgili süreçleri etkin ve zamanında yerine getirebilmemde fayda sağladığını düşünüyorum.	3	3,3%	9	10,0%	23	25,6%	42	46,7%	13	14,4%	90	3,59
ISO/IEC 27001 kapsamında alınan önlemler sayesinde Bilgi Güvenliği olaylarında azalma yaşandığını düşünüyorum.	3	3,3%	5	5,6%	15	16,7%	49	54,4%	18	20,0%	90	3,82
ISO/IEC 27001 Standardının, geliştirilen kurumsal uygulamaların güvenliğine olumlu katkı sağladığını düşünüyorum.	2	2,2%	5	5,6%	11	12,2%	53	58,9%	19	21,1%	90	3,91
ISO/IEC 27001 sayesinde, bilgi güvenliği ihlal olaylarının kontrol edilebilir noktaya geldiğini düşünüyorum.	2	2,2%	5	5,6%	20	22,2%	52	57,8%	11	12,2%	90	3,72
Bilişim sistemlerinde tespit edilen aksaklıklar üzerinde düzenleyici ve önleyici faaliyetler uygulanmasının faydalı olduğunu düşünüyorum.	2	2,2%	6	6,7%	2	2,2%	52	57,8%	28	31,1%	90	4,09
ISO/IEC 27001 kapsamında güvenlik açısından daha fazla önlem alınmış bir sistem üzerinde daha az problem yaşanacağını düşünüyorum.	1	1,1%	8	8,9%	13	14,4%	43	47,8%	25	27,8%	90	3,92
ISO/IEC 27001 standardının bütün süreçlerinin en iyi şekilde işletilmesi durumunda olası risklerin önceden tespit edilebileceğini düşünüyorum.	3	3,3%	4	4,4%	12	13,3%	50	55,6%	21	23,3%	90	3,91

Tablo 4 incelendiğinde kurum teknik ekiplerinin ISO27001 hakkındaki görüşlerinin genel anlamda olumlu yönde olduğu görülebilir. Diğer taraftan teknik personelin sayısal anlamda yeterli olup olmadığı sorusuna %40 oranında olumsuz cevap verildiği, %51,1 oranında ise olumlu cevap verildiği görülmüştür. ISO27001'in kurumsal süreçlere uyumluluğu konusunda %70'lik bir oranda olumlu görüşün hakim olduğu görülmüştür. Diğer taraftan teknik personelin %80'inden fazlasının eğitim ihtiyacı olduğu konusunda fikir birliğine vardığı görülmüştür. ISO27001'in süreçlerinin bilgi güvenliği olaylarının azalmasına katkı sağladığı yönünde olumlu görüş bildirenlerin oranı ise %74,4 olarak gözlemlenmiştir. ISO27001 ile birlikte kurumlar bünyesinde geliştirilen yazılımların bilgi güvenliği açısından incelenmesi konusunda bir farkındalık oluştuğu yönündeki görüşlerin oranı ise %80'dir. Aynı zamanda bilgi güvenliği olaylarının gerçekleşmeden önce tahmin edilebilmesi ve düzenleyici ve önleyici faaliyetlerin olumlu yönde katkı sağladığı görüşünün ağır bastığı görülmüştür. Teknik personelin ISO27001 kapsamında alınan önlemlerin daha fazla olması durumunda yaşanması muhtemel bilgi güvenliği olaylarında azalma yaşanacağı şeklinde görüş bildirdikleri görülmüştür.

3.4. Kurum Personellerinin Bilgi Güvenliği Yönetim Sistemi ve Farkındalık Eğitimleri Hakkındaki Görüşleri

Bu bölümde ISO27001 sahibi kamu kurumlarında görevli personelden elde edilen veriler incelenmiştir. Personele sorulan sorular ile personelin bilgi güvenliği yönetim sistemi çalışmaları kapsamında almış oldukları farkındalık eğitimleri, sistem ile ilgili genel görüşleri hakkında bilgi sahibi olunmaya çalışılmıştır. Altı kamu kurumunda görevli toplam 329 personel yapılan ankete katılım sağlamıştır. Katılımcıların anket sorularına vermiş oldukları cevaplar aşağıda soru bazlı olarak incelenmiştir.

Personele sorulan sorular ile personelin bilgi güvenliği yönetim sistemi çalışmaları kapsamında almış oldukları farkındalık eğitimleri ve sistem ile ilgili genel görüşleri hakkında bilgi sahibi olunmaya çalışılmıştır. Verilen cevaplar incelendiğinde, %65,3'lük bir oranın verilen eğitimlerin sürelerinin yeterli olduğunu düşündüğü görülmüştür. Diğer taraftan eğitimde kullanılan materyallerin ve eğitim içeriğinin yeterliliği konusunda yaklaşık %60'lık bir oranda olumlu görüş bildirildiği görülmüştür. Bununla birlikte alınan eğitimlerin bilgi güvenliği farkındalığı açısından faydalı olduğunu düşünenlerin oranı ise %73,3 seviyesinde. Eğitim içeriklerinden memnun olunmasına rağmen, eğitimlerin sadece slaytlar üzerinden yapılmasının yeterli olmadığını düşünenlerin oranı %44,4 olarak görülmektedir. BGYS kapsamında alınan önlemler ve kısıtlamaların kullanıcı yetkilerini kısıtlayıp kısıtlamadığı konusunda ise personel içerisinde bir görüş birliği olmadığı görülmektedir. Personelin %42,5'lik bir bölümünün yetkilerin kısıtlanmadığı yönünde, %27,4'ünün bu konuda kararsız olduğu ve geri kalan %30,1'lik kesiminin ise yetkilerin aşırı derecede kısıtlandığı yönünde görüş bildirdikleri görülmektedir.

4. SONUÇ VE ÖNERİLER

Kurumsal bilgi güvenliği yönetimlerinin veya bu sistemlerin herhangi bir standardizasyona uyumlu hale getirilmiş olması, kurumsal süreçlerde bilgi güvenliğinin tam olarak sağlandığı anlamına gelmediği açıktır. Kurulan sistemlerin, özellikle kurum yönetimi ve tüm kademeleriyle kurum personeli tarafından sahiplenilmesi büyük önem arz etmektedir. Bu sebeple özellikle ISO27001 uyum süreçlerinin olmazsa olmaz unsurlarından biri de sistemin arkasında sağlam bir iradenin varlığının kanıtlanması ve bu iradenin ilgili süreçlerin etkin bir şekilde yürütülebilmesi için gerekli çalışmaları yapmış olduğunu kanıtlaması beklenmektedir.

Tablo 5: Kurum Personelinin BGYS ve Farkındalık Eğitimleri Hakkındaki Görüşleri

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		N	Ort
	f	%	f	%	f	%	f	%	f	%		
ISO/IEC 27001 hakkında verilen bilgilendirme eğitimlerini süresinin yeterli olduğunu düşünüyorum.	13	4,0	40	12,2	61	18,5	181	55,0	34	10,3	329	3,56
ISO/IEC 27001 hakkında verilen bilgilendirme eğitimlerinin içeriklerinin yeterli olduğunu düşünüyorum.	8	2,4	43	13,1	78	23,7	162	49,2	38	11,6	329	3,54
ISO/IEC 27001 hakkında verilen Bilgi Güvenliği bilgilendirme eğitimleri esnasında verilen materyal ve örneklerin yeterli ve güncel olduğunu düşünüyorum.	12	3,6	30	9,1	99	30,1	159	48,3	29	8,8	329	3,50
Almış olduğum Bilgi Güvenliği Eğitimlerinin faydalı olduğunu düşünüyorum.	10	3,0	25	7,6	54	16,4	168	51,1	72	21,9	329	3,81
Bilgi Güvenliği Eğitimleri kapsamında verilen bilgilerin kurumsal süreçler açısından uygulanabilir olduğunu düşünüyorum.	4	1,2	27	8,2	80	24,3	170	51,7	48	14,6	329	3,70
Danışmanlık kapsamında verilen Bilgi Güvenliği Eğitimlerinin süresinden ziyade içeriklerinin dolu olması gerektiğini düşünüyorum.	10	3,0	11	3,3	44	13,4	143	43,5	121	36,8	329	4,08
Bilgi Güvenliği Eğitimlerinin sadece slaytlar üzerinden yapılmasının yeterli olduğunu düşünüyorum.	38	11,6	108	32,8	89	27,1	79	24,0	15	4,6	329	2,77
Bilgi Güvenliği Eğitimi veren firmanın diğer müşterilerinden elde ettiği tecrübeleri de bize aktardığını düşünüyorum.	15	4,6	37	11,2	102	31,0	148	45,0	27	8,2	329	3,41
Bilgi Güvenliği kapsamında alınan önlemlerin kullanıcı yetkilerini aşırı derecede kısıtladığını düşünüyorum.	31	9,4	109	33,1	90	27,4	82	24,9	17	5,2	329	2,83
Kurumumuzda yürütülen bilgi güvenliği yönetim sisteminin iyi bir şekilde yönetildiğini düşünüyorum.	8	2,4	19	5,8	89	27,1	159	48,3	54	16,4	329	3,71

Diğer taraftan kurulan BGYS süreçlerinin, gerek teknik personel tarafından gerekse operasyonel süreçleri yürüten personel tarafından anlaşılması ve sahiplenilmesi de büyük önem arz etmektedir. Bu kapsamda da ISO27001 tüm kademeden personel için yapılması zorunlu bir takım bilgilendirme ve farkındalık oluşturma çalışmalarını zorunlu tutar.

Bilgi güvenliğinin insan, teknoloji ve süreç, üç temel unsurudur ve bu üç unsurdan herhangi birinin aksaması bilgi güvenliğinin tam olarak sağlanamayacağı anlamına gelmektedir. Bu üç unsur teknolojik gelişmeler ve değişimler sebebiyle sürekli güncelliğini korumalıdır. Teknoloji ve süreç unsurları her ne kadar kusursuz ve güncel bir şekilde kurgulanmış ve konumlandırılmış olursa olsun insan unsuru gelişmeler ve değişimler karşısında güncel olmadığı sürece bir anlam ifade etmemektedir. Bu sebeple insan unsurundan ötürü kurumsal bilgi güvenliği yönetimlerinin etkinliği ve sürekliliği devamlı sorgulanmaktadır ve sorgulanmalıdır.

Bu çalışma kapsamında, bilgi güvenliğinin en önemli unsuru olan kurum personeli üzerinde bir araştırma yapılmıştır. Bu kapsamda, ISO27001 sertifikası sahibi olan kamu kurumlarının çeşitli kademe ve görevlerden personel grupları üzerinden incelenmesine yer verilmiştir. İnceleme sonucunda elde edilen bulgular ve sonuçlar aşağıda sunulmuştur.

Kurum yönetici kademelerinin vermiş olduğu cevaplar incelendiğinde, genel anlamda ISO27001 standardizasyon süreçleri ve kurumsal katkıları yönünde olumlu görüşün hâkim olduğu görülmektedir. ISO27001 in genel anlamda kurumlar için gerekli olduğu ve kurumsal anlamda itibar ve güven göstergesi olduğu yönünde görüşlerin ağır bastığı görülmektedir. Diğer taraftan ISO27001'in kurumsal bilgi güvenliği hedeflerine erişmesinde ve BGYS kapsamında geliştirilen kurumsal politikaların işletilmesi ve etkinliğinin artırılmasına katkı sağladığı konusunda da yönetici kademesinin olumlu görüş bildirdikleri görülmektedir. Aynı zamanda kurumsal bilgi güvenliği farkındalığı oluşturma noktasında da ISO27001 olumlu yönde katkı sağladığı düşünülmektedir.

ISO27001 sertifikasyon sürecinin ve BGYS'nin gerekliliklerinin yerine getirilmesi noktasında yönetim desteğinin büyük önem arz ettiği ve bu noktada yönetim kademesinin üzerine düşen görevlerin kabul edilebilir seviyede olduğu görüşü de elde edilen verilerden çıkarılan önemli sonuçlardan biridir. Diğer taraftan ISO27001 ile gelen yetkilendirme politikaları kapsamında yöneticilerin ayrıcalıklı olmaları gerektiği ve ilgili BGYS süreçlerinin ek iş yükü getirip getirmediği noktasında yöneticiler arasında fikir birliği olmadığı görülmektedir. Ek iş yükü getirdiğini düşünen yönetici sayısı ile getirmediği düşünen ve ayrıcalık sahibi olmaları gerektiğini düşünen ve düşünmeyen yönetici sayılarının birbirine yakın olduğu görülmüştür. Genel anlamda yönetim kademesinin ISO27001 süreçlerini olumlu buldukları ve sürecin kurumsal bilgi güvenliğine olumlu yönde katı sağladığını düşündükleri görülmüştür.

ISO27001 uyum süreçlerinin yönetilmesi ve geliştirilmesi amacıyla oluşturulmuş olan BGYS ekip üyeleri tarafından verilmiş cevaplar incelendiğinde, öncelikli olarak ekip üyelerinin ISO27001 in kurumsal bilgi güvenliğinin sağlanması noktasında gerekli olduğunu düşündükleri görülmektedir. Bu görüşle paralel olarak, ISO27001'in kurumu iç ve dış tehditlere karşı koruma noktasında faydalı olduğu yönünde görüş bildirildiği de görülmüştür. ISO27001 uyum süreçlerin kurumun sahip olduğu sayısal anlamda insan kaynağı ile yönetilmesinin zor olduğu ve kurum dışından profesyonel danışmanlık desteği alınması gerektiği yönünde görüşün ağır bastığı görülmüştür. Bununla birlikte, kurumlar sahip oldukları insan kaynağının, tecrübe ve bilgi açısından yetersiz olduğu, süreçlerin yönetiminin sağlıklı bir şekilde yürütülebilmesi amacıyla BGYS ekip üyelerinin eğitimler alması gerektiğini düşündükleri görülmektedir. Bununla birlikte kurulacak olan BGYS ekibinin bilişim personellerinden oluşup oluşmaması gerektiği yönünde bir fikir birliği olmadığı zıt görüşlerin ve kararsızların sayılarının birbirine yakın olduğu görülmüştür. ISO27001 uyum süreçleri kapsamında kurum personeli ile uyumlu çalışma yapılabileceği fakat kurumsal bilgi güvenliği risk süreçlerinin yönetimi noktasında yeterli desteğin alınamadığı yönünde görüş bildirildiği görülmektedir.

Kurum personelinin ISO27001 ile gelen süreç değişikliklerine, eski alışkanlıklarını terk etmekte zorlandıkları için uyum sağlamakta güçlük çektikleri yönünde görüşün daha ağır bastığı da görülmüştür. Bilişim personeli açısından bakıldığında ise ISO27001'in iş yükünü azaltıp azaltmadığı sorusuna, iş yükünün azalmadığı yönünde geri dönüşün daha fazla olduğu görülmüştür. Genel anlamda bakıldığında, BGYS ekiplerinin gerek tecrübe, gerek sayısal olarak yeterli olmadıklarını ve eğitime ihtiyaç duyduklarını düşündükleri, personel ile çalışma noktasında özellikle risk çalışmalarında yeterli desteği göremedikleri yönünde görüş bildirdikleri görülmüştür. ISO27001'in her ne kadar kurum için gerekli olduğu yönünde görüş bildirilmiş olsa da iş yükünün azalmadığı yönünde de görüş bildirildiği görülmüştür.

Kurumlarda görevli bilgi sistemleri ve teknik altyapının yönetiminden ve kurumsal ihtiyaçlar doğrultusunda çözümler üretmekle görevli teknik personelin vermiş olduğu cevaplar incelendiğinde genel olarak sorumlu teknik personelin teknik açıdan ve sayısal yeterli olup olmadığı noktasında bir görüş birliği olmadığı görülmektedir. Bunun sebebi olarak faklı kamu kurumlarında yer alan teknik

ekip sayı yeterliliklerin farklılık göstermesi olduğu düşünülmektedir. ISO27001 in kurumsal teknik süreçler üzerinde uygulanabilir olduğu görüşünün ağır bastığı görülmektedir. Aynı zamanda teknik ekiplerinde ISO27001 süreçleri hakkında eğitim ihtiyaçlarının olduğu yönünde görüş bildirdikleri de görülmüştür. Diğer taraftan teknik ekip tarafından geliştirilen kurumsal uygulamalarının güvenliğine de ISO27001 uyum sürecinin olumlu yönde katkı sağladığı şeklindeki görüşlerin ağırlıkta olduğu görülmüştür. Aynı zamanda verilen cevaplar doğrultusunda, ISO27001'e geçiş ile birlikte yaşanan bilgi güvenliği olaylarının sayısında önemli ölçüde bir azalma olduğu yönünde de değerlendirme yapılabilmektedir.

Kurum personelinin genel farkındalık seviyeleri, almış oldukları eğitimler ve BGYS hakkındakileri düşüncelerinin öğrenilmeye çalışıldığı bu bölümde alınan cevaplar incelendiğinde, genel olarak personelin almış oldukları farkındalık eğitimlerinden memnun oldukları, içeriklerinin ve sürelerinin yeterli olduğu fakat sadece slaytlar üzerinde yapılan eğitimlerin yeterli olmayacağı şeklinde görüş bildirdikleri görülmüştür. Aynı zamanda eğitim firmalarının veya eğitmenlerin eğitimde vermiş oldukları bilgilerin güncel ve diğer kurumlar elde etmiş oldukları bilgileri de içerdiği yönünde görüş bildirdikleri görülmüştür. Bununla birlikte personelin yetkilerinin aşırı derece kısıtlanıp kısıtlanmadığı şeklindeki soruya verilen cevapta ise olumlu ve olumsuz cevapların birbirine yakın olduğu farklı görüşler arasında çok önemli bir fark olmadığı görülmüştür.

Sonuç olarak, personel açısından yapılan inceleme sonucunda ise kurum personeline verilen bilgi güvenliği farkındalık eğitimlerinin içeriği, süresi ve sağladığı fayda açısından olumlu bulunduğu görülmüştür. Diğer taraftan personel tarafında da uygulanan kontrolleri ve yetki kısıtlamalarının çok fazla olduğu yönünde görüşlerin olduğu da görülmektedir. Genel anlamda personel tarafında kurulan sisteme karşı bir güven olduğu, ISO27001 in kurum personeli tarafından benimsendiği ve kurumlarında BGYS süreçlerinin etkin bir şekilde yönetildiğini düşündükleri yönünde görüş bildirdikleri görülmüştür.

4.1. Öneriler

Bu bölümde uygulanan anket çalışmalarından elde edilen bulgulara dayalı olarak geliştirilen öneriler aşağıda farklı başlıklar altında verilmiştir.

Yönetim kademesine yönelik öneriler

- Yönetim kademesinin büyük oranda üzerine düşen sorumluluklar konusunda bilgi sahibi olmadıkları görülmüştür. Bunun için Siber Eylem Planları veya genelgelerle yönetim kademesine özel yönlendirmeler yapılabilir.
- Yönetim kademesine uygun farkındalık ve sahiplenme seviyelerinin ölçümünün yapılabilmesi amacıyla bir çalışma yapılabilir.
- BGYS çalışmalarının öneminin özellikle yönetim kademesine daha detaylı aktarılarak sahiplenme seviyelerinin artırılması sağlanabilir.
- Kurulan bilgi güvenliği yönetim sisteminin gerekliliğin yönetim kademesi tarafından daha iyi algılanabilmesi için risk çalışmaları dâhil edilmesi sağlanabilir.
- Kamu yöneticileri ile bir çalışma yürütülerek ortak BGYS kurulum yönergesi oluşturulması üzerinde çalışılabilir.
- Kamu yöneticileri ile birlikte kamu kurumlarına özel risk ve fırsatların çalışması yapılabilir.

BGYS ekibine yönelik öneriler

- BGYS ekiplerinin kurulumuna daha fazla özen gösterilmelidir. Kurulan ekibin sorumlulukları net bir şekilde belirlenmeli ve eğitim seviyesi uygun personeller arasından seçilmelidir.

- BGYS ekip üyelerinin sayılarının yetersiz olduğu düşünülmektedir. Bu konuda kurum personel sayısı ile doğru orantılı olacak şekilde ekip üyeleri belirlenmelidir.

- Ekip üyeleri her ne kadar farkındalık eğitimlerinde kurum personeline tanıtılıyor olsa da personelin büyük çoğunluğunun ekip üyelerini tanımadıkları görülmüştür. Bununla ilgili bilgilendirmelerin daha etkin bir şekilde yapılması sağlanabilir.

- Ekip üyelerinin çalışmalarının kolaylaştırılması amacıyla, üst yönetim tarafından tüm birimlerden atama yolu ile görevlendirmeler yapılarak ve kurum personelinin de BGYS yönetim süreçlerini sahiplenmesi sağlanabilir.

- BGYS ekip üyelerinin kurumsal risk çalışmalarında kurum personeli ile uyumlu bir şekilde çalışamadığı tespit edilmiştir. Bu süreçte görevlendirilen kurum personeline risk belirleme ve işleme konularında eğitim verilmesi sürecin daha etkin bir şekilde yönetilmesine katkı sağlayabilir.

- BGYS ekip üyelerinin sahiplenme seviyelerinin artırılması amacıyla çalışmalar yapılabilir.

- BGYS ekip üyelerinin kendilerini yetersiz buldukları ve eğitim ihtiyaçları olduğu yönünde görüş bildirdikleri görülmüştür. Bu kapsamda ihtiyaç duyulacak tüm eğitim içeriğinin belirlenmesi ve görevlendirme öncesinde tüm eğitimlerin alınması sağlanabilir.

- BGYS ekip üyelerinin tamamen bilgi işlem personellerinden oluşmaması gerektiği yönünde bir görüş bildirenlerin olduğu görülmüştür. Ekip üyelerine bilgi işlem personeli dışında da görevlendirmeler yapılabilir.

- BGSY ekip üyeleri ile ilgili daha detaylı bir çalışma yapılarak, ekip üyelerinin görev tanımlarının netleştirilmesi ve hatta ekibe özel kadro çalışması yapılması sağlanabilir.

- BGYS ekip üyelerinin görev tanımları siber eylem planları veya yönergeler ile desteklenebilir.

Teknik ekibe yönelik öneriler

- Teknik personel sayılarının yetersiz olduğu yönünde görüşün ağırlıklı bir şekilde dile getirildiği görülmüştür. Bu kapsamda teknik ekip üyelerinin sayılarının artırılması sağlanmalıdır.

- ISO27001 konusunda teknik ekiplerin bilgi seviyelerinin yeterli olmadığı fakat buna rağmen süreci sahiplendikleri görülmektedir. Bunun sebebi olarak operasyonel süreçlerin yönetilmesi sistemin olumlu yönde katkı sağladığı düşünülebilir. Bu sebeple teknik ekibin ISO27001 hakkında farkındalık seviyelerinin artırılması sebebiyle temel BGYS eğitimleri verilebilir.

- Yazılım ekiplerinin, çalışmaları sırasında bilgi güvenliği konularına daha fazla özen göstermeleri sağlanabilir. Bu kapsamda güvenli kod geliştirme, temel BGYS, temel ağ güvenliği gibi giriş seviyesinde eğitimler verilerek farkındalık seviyelerinin artırılması sağlanabilir.

- BGYS kapsamında yapılan sızma testlerine yazılım ekiplerinin daha aktif katılımları sağlanabilir.

Personele yönelik öneriler

- Farkındalık eğitimlerinin sunumlardan ziyade uygulamalı şekilde ve somut örnekler üzerinden verilmesinin daha faydalı olacağı düşünülmektedir.

- Farkındalık eğitimlerinin sürelerinin ve içeriklerinin yeterli olduğu fakat içeriğinin her eğitimde aynı olmasının katılım isteğini olumsuz yönde etkilediği görülmüştür. Bu sebeple eğitim süreleri mümkün olduğu kadar kısa ve eğitim içeriği de her eğitimde değiştirilerek planlanabilir.

- BGYS kapsamında alınan önlemler doğrultusunda yapılan kısıtlamaların personelin bir kısmı tarafından fazla bulunduğu görülmüştür. Bunun personelin farkındalık seviyeleri ile ilişkili olduğu düşülmektedir. Farkındalık eğitimlerinde özellikle yetkilendirmeler ile ilgili bilgilendirmelere ağırlık verilmesi sağlanabilir.

KAYNAKÇA

Achmadi, D., Suryanto, Y., & Ramli, K. (2018, 12-13 May 2018). On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. Paper presented at the 2018 International Workshop on Big Data and Information Security (IWBIS), Jakarta, Indonesia.

Akay, İ. G. (2014). Bilgi güvenliği yönetim sistemleri: Bilgi güvenliği uygulama mülakatları. Bilecik Şey Edebali Üniversitesi, Bilecik.

Arce, I. (2003). The weakest link revisited [information security]. IEEE Security & Privacy, 1(2), 72-76. doi:10.1109/msecp.2003.1193216

Asosheh, A., Hajinazari, P., & Khodkari, H. (2013). A practical implementation of ISMS. Paper presented at the 7th International Conference on e-Commerce in Developing Countries:with focus on e-Security, Kish Island, Iran. https://ieeexplore.ieee.org/ielx7/6552353/6556712/06556730.pdf?tp=&arnumber=6556730&isnumber=6556712

Aydoğmuş, E. (2010). Türkiye'deki organizasyonların bilgi güvenliği olgunluk seviyelerinin belirlenmesi ve ISO/IEC 27001:2005 standardına uyumluluklarının değerlendirilmesi. İstanbul.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. Politeknik Dergisi, 9(3), 165-174.

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report, 14(4), 186-196. doi:10.1016/j.istr.2010.04.004

Çek, E. (2017). Kurumsal Bilgi Güvenliği Yönetişimi Ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi. İstanbul Bilgi Üniversitesi, İstanbul.

Demirtaş, H. (2013). Bilgi Güvenliği Yönetiminin Gerekleri Ve Başarı Dayanakları: Bir Uygulama Örneği. (Yüksek Lisans), Sakarya Üniversitesi.

Ganbat, O. (2013). Bilgi güvenliği yönetim sistemi ISO/IEC 27001 ve bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması. (Yüksek Lisans Tezi), İzmir.

Gencer, K. (2015). ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım. Afyon Kocatepe Üniversitesi.

Gikas, C. (2010). A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. Information Security Journal: A Global Perspective, 19(3), 132-141. doi:10.1080/19393551003657019

Güldüren, C. (2015). Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi. (Doktora Tezi), Ankara Üniversitesi, Ankara.

Gürcan, İ. A. (2014). Finans sektörü için bilgi güvenliği yönetim gereksinimlerinin ISO 27001 tabanlı incelenmesi. İstanbul.

Haklı, T. (2012). Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi. (Yüksek Lisans Tezi), Isparta.

ISO. (2017). Uluslararası Standart Organizasyonu 2017 İstatistik Raporu. Retrieved from https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

ISO. (2019). Uluslararası Standart Organizayonu Web Sayfası. Retrieved from https://www.iso.org/

King, K. E. (2017). Examine the relationship between information technology governance, control objectives for information and related technologies, ISO 27001/27002, and risk management. (10256918 Ph.D.), Capella University, Minneapolis, USA. Retrieved from https://search.proquest.com/docview/1877918458?accountid=11054

http://JJ2EC6WC6Q.search.serialssolutions.com?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQuest+Dissertations+%26+Theses+Global&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&rft.genre=dissertations+%26+theses&rft.jtitle=&rft.atitle=&rft.au=King%2C+Kenneth+E.&rft.aulast=King&rft.aufirst=Kenneth&rft.date=2017-01-01&rft.volume=&rft.issue=&rft.spage=&rft.isbn=9781369575507&rft.btitle=&rft.title=Examine+the+relationship+between+information+technology+governance%2C+control+objectives+for+information+and+related+technologies%2C+ISO+27001%2F27002%2C+and+risk+management&rft.issn=&rft_id=info:doi/ ProQuest Dissertations & Theses Global database.

Mete, H. (2010). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin bilgi işlem merkezlerinde uygulanması. Sakarya.

Rhodes-Ousley, M. (Ed.) (2013). Information Security, Complete Reference. San Francisco: McGraw-Hill Education.

Shoraka, B. (2011). An Empirical Investigation of the Economic Value of Information Security Management System Standards. (3456209 Ph.D.), Nova Southeastern University, Florida, USA. Retrieved from https://search.proquest.com/docview/871586434?accountid=11054

http://JJ2EC6WC6Q.search.serialssolutions.com?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQuest+Dissertations+%26+Theses+Global&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&rft.genre=dissertations+%26+theses&rft.jtitle=&rft.atitle=&rft.au=Shoraka%2C+Babak&rft.aulast=Shoraka&rft.aufirst=Babak&rft.date=2011-01-01&rft.volume=&rft.issue=&rft.spage=&rft.isbn=9781124655314&rft.btitle=&rft.title=An+Empirical+Investigation+of+the+Economic+Value+of+Information+Security+Management+System+Standards&rft.issn=&rft_id=info:doi/ ProQuest Dissertations & Theses Global database.

UDHB. (2017). KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ. Retrieved from http://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm

UHDB. (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. Retrieved from http://www.edevlet.gov.tr/wp-content/uploads/2016/07/2016-2019-Ulusal-e-Devlet-Stratejisi-ve-Eylem-Plani.pdf

AĞ TABANLI VERİ SIZINTISI TESPİTİ VE ÖNLENMESİ ÜZERİNE BİR İNCELEME

***

A REVIEW ON NETWORK BASED DATA LEAKAGE DETECTION AND PREVENTION

Cengiz PAŞAOĞLU[*]
Habibe GÜLER[**]
Masoma JAFARI[***]

DOI: 10.33461/uybisbbd.611768

Öz

Bilgi güvenliği sistemlerinin temel amacı yetkisiz kişilerce gerçekleştirilen veri ihlallerine karşı önlem almaktır. Bu sebeple, kullanımda, hareket halinde veya durağan durumda olan gizli/hassas verilerin sızıntılarının tespiti ve önlenmesinde daha etkili çözümler sunabilen veri sızıntısı önleme sistemleri (DLPS-Data Leakage Prevention System) geliştirilmiştir. Bu çalışma kapsamında, özellikle ağ tabanlı veri sızıntısı tespit (DLP-Data Leakage Prevention) sistemleri üzerinde durularak veri sızıntısı tespitinde kullanılan bağlam tabanlı, içerik tabanlı ve içerik etiketleme yöntemleri detaylı bir şekilde açıklanmıştır. Bunun yanı sıra önleme yöntemleri de incelenmiştir. Son olarak günümüz DLP sistemlerinin yaygın olarak karşılaştığı zorluklardan bahsedilmiştir.

***Anahtar Kelimeler**: Hassas Veri, DLPS, Bağlam Tabanlı Denetim, İçerik Tabanlı Denetim, İçerik Etiketleme, Ağ Tabanlı Veri Sızıntısı Tespiti.*

Abstract

The main purpose of information security systems is to take measures against unauthorized data violations. For this reason, Data Leakage Prevention Systems (DLPS) which can provide more effective solutions in detecting and preventing leakage of confidential data in use, in motion or at rest, have been developed. In this study, context-based, content-based and content tagging methods that are used -especially with network based Data Leakage Prevention (DLP) systems- in data leak detection are explained in detail. In addition, prevention methods are also examined. In conclusion, the challenges encountered by today's DLP systems have been discussed.

***Keywords:** Sensitive Data, DLPS, Context Based Method, Content Based Method, Content Tagging, Network Based Data Leakage Detection.*

[*] Dr., Kişisel Verileri Koruma Kurumu, cengizpasaoglu@kvkk.gov.tr,
ORCID: 0000-0002-4583-5461
[**] Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, habibeguler@outlook.com,
ORCID: 0000-0003-2607-4801
[***] Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, masomashams1@gmail.com,
ORCID: 0000-0003-0824-8601

Geliş Tarihi / Received: 27.08.2019
Kabul Tarihi / Accepted: 09.10.2019

1. GİRİŞ

Günümüzde hassas/gizli verilerin ifşası bireyler ve organizasyonlar için giderek büyüyen bir sorun haline gelmeye başlamıştır. Bilgi güvenliği sistemlerinin temel amacı yetkisiz kişilerce gerçekleştirilen veri ihlallerine karşı önlem almaktır. Veri sızıntısı riskine karşı güvenlik duvarları (firewall), sanal özel ağlar (VPN-Visual Private Network), saldırı tespit ve önleme sistemleri (IDS/IPS-Intrusion Detection/Prevention Systems) gibi birçok geleneksel güvenlik çözümü vardır. Ne var ki, bu sistemler veri sızıntılarının tespiti ve önlenmesinde yetersiz kalmaktadır. Hassas/gizli veriler farklı sızıntı kanallarında farklı formlarda olabileceği için bu sistemlerin yetersizliği sebebiyle gerçekleşecek veri sızıntıları hem bireyler hem de organizasyonlar açısından çok ciddi sonuçlara yol açabilir. Bu sebeple, kullanımda, hareket halinde veya durağan durumda olan verilerin sızıntılarının tespiti ve önlenmesinde daha etkili çözümler sunabilen veri sızıntısı önleme sistemleri geliştirilmiştir.

Bu çalışma kapsamında özellikle ağ tabanlı veri sızıntısı tespit sistemleri tarafından kullanılan yöntemler üzerine kapsamlı bir inceleme yapılmıştır. Bu bağlamda makale yedi ana başlık altında ele alınmıştır. Öncelikle veri sızıntısı problemi ele alınarak konu hakkında genel bilgiler verilmiştir. Daha sonra konu ile ilgili literatür taramasına yer verilmiştir. İlerleyen bölümlerde önce veri sızıntısı tespitinde yaygın olarak kullanılan yöntemler üç ana başlık altında irdelenmiş sonrasında ağlarda veri sızıntısı tespiti detaylandırılmıştır. Bunun yanı sıra veri sızıntıları önleme yöntemlerinden de bahsedilmiştir. Son olarak günümüz DLP sistemlerinin yaygın olarak karşılaştığı zorluklardan bahsedilerek sonuç bölümü ile makale sonlandırılmıştır.

2. VERİ SIZINTISI PROBLEMİNE GENEL BAKIŞ

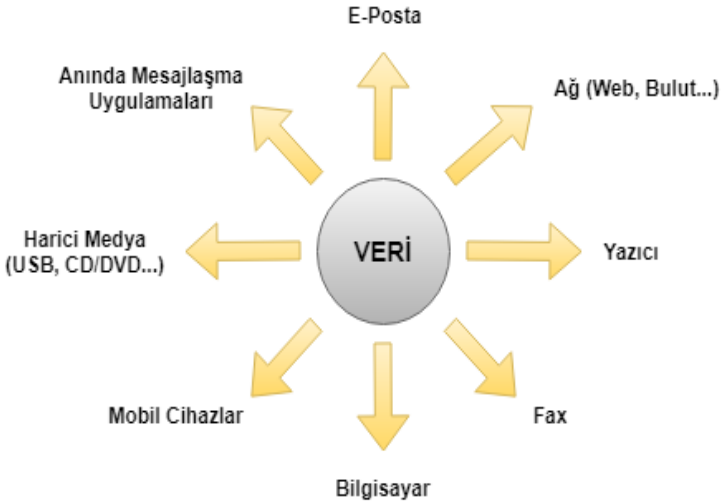
Bilgi piramidinin temelinde yer alan veri kavramı, işlenip anlamlandırılmamış en küçük bilgi (information) parçasına verilen isimdir. Henüz işlenmemiş veriler tek başlarına bir anlam ifade etmezler fakat belirli kriterlerde bir araya gelmeleri sonucu önemli hale gelirler.

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir (Kişisel Verilerin Korunması Kanunu, 2016). Genel bir ifade ile hassas veri ise sadece yetkili kişi veya kişiler tarafından erişilebilen ve herhangi bir kanuni dayanak olmadan ifşa edilmeye karşı korunan bilgiler olarak tanımlanabilir. Hassas/özel nitelikli kişisel veriler (ırk, etnik köken, din, mezhep, siyasi düşünce, sağlık vb.), başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikteki verilerdir (Kişisel Verilerin Korunması Kanunu, 2016). Öte yandan şirketler, kurum ve kuruluşlardaki hassas veriler ise fikri mülkiyet, finansal bilgiler, hasta bilgileri, kişisel kredi kartı verileri, iş ve işletmeye bağlı diğer bilgilerden oluşmaktadır (Shabtai, Elovici, & Rokach, 2012). Kısaca kurumsal veri ise kurumlar tarafından kullanılan, işletilen veya üretilen verilerdir. Bahsi geçen tüm bu kavramlar doğrultusunda veri sızıntısı, hassas/gizli kurumsal veriler ya da hangi nitelikte olduğuna bakılmaksızın kişisel verilerin ihmal/kaza yahut kasti bir şekilde hukuka aykırı olarak, farklı yollardan yetkisiz kişilerin eline geçmesi olarak tanımlanabilir.

2.1. Veri Sızıntısı Kanalları

Farklı kanallar vasıtasıyla birçok sebepten ötürü veri sızıntıları gerçekleşmektedir. INFOWATCH güvenlik firması tarafından hazırlanan 2017 yılı küresel veri sızıntısı raporuna göre (Global Data Leak Report, 2017) veri sızıntılarının en çok %69,8 ile ağ üzerinden gerçekleştiği görülmektedir. Bunu %13,3 ile e-postalar, %8,2 ile yazdırılan dokümanlar takip etmektedir. Yine aynı rapora göre 2017 yılında gerçekleşen veri sızıntılarının %60,5 gibi büyük bir çoğunluğu içeriden kaynaklı, %39,5'i ise dışarıdan kaynaklı sızıntılardır. Veri sızıntısına bilinçli veya bilinçsiz yollarla %50,3 oranında çalışanların sebep olduğu görülmektedir. %41,7 ile bunu harici saldırganlar takip etmektedir. Tüm bunlara ek olarak sızdırılan verilerin %64,8'i kişisel verilerden, %21,1'i

ödeme ayrıntılarından, %8'i ticari sırlar ve teknik bilgilerden, %6,1'inin ise devlet sırlarından oluştuğu görülmektedir. Şekil 1'de veri sızıntılarının gerçekleştiği bazı kanallar görülmektedir.



Şekil.1. Bazı veri sızıntısı kanalları

2.2. Veri Sızıntılarının Etkileri ve Sonuçları

Hassas veriler, stratejik gereksinimler, iş gizliliği, veri gizliliği, hukuki yükümlülükler, kişisel verilerin gizliliği, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA- Health Insurance Portability and Accountability Act), Gramm–Leach–Bliley Yasası (GLBA- Gramm–Leach–Bliley Act), BASEL II (Uluslararası Bankacılık 2. Basel Uzlaşısı), Sarbanes-Oxley Yasası (Sarbanes-Oxley Act), Veri Güvenliği Standardı (DSS- Data Security Standard) gibi sağlık, finans, bankacılık ve birçok alanda kullanılan verilerin güvenliğini sağlamaya yönelik çıkarılan yasalara, yönetmeliklere ve uluslararası bilgi güvenliği standart ve akreditasyonlarına uyum açısından önemli olup sızıntılara karşı korunması gereken verilerdir (Başak, 2016). Söz konusu verilerin kanuni olmayan yollarla başkaları tarafından ele geçirilmesine veri ihlali denilmektedir. Gerek ülkemizde 2016 yılında çıkarılan Kişisel Verilerin Korunması Kanunu (KVKK), gerekse Avrupa Birliği Parlamentosu tarafından 2016 yılında kabul edilip Mayıs 2018 yılında yürürlüğe giren Genel Veri Koruma Tüzüğü (GDPR-General Data Protection Regulation) kapsamında veri ihlalleri hususu özel maddeler ile düzenlenmiştir.

Hem kötücül yazılımlar, davranışlar, tutumlar veya düşüncelerle hem de istenmeyen bir durum ile içeriden veya dışarıdan hassas verilerin saldırıya maruz kalmaları, bir kurumu veya organizasyonu ciddi bir şekilde zarara uğratabilmektedir (Canbay ve Sağıroğlu, 2016). Saldırılar sonucu oluşabilecek veri sızıntılarının dolayısıyla veri ihlallerinin kurum veya kuruluşlara hem maddi olarak hem de hukuki olarak ciddi olumsuz etkileri olabilmektedir. Sonuç olarak kurumlar itibarlarını ve hatta müşterilerini kaybetmekte bunun sonucunda hisse senetleri düşmekte ve dolaylı olarak daha çok maddi zarara uğramaktadırlar. Bu noktada veri sızıntısı probleminin günümüzde gerek ülkemizdeki gerekse dünyadaki tüm kurum ve kuruluşlar için çok büyük ve en önemli problemlerden biri olduğu açıkça görülmektedir. Ponemon Enstitüsü'nün IBM'in de sponsorluğunda yaptığı çalışma sonucu yayınladığı 2018 Veri İhlalinin Küresel Maliyeti raporuna göre (Cost of a Data Breach Study: Global Overview, 2018) bir veri ihlalinin küresel ortalama toplam maliyetinin 3.86$ milyon dolar olarak hesaplandığı görülmektedir. Ülkeler bazında incelendiğinde ise ABD'nin ortalama 7.91$ milyon dolar ile en yüksek paya sahip olduğu, bunu 5.31$ ve 4.74$ milyon dolar ile sırasıyla Orta Doğu ülkeleri ve Kanada'nın takip ettiği görülmektedir. Söz konusu rapora göre Türkiye 2.16$ milyon dolar ortalama maliyet ile 12. sırada yer almaktadır. Bu açıdan bakıldığında veri ihlalleri sonucu ülkemizin mali kaybının ortalamadan

kısmen daha az olduğu söylenebilir, ancak ülkemiz anılan raporda da vurgulandığı üzere en çok kaybı olan ilk 15 ülke içinde yer almaktadır.

3. LİTERATÜR TARAMASI

Bu bölümde makale kapsamında incelenen ve makalenin hazırlanmasında yol gösterici olan bazı çalışmalar ele alınacaktır. Bu bağlamda ağ tabanlı veri sızıntılarının tespiti ve önlenmesine yönelik çalışma yapan ve yeni yaklaşımlar öneren makaleler incelenmiştir.

İncelenen söz konusu makalelerin birçoğunda veri sızıntısı tespitine yönelik yöntemlerin ele alındığı görülmektedir. Bunlardan (Trieu, Tran, Tran, & Tran, 2017) ve (Alneyadi, Sithirasenan, & Muthukkumarasamy, 2015) de yapılan çalışmalarda hem tespit hem de önleme/engelleme yöntemlerinin beraber kullanıldığı görülmüştür.

Yine bu makalelerde ağdaki paketleri analiz ederken içerik tabanlı analiz tekniği olan istatistiksel analiz tekniğinin yaygın olarak kullanıldığı görülmüştür. (Shu, Zhang, Yao, & Feng, 2016) ve (Canbay, Yazıcı, & Sağıroğlu, 2017) yaptıkları çalışmalarında istatistiksel analiz yönteminin yanında anahtar kelime eşleme yöntemini de kullanarak ağ tabanlı veri sızıntılarının tespitini yapmayı hedeflemektedirler. (Huang, Lu, Li, & Ma, 2018; Katz, Elovici, & Shapira, 2014; Soumya & Smitha, 26 June, 2014) de incelenen diğer makalelerden farklı olarak, bağlam tabanlı yönteme yeni bir yaklaşım getirerek veri sızıntılarının tespitine yönelik çalışmalar önermişlerdir.

İncelenen çalışmalarda önerilen yöntemlerin performans ölçümleri için farklı birçok ölçütün kullanıldığı görülmüştür. Bunlar; ayrım eşik değerinin farklılık gösterdiği durumlarda doğru pozitiflerin yanlış pozitiflere olan kesri ile hesaplanan alıcı işletim karakteristiği (ROC- Receiver Operating Characteristic), doğruluk (ACC- Accuracy), kesinlik (precision), hassasiyet (recall), tespit oranı (DR- Detection Rate), doğru pozitif, yanlış pozitif ve yanlış negatif oranı (TPR-True Positive Rate, FPR- False Positive Rate, FNR- False Negative Rate) olarak söylenebilir. Ek olarak önerilen bu modellerin verinin hangi durumu için uygun oldukları konusuna da incelenen çalışmalarda değinilmiştir. Bu bağlamda durağan veri (DAR- Data At Rest), kullanımda veri (DIU- Data In Use) ve hareket halinde veri (DIM- Data In Motion) olarak veri durumu sınıflandırılabilir. Sonuç olarak bu çalışmalar tarafından kullanılan yöntem, analiz tekniği, verinin hangi durumu için uygun olduğu ve önerdikleri modelin doğruluğunu test etmek üzere kullandıkları performans metriği Tablo 1' de özetlenerek incelenen makalelerin benzerlikleri ve farklılıkları ortaya konmuştur.

Tablo 1: Literatür İncelemesi

Makale	***Yöntem***	**Analiz Tekniği**	**Veri Durumu**	**Performans Ölçütü**
(Trieu vd., 2017)	Tespit/Önleme	İçerik Tabanlı – İstatistiksel Analiz + Makine Öğrenmesi	DIU, DIM, DAR	DR, FNR
(Alneyadi vd., 2015)	Tespit/Engelleme	İçerik Tabanlı – İstatistiksel Analiz	DIM	Precision, Recall
(Shu vd., 2016)	Tespit	İçerik Tabanlı – Anahtar Kelime Eşleme + İstatistiksel Analiz	DIM, DAR	TP, FP
(Canbay vd., 2017)	Tespit	İçerik Tabanlı – Anahtar Kelime Eşleme + İstatistiksel Analiz	DIM	ACC
(Soumya ve Smitha, 2014)	Tespit	Bağlam Tabanlı	DIM	DR
(Katz vd., 2014)	Tespit	Bağlam Tabanlı (CoBAn)	DIM	TPR, FPR
(Huang vd., 2018)	Tespit	Bağlam Tabanlı (AGW)	-	ACC, ROC, Recall
(Liu vd., 2009)	Tespit	İçerik Tabanlı – İstatistiksel Analiz	DIM	ROC
(Gugelmann, Studerus,	Tespit	İçerik Tabanlı	DIM	-

Lenders, & Ager, 2015)				
(Hemalatha, Somasundaram, & Thirugnanam, 2016)	Tespit	İçerik Tabanlı – İstatistiksel Analiz	DIM	-
(Shu, Yao, & Bertino, 2015)	Tespit	İçerik Tabanlı – Bulanık Parmak izi	DIM	FNR, FPR
(Breitinger ve Baggili, 2014)	Tespit	İçerik Tabanlı- Yaklaşık Eşleşme	DIM	DR
(Shapira, Shapira, & Shabtai, 2013)	Tespit	İçerik Tabanlı – Parmak izi (Geliştirilmiş Versiyon)	-	ROC

4. VERİ SIZINTISI TESPİTİ VE ÖNLENMESİ

Veri sızıntısı tespitine yönelik yaklaşımlar kurum dışına çıkarılmaması gereken hassas verilerin korunmasına yönelik bir takım tespit ve önleme teknikleri kullanırlar. Bu tanıma göre S. Alneyadi ve ark. (Alneyadi, Sithirasenan, & Muthukkumarasamy, 2016) yazdıkları inceleme yazısında veri sızıntısı önleme sistemlerini geleneksel yöntemlerden ayıran üç temel özelliği olduğundan bahsetmişlerdir. Bu özellikler;

- DLP sistemleri hassas veya gizli verilerin ve bunları çevreleyen kaynağın içeriğini analiz edebilmektedir,
- DLP sistemleri hareket halinde, kullanımda veya durağan durumda olan gizli veriler için koruma sağlayabilir,
- DLP sistemleri bildirme, denetleme, engelleme, şifreleme gibi birtakım eylemler yoluyla gizli veriyi koruyabilmektedir.

şeklinde sıralanabilir.

4.1. DLP Tanımı

Güvenlik duvarları (firewall), saldırı tespit sistemleri (IDS-Intrusion Detection Systems), saldırı önleme sistemleri (IPS-Intrusion Prevention Systems) ve sanal özel ağlar (VPN-Virtual Private Network) gibi geleneksel sistemlerin veri sızıntılarının tespiti ve önlenmesi konusunda yetersiz kaldığı görülmüştür (Alneyadi vd., 2016). Bu sorunun üstesinden gelmek ancak veri sızıntısı tespiti ve önlenmesine yönelik yeni bir sistemin olması ile mümkündür. Bu noktada veri sızıntısı önleme çözümleri devreye girmektedir. DLP sistemleri ilk kez 2006 yılında geliştirilmeye başlanmıştır, bu sebeple henüz yeni bir sistem olarak kabul görmektedir.

Shabtai ve arkadaşları (Shabtai vd., 2012) DLP çözümünü "gizli bilgilerin yetkisiz erişimi, kullanılması veya iletilmesini önlemek için tasarlanmış bir sistem" olarak adlandırmışlardır. Başka bir çalışmada (Mogull ve Securosis, 2007) ise DLP çözümleri, beklemede, kullanımda veya hareket halindeki verileri derin içerik analizi vasıtasıyla tanımlayan, izleyen ve koruyan merkezi politikalara dayanan ürünler olarak tanımlanmaktadır. DLP çözümleri, hem yetkili olmayan bir kullanıcının gizli verilere erişmesini tespit etme ve önlemede hem de gizli verilerin yanlışlıkla paylaşılmasını engellemek için kullanılmaktadır (Tahboub ve Saleh, 2014) .

4.2. Veri Sızıntısı Tespit Yöntemleri

Veri sızıntısı tespitinde kullanılan yöntemler, incelenen makalelerden (Alneyadi vd., 2016; Mogull ve Securosis, 2007; Shabtai vd., 2012) yola çıkılarak üç ana başlıkta incelenebilir. Bunlardan en yaygın olarak karşımıza çıkan yöntemler ise içerik tabanlı denetim yapan veri sızıntısı

tespit yöntemleridir. Bu yöntemler aynı zamanda ağ tabanlı veri sızıntısı tespitinde derin paket analizinde kullanılmaktadır.

Veri sızıntılarını DLP sistemleri yardımıyla doğru bir şekilde tespit edebilmek için öncelikle verinin durumunu ve verinin hassas nitelikli/gizli veri olup olmadığını belirlemek gereklidir. DLP sistemleri farklı yaklaşımlar kullanarak verinin 3 durumu için de çözüm sunmayı amaçlamaktadır. Bu durumlar şu şekilde tanımlanabilir;

- Durağan veri (Data-at-Rest), diğer bir deyişle kaynakta duran veriler, veri tabanlarında, dosya ve ağ sunucularında, bulut depolama alanlarında, dosya yönetim sistemlerinde, sabit diskler veya hafıza kartları gibi veri depolama cihazlarında depolanan henüz kullanılmayan ve hareket halinde olmayan verilerdir. Bu tip verilerin yetkisiz kişilerce erişimi, çalınması veya değiştirilmesini engellemek için genellikle veri şifreleme veya erişim kontrolü gibi güvenlik önlemleri alınır (Shabtai vd., 2012). Bu önlemlerin alınabilmesi için öncelikle içeriklerin nerede tutulduğunun bilinmesi gerekmektedir. Bu noktada depolanan hassas içeriklerin tespit edilmesinde DLP sistemlerinin içerik keşif özelliği kullanılmaktadır (Securosis, 2010; Shabtai vd., 2012).
- Kullanımda olan veri (Data-in-Use), bu tip veriler herhangi bir kullanıcı veya yazılım tarafından etkileşimde olunan verilerdir. Word, Excel gibi ofis dosyaları, veri tabanı erişimleri, bulut uygulamaları veya mobil uygulamalar tarafından kullanılan veriler bunlara örnek olarak verilebilir. Uç nokta ile ilgili DLP sistemleri bu tip verileri korumak ve kullanıcı bu verilerle etkileşime girdiğinde verileri izlemek için kullanılırlar (Securosis, 2010; Shabtai vd., 2012). Kullanımdaki verileri korumaya yönelik geliştirilen DLP araçları kopyala-yapıştır, ekran görüntüsü alma, USB, CD-DVD veya akıllı telefona aktarma, yazdırma ve fakslama gibi faaliyetleri izleyerek hassas verilerin kurum dışına çıkarılmasını engellemeye çalışmaktadır (Shabtai vd., 2012).
- Hareket halindeki veri (Data-in-Motion), kurum içinde bir yerden bir yere giden veya internet yoluyla kurum dışına giden verilerdir. Hareket halindeki veriler için geliştirilen DLP çözümleri iletişim kanalları vasıtasıyla ağ üzerinden bilinen veya bilinmeyen protokoller kullanılarak gönderilen verilerin organizasyon tarafından önceden belirlenmiş politikalar doğrultusunda incelenerek hassas veri olup olmadığının tespiti için kullanılır (Al-Sanabani, 2016; Shabtai vd., 2012).

Bu kapsamdaki denetim yaklaşımları sonraki kısımlarda ele alınmıştır.

4.2.1. Bağlam Tabanlı Denetim

Bu yaklaşımda sistem temel olarak denetimi yapılacak dosyanın alıcı/gönderici, zaman, boyut, format ve başlık bilgileri gibi meta verileri üzerinde inceleme yapar. Bu meta verilere ek olarak günümüz sistemleri tarafından bağlam-tabanlı denetim kapsamında dosya sahibi ve izinleri, kullanılan şifreleme formatı veya ağ protokolleri, web tabanlı e-posta ve sosyal ağ siteleri gibi özel servisler, site adresleri, masaüstü uygulamaları gibi faktörlerde analiz edilmektedir (Mogull ve Securosis, 2007).

4.2.2. İçerik Tabanlı Denetim

Tipik bir içerik tabanlı DLP sistemi düzenli ifadeler, veri parmak izi, istatistiksel analiz gibi yöntemleri kullanarak veri havuzunda veya hareket halinde olan hassas verileri izleyerek çalışır (Alneyadi vd., 2016). İçerik tabanlı analiz yapılırken veriyi çevreleyen bağlamdan ziyade verinin kendisi üzerinde denetim amaçlanır, bu sebeple içerik tabanlı denetim yaklaşımı bağlam tabanlı denetim yaklaşımına göre daha yaygın ve tercih edilen bir yöntemdir (Securosis, 2010).

Aynı zamanda derin içerik analiz teknikleri olarak da kabul edilen içerik tabanlı denetim tekniklerinden yaygın olarak kullanılanları (Kaur, Gupta, & Singh, 2017; Mogull ve Securosis, 2007; Securosis, 2010) aşağıda olduğu gibi altı başlıkta incelenebilir.

4.2.2.1. Parmak izi oluşturma

En bilinen içerik tabanlı denetim yaklaşımlarından biri olan ve parmak izi çıkarma olarak bilinen metinsel bir özellik oluşturulan bu yöntemde, hassas nitelikli veri içerdiği bilinen dosya veya veri tabanı girdilerinin genellikle özet (hash) fonksiyonları yardımıyla parmak izi çıkarılır, bu bilgiler bir veri tabanında veya incelenecek olan makinede yerel olarak saklanabilir, incelenecek olan içeriklerinde aynı şekilde parmak izi çıkarılır ve daha önceden saklanmış parmak izi bilgileriyle karşılaştırılarak veri sızıntısı olup olmadığını tespit etmek için tam eşleşme aranır (Al-Sanabani, 2016; Shabtai vd., 2012; Shapira vd., 2013).

Y. Shapira ve ark. (Shapira vd., 2013) tarafından yapılan çalışmada parmak izi yönteminin kullanılan özet fonksiyonlarına göre 4 farklı tipte olduğu görülmektedir. Bunlar; klasik, bölgeye duyarlı karma (LSH-Locality Sensitive Hashing) tabanlı, toplama istatistikleri tabanlı, ankraj tabanlı parmak izi oluşturmadır.

Parmak izi oluşturma yöntemi normal koşullarda düşük oranda yanlış alarm verse de bazı kısıtları olabilmektedir. Örneğin, parmak izi çıkarılmış bir dosyada yapılan herhangi küçük bir değişiklik bu dosyadan üretilen özet değerinin farklı olmasına yol açacaktır bunun sonucunda gizli içerikteki bazı karakterler değiştirilerek bu yöntem bypass edilebilir (Shapira vd., 2013). İkinci olarak ise, parmak izi çıkarma işlemi sırasında genellikle bir dokümanın içeriği bütün olarak ele alınır ve bu yaklaşım bazı durumlarda standart içeriğe sahip fakat gizli olmayan dokümanlar için yanlış alarma sebep olabilir. Bu iki problemin üstesinden gelmek için k-atlama-n-gram (Shapira vd., 2013) ve bulanık parmak izi oluşturma (Shu vd., 2015) gibi genişletilmiş teknikler üzerine çalışmaların yapıldığı görülmektedir.

4.2.2.2. Çoklu anahtar kelime eşleme

Bu yaklaşımda, hassas nitelikli/gizli bir dokümanda bulunan karakter katarlarından seçilerek bir hassas kelime listesi oluşturulur. Bu listeler oluşturulurken makine öğrenmesi algoritmaları (V. Gupta, 2013) veya Terim Frekansı – Ters Metin Frekansı (TF/IDF- Term Frequency/Inverse Document Frequency) (Canbay vd., 2017) gibi yöntemlerin kullanıldığı görülmüştür. Gizli dokümanlardan elde edilen bu anahtar kelimeler bir araya toplanarak tek bir veri tabanında saklanmak suretiyle büyük bir sözlük oluşturulur (V. Gupta, 2013). Daha sonra, veri sızıntısı olup olmadığını tespit edebilmek için ağda hareket eden paketlerin analizi sırasında sözlükteki kelimelerin Naive String Match, Knuth- Morris- Pratt, Boyer- Moore (Canbay vd., 2017), Boyer-Moore-Horspool, Boyer-Moore-Horspool-Raita, Rabin Karp, Aho-Corasick, Sun-Manber gibi tekli veya çoklu desen eşleştirme algoritmaları ile paket içerisinde bulunma durumuna bakılmaktadır (Ren, 2013).

4.2.2.3. Tam dosya eşleme

Bu yöntemde video, resim gibi medya dosyaları veya proje ve çizim gibi özel formattaki dosyaların özetleri (hash) çıkarılır, karşılaştırma sırasında ise üretilen özet değeriyle tam eşleşen bir değerin olması beklenir. Bu yaklaşımda bir dosyadaki hassas verilerin kelimesi kelimesine analizinden ziyade dosyanın bir bütün olarak özeti çıkarılır bu açıdan parmak izi oluşturma yaklaşımından farklıdır (Mogull ve Securosis, 2007; Securosis, 2010). Bu yaklaşım her dosya tipine uygulanabilir fakat içerikte yapılan ufak bir değişiklik tüm dosyanın özet değerini değiştireceğinden yeterince etkili bir çözüm sunamaz.

4.2.2.4. Kısmi doküman eşleme

Bu yaklaşımda, korunan içeriğin tam veya kısmi eşleşmesi denetlenir (Pesen, 2015; Securosis, 2010). Önceden belirlenen politikalar doğrultusunda hassas veya gizli içeriğe sahip dokümanın ya tüm içeriği ya da cümle bazlı olarak özeti alınır. Bu yöntemle içeriğin tamamının veya bir kısmının anlık mesajlaşma, forum siteleri, sosyal ağlardaki formlardan herhangi birine kopyalanıp yapıştırılması tespit edilebilmektedir. Bunu yaparken kullanılan en yaygın özet çıkarma şekli

dairesel özetleme metodudur, bu yöntemde önceden belirlenmiş sayıda karakter seçilip özeti alınır ve bu şekilde devam ederek tüm belgenin özeti alınmış olur (Securosis, 2010). Dışarı giden içeriğe de aynı yöntem uygulanarak bulunan özet değerleri karşılaştırılır. Yapılandırılmamış hassas veriler üzerinde, kaynak kodlarda koruma sağlayabilen bir yaklaşımdır. Bu yöntem fazla miktarda içerik olması durumunda düşük performans göstermektedir ayrıca ortak sözcükler ve standart kalıplar bu yöntemin yanlış alarmları üretmesini tetiklemektedir (Pesen, 2015).

4.2.2.5. Düzenli ifade eşleme

Düzenli ifadeler 1951 yılında Kleene (Kleene, 1951) tarafından tanıtılmıştır ve veri sızıntısı önleme sistemlerinde en yaygın kullanılan analiz tekniklerinden bir diğeridir (Alneyadi vd., 2016). Sadece endüstriyel DLP sistemlerinde değil DLP özelliği gösteren tüm araçlarda kullanılan bir tekniktir ve hassas/gizli içeriği belli kurallar dahilinde analiz eder (Securosis, 2010). Literatürde desen eşleştirme veya kural tabanlı eşleştirme (Al-Sanabani, 2016; Alneyadi vd., 2015; K. Gupta ve Kush, 2017; Securosis, 2010; Shabtai vd., 2012) olarak da adlandırılan bu yöntem ile sosyal güvenlik numarası, kredi kartı numarası, TC kimlik numarası, vergi numarası, banka hesap numarası gibi hassas/gizli kurumsal veya kişisel kayıtların tam veya kısmi tespitinde kullanılır (Securosis, 2010). Düzenli ifadelerle analiz yapılırken hassas veya gizli nitelikli ifadelerin tespiti için birtakım desenler kullanılır bu desenler; terim, gerçek anlam ifade eden karakterler veya özel anlam ifade eden (. | * $? +) gibi meta karakterlerden oluşur. Bu yaklaşım kolayca tanımlanmış yapılandırılmış veri parçalarının tespitinde oldukça etkili olmasına rağmen yapılandırılmamış verilerin tespitinde yetersizdir ve yanlış alarm üretir (Hauer, 2015; Securosis, 2010). Bu yöntemin bir diğer özelliği ise bir doküman içeriğinin anlamsal ifadesinden çok şekilsel gösterimi üzerine analiz yapmasıdır. Bu bazı durumlarda sızıntı tespiti için yeterli iken bazı durumlarda yetersiz bir çözümdür.

4.2.2.6. İstatiksel analiz

Bu yöntem bir içeriğin yapısını analiz etmek ve korunan içeriğe benzeyen içeriklerde politikaları ihlal eden kısımları bulmak için makine öğrenmesi, Bayes analizi ve diğer istatistiki yöntemleri kullanmaktadır (Pesen, 2015; Securosis, 2010). İstatistiksel analiz sırasında kullanılan bu teknikler karışık veya belirsiz tipteki veriler üzerinde de etkilidir. Ayrıca bu yöntem kısmi dokuman eşleme yönteminden farklı olarak yapılandırılmamış içeriklerin tespitinde de oldukça başarılıdır. N- gram ve bir dokümanda geçen kelimelerin önemini belirten terim ağırlığı bulma teknikleri (örneğin TF-IDF) temel istatistiksel analiz teknikleridir (Alneyadi vd., 2016). N-gram analiz yöntemi makine öğrenmesi algoritmaları ile birlikte dokümanların hassas veya hassas olmayan şeklinde sınıflandırılmasında DLP sistemlerinde yaygın olarak kullanılır (Alneyadi vd., 2016). İstatistiksel analiz yöntemlerinin en belirgin avantajı yapılandırılmamış veriler üzerinde içerikleri hassas ve hassas olmayan şeklinde sınıflandırabiliyor olmasıdır. Bunun yanında bu sınıflandırmanın en doğru şekilde yapılabilmesi algoritmanın öğrenmesine bağlıdır bu da algoritmanın büyük miktarlarda veriye ihtiyacı olduğu anlamına gelmektedir bu sebeple bu yöntem yanlış pozitif veya yanlış negatif sonuçlar vermeye eğilimlidir (Securosis, 2010).

4.2.3. İçerik Etiketleme

Bu yaklaşımda, hassas veri içeren bir dosyaya içerdiği verinin çok gizli, gizli, özel gibi gizlilik seviyesine göre bir etiket atanır ve atanan etikete dayalı bir politika uygulanır. İçerik diğer uygulamalar tarafından işlendiğinde bile etiketlenmeye devam edecektir (Al-Sanabani, 2016; Shabtai vd., 2012; Shapira vd., 2013). Etiketler farklı yollar kullanılarak atanabilir örneğin; manuel olarak hassas verinin yaratıcısı tarafından, otomatik olarak içerik veya bağlam tabanlı analiz yöntemleri kullanılarak, otomatik olarak belirli bir yerde tutulan tüm dosyalara ve son olarak özel bir uygulama ya da kullanıcı tarafından oluşturulan dosyaların tümüne uygulanabilir. Geleneksel içerik etiketleme çözümleri, hedef iş istasyonunu veya sunucuyu tarayan, veri dağıtım politikasını

ihlal eden depolanmış verileri algılayan aracılar kullanır ve sonrasında da gerekli işlemleri yapar (Matthee, 2016).

4.3. Veri Sızıntısı Önleme Yöntemleri

Bu yaklaşımlar uygun teknik ve yöntemler kullanılarak veri sızıntısı olayları meydana gelmeden önce önlenmesi için kullanılan proaktif yaklaşımlardır. İncelenen makalelerde (Al-Sanabani, 2016; Alneyadi vd., 2016; Shabtai vd., 2012) önleyici yaklaşımlar için dört temel yöntem olduğu görülmüştür. Bunlar erişim kontrolü, şifreleme, devre dışı bırakma ve farkındalık olarak söylenebilir.

4.3.1. Erişim Kontrolü

Erişim kontrolü, bir kullanıcı tarafından belirli bir kaynağın kullanımına izin verme veya reddetme olarak söylenebilir. Bu bağlamda erişim kontrolü, hassas verilere kimin veya kimlerin erişebileceğine dair kuralların belirlenmesi ve uygulanması hususundaki süreçleri kapsamaktadır. Organizasyon tarafından tanımlanan politikaya göre, bir kullanıcının veya çalışanın hassas bilgilere erişim izni yoksa, DLP bu bilgilerin kullanımını kısıtlar, aksi halde erişim kabul edilir. Erişim kontrolü sağlamanın bir yolu, erişim denetimini belgelere otomatik olarak uygulamak için kurumsal dijital haklar yönetimi (EDRM-Enterprise Digital Rights Management) ile entegrasyondur (Shabtai vd., 2012).

4.3.2. Şifreleme

Durumu ve niteliği göz önüne alınarak hangi hassas verinin şifrelenmesi gerektiği ve şifrelenmiş bu hassas verilerin şifresini çözme hususunda kimlerin yetkili olabileceğine dair ilkelerin belirlendiği bir yaklaşımdır. Bu yaklaşımda DLP sistemleri, hassas verilerin yalnızca onaylı kurumsal uygulamalarla şifrelemeye ve şifresinin çözülmesine izin vererek hassas verilerin güvenliğini garantilemeyi amaçlamaktadır.

4.3.3. Devre Dışı Bırakma

Bu yaklaşım hassas verilerin sızmasına neden olabileceği düşünülen işlevleri devre dışı bırakmayı içeren önleyici bir yaklaşımdır. Örneğin, hassas içeriğe kopyalama ve yapıştırma işlemlerinin kısıtlanması, içeriğin taşınabilir depolama birimine kaydedilmesi veya ekran görüntüsünü alma işlevlerinin devre dışı bırakılması gibi önlemlerdir.

4.3.4. Farkındalık

Farkındalık, kullanıcıları ve çalışanları hangi verinin hassas/gizli nitelikte olduğu, kimin neye erişiminin olduğu ve bunu korumak için ne yapılması gerektiğine dair bilgilendiren bir süreçtir (Al-Sanabani, 2016; Shabtai vd., 2012). Bunun için çalışanlara ve kullanıcılara birtakım eğitimler verilerek onların farkındalıklarını artırmak amaçlanmaktadır çünkü güvenlik sistemlerinde her ne kadar en son teknolojiyi kullanarak önlemler alınsa da en zayıf halka olan insan faktörü asla göz ardı edilmemelidir. Çalışanlar organizasyonun güvenlik politikaları hakkında sürekli olarak bilgilendirilmeli ve bu ilkelere uyulması için gereken çalışmalar yapılmalıdır.

5. AĞ TABANLI VERİ SIZINTISI TESPİTİ VE ÖNLENMESİ

Veri sızıntısı olaylarının büyük bir kısmı ağ üzerinden gerçekleşmektedir. Bu sebeple ağ tabanlı DLP sistemleri geliştirilmiştir. Bu sistemler hareket halindeki veriler için koruma sağlamayı hedeflemektedir. Bunu yaparken DLP merkezi sunucusunda bulunan organizasyon tarafından önceden belirlenmiş politikaları ihlal eden içeriğin olup olmadığına bakılır.

Bilgi güvenliğinin sağlanabilmesi hususunda gerekli gizlilik, bütünlük ve erişilebilirlik kriterlerinin korunması kurumsal ağın çıkış noktasına kurumun ihtiyaçlarına uygun olacak şekilde tasarlanmış bir DLP sisteminin konumlandırılması ile mümkündür. Söz konusu DLP sistemleri organizasyonlarda yürütülen işin ve uygulamanın erişilebilirliğini garanti altına alabilmeli ve bunun için HTTP, FTP, IM, Telnet, TCP/IP, SMTP, POP3, IMAP gibi güncel protokoller üzerinden gönderilen paketlerin yalnızca başlık değil ayrıca derin paket analiziyle paketin payload kısımlarına da bakarak olası veri sızıntılarını tespit edebilmelidir (Oğuz ve Cevahir, 2010). Bu makale kapsamında detaylı bir şekilde incelenen bağlam tabanlı, içerik tabanlı ve içerik etiketleme olarak üç temel başlıkta sınıflandırılan veri sızıntısı tespit yöntemleri bugün endüstriyel amaçlı geliştirilen DLP çözümlerinde derin paket analizi sırasında kullanılan yaklaşımlardır. Email, webmail, HTTP/FTP, HTTPS, IM/Messaging, TCP/IP, P2P (Peer-to-Peer) izlenme ve uyarma gerektiren network kanalları olarak söylenebilir (Oğuz ve Cevahir, 2010). Bu açıdan bakıldığında bir organizasyonun dış ağa çıkmadan önce DLP sistemlerinin konumlandırılması Şekil 2'deki gibidir.

Şekil 2. Kurum dış ağı DLP pasif izleme mimarisi (Securosis, 2010).

Bunun yanı sıra e-posta için organizasyon ağında pasif izleme mimarisinden farklı olarak posta sunucusu ile aktarım temsilcisi (mail transfer agent) arasına DLP sistemi yerleştirilmektedir (Securosis, 2010). Ağlarda veri sızıntısı tespiti için endüstriyel DLP çözümleri pasif izleme dışında bloklama/filtreleme için 3 farklı şekilde kullanılabilmektedir. Bunlar; köprü (bridge), tcp reset ve vekil sunucu (proxy) olarak belirtilebilir. Köprü görevi yapan DLP sistemi iki farklı ağ arasına konumlandırılarak ortada derin içerik analizi yapar. Bu yöntemde DLP merkez sunucusunda önceden belirlenmiş politikayı ihlal eden bir içeriğin tespit edilmesi durumunda oturum sonlandırılarak bağlantı kesilir. İkinci yöntem olarak ise trafik izleme sırasında veri sızıntısı tespit edildiğinde ağa TCP reset paketi enjekte edilerek bağlantı sonlandırılır ve hassas nitelikli verilerin kurum dışına çıkması engellenmiş olur. Üçüncü ve en önemlisi kendisine ait vekil sunucusu bulunan DLP sistemleridir. Bu durumda ağ trafiği önce Proxy tarafından yakalanıp analiz için ilgili DLP ürününe gönderilir burada derin paket analizleri gerçekleştirilir. Bu yöntemle paket analizleri çok daha sağlıklı yapılabilmektedir. Ayrıca bu yaklaşımın en büyük avantajı günümüzde yaygın olarak kullanılmaya başlanan akan trafiğin şifreli iletilmesini sağlayan SSL/TLS gibi protokollerle sarmalanmış şifreli paketlerin analizinin yapılabiliyor olmasıdır. "Reverse SSL/TLS" özelliğine sahip bir DLP vekil sunucusu yakaladığı şifreli paketleri deşifre edebilme yetkisine sahiptir bu sayede şifreli akan trafikte bile veri sızıntısı tespiti yapılabilmektedir (Farrell, 2017; Securosis, 2010).

6. VERİ SIZINTISI TESPİTİ VE ÖNLENMESİNDE KARŞILAŞILAN ZORLUKLAR

Günümüzde bilgi güvenliğinin sağlanması adına farklı sistemler organizasyonlar tarafından kullanılmaktadır. Ne var ki artan teknoloji kullanımı beraberinde birçok güvenlik açığını da getirmektedir. Bunlardan en önemlisi de veri sızıntısı problemidir. Veri sızıntılarının tespitinde ve

engellenmesinde oldukça etkili olmasına rağmen DLP sistemleri, diğer güvenlik mekanizmalarında olduğu gibi farklı birçok zorlukla karşı karşıya kalmaktadır. İncelenen makalelerde (Alneyadi vd., 2016; K. Gupta ve Kush, 2017; Kaur vd., 2017) karşılaşılan zorluklar şifreleme, erişim kontrolü, uyarlama/güncelleme ve insan faktörü olarak dört ana başlık altında toplanabilir.

Şifreleme veri güvenliğini sağlamak için yaygın olarak kullanılan bir yaklaşımdır ve özellikle ağ tabanlı DLP sistemlerinde en temel zorluklardan birisi olarak söylenebilir. Bu sistemler ağ üzerinden akan trafiği çeşitli analiz yöntemleri ile paket içerikleriyle orijinal verileri karşılaştırarak veri sızıntılarını tespit etmeye çalışır fakat güçlü şifreleme algoritmalarıyla şifrelenmiş içeriklerin analiz edilmesi, organizasyon dışına ağ yoluyla çıkarılmaya çalışılan içeriğin hassas olup olmadığının sınıflandırılması oldukça zor olmaktadır (Alneyadi vd., 2016).

Bilgi güvenliği alanında, erişim kontrolü, bir sisteme, fiziksel veya sanal kaynaklara erişimi sınırlandırmanın bir yoludur (Kaur vd., 2017). Bir organizasyondaki kullanıcıların veya çalışanların hangi veriye erişebileceğinin öncelik ve izinlerinin önceden belirlenmesi önemlidir. Bu erişim izinlerinin doğru ve net bir şekilde tanımlanmaması durumunda DLP sistemleri erişilen verinin meşru bir kullanıcı tarafından mı yoksa izinsiz bir kullanıcı tarafından mı erişildiğine karar verememektedir (Alneyadi vd., 2016). Bazı DLP sistemleri erişim izin kontrolünü sağlamak için Microsoft tarafından sağlanan bir dizin hizmeti olan Active Directory sistemleri tarafından sağlanan erişim listelerini kullanırlar (Mogull ve Securosis, 2007). Erişim izin listelerinin güncel olması konusu işten ayrılan veya görevi değişen çalışanların veri sızıntılarına sebep olabilme riski açısından DLP sistemleri için önemli bir konudur. Erişim izinleri kontrolü veri sızıntılarının önlenmesinde önemli bir rol oynamaktadır bu bağlamda DLP sistemleri, verileri kazara veya kasti sızıntılardan korurken erişim izinleri dahilinde çalışmasını sürdürebilmelidir.

Kurumlar tarafından işlenen verilere yenileri eklenmekte bazıları ise artık işlenmemektedir yani veriler sürekli bir değişim içindedir, sabit değildir. Bu veriler içinde hassas nitelikli olanların kurum dışına izinsiz çıkarılmaması için DLP sistemleri ile sızıntılar denetim altına alınmaya çalışılmaktadır. Özellikle düzenli ifadeler, veri imzası veya parmak izi oluşturma gibi yöntemlerle incelenen trafik ile orijinal gizli veriyi karşılaştırarak sızıntı tespit etmeye çalışan DLP sistemlerinde politikaların güncel olması büyük önem teşkil etmektedir. Var olan veriler üzerinde yapılan değişiklikler veya yeni verilerin eklenmesi DLP sistemlerinde önceden belirlenmiş kuralların bu değişimlere uyarlanarak güncel tutulması gerekliliğini ortaya çıkarmaktadır. Örneğin, parmak izi çıkarılmış bir veri tabanında bulunan hassas veriler üzerinde değişiklik yapılmış olsun, bu durumda daha önceden üretilen parmak izi ile veri tabanının son durumdaki parmak izi birbiriyle uyuşmayacaktır. Böyle durumlarda DLP sisteminde belirlenen kuralların değiştirilmemesi, anılan veriler trafik üzerinde akarken onların tespit edilememesi anlamına gelir. Sonuç itibariyle veri sızıntısı tespiti ve önlenmesinde DLP sistemlerinin sürekli güncellenmesi ve yeniliklere uyum sağlayabilmesi karşımıza çıkan zorluklardan bir diğeridir.

Son olarak veri sızıntısı tespiti ve önlenmesinde karşılaşılan zorluklardan en önemli ve kontrol edilmesi en güç olanı insan faktörüdür. Birçok psikolojik ve sosyal faktörlerden etkilendiği için insan davranışlarının tahmin edilmesi her zaman zor olmuştur (Alneyadi vd., 2016). Veri sızıntısı tespiti ve önlenmesinde özellikle verilerin gizlilik düzeyini tanımlama, belirli kullanıcılara erişim hakları atama ve bir DLP sisteminin algılama eşiğini kalibre etme gibi karar verme durumlarında insan eylemi gerekmektedir. Bu noktada insanların doğası gereği objektiflikten uzaklaşıp yanlış kararlar vermesi kaçınılmaz bir gerçektir. Bunun yanı sıra organizasyonlar tarafından belirlenen güvenlik politikaları ne kadar katı olursa olsun, çalışanların bu kurallara tam olarak uyacağı hiçbir zaman garanti değildir. Örneğin, gizli verilere erişim yetkisi olmayan bir çalışan yetkili bir çalışanın erişim bilgilerini izinli veya izinsiz bir şekilde kullanarak kuralları ihlal edebilmektedir ve bunun gibi birçok örnek daha verilebilir. Bu bağlamda, insan faktörü olduğu sürece DLP ve diğer güvenlik sistemlerinde her zaman zorluklar olmaya devam edecektir.

7. TARTIŞMA VE SONUÇ

Bu makale çalışmasında, ağ tabanlı veri sızıntılarının tespiti ve önlenmesinde kullanılan yöntemlerin incelenmesi kapsamında veri sızıntısı tespiti hakkında bir literatür taraması yapılmış, veri sızıntısı tespitinde kullanılan yöntemler araştırılmış ve yapılan çalışmalar gözden geçirilmiştir.

Çalışmamız için gerçekleştirdiğimiz literatür incelemesi sonucunda veri sızıntısı tespiti ve önlenmesi konusunda benzerlik ve farklılıklarının görülebilmesi amacıyla çalışmalar (Trieu vd., 2017; Alneyadi vd., 2015; Shu vd., 2016; Canbay vd., 2017; Soumya ve Smitha, 2014; Katz vd., 2014; Huang vd., 2018; Liu vd., 2009; Gugelmann vd., 2015; Hemalatha vd., 2016; Shu vd., 2015; Breitinger ve Baggili, 2014; Shapira vd., 2013) kullanılan yöntem, analiz tekniği, incelenen verinin durumu ve tasarlanan sistemin performansının test edilmesinde kullanılan ölçütler şeklinde kategorize edilmiştir. Tablo 1'de görüleceği üzere veri sızıntısı tespitinde bağlam tabanlı, içerik tabanlı ve içerik etiketleme analiz tekniklerinin kullanıldığı görülmüştür. İncelenen araştırmalar, verilerin en çok ağ kanalıyla sızdırıldığını göstermektedir, bu sebeple literatürde özellikle hareket halindeki verilerin incelenmesi çalışmaların en belirgin benzerliklerinden biri olarak tespit edilmiştir. Yapılan çalışmalarda özellikle veri sızıntısı tespitine odaklanıldığı ve bunun için içerik tabanlı yöntemlerin yaygın olarak tercih edildiği saptanan benzerliklerden bir diğeridir. Bununla birlikte çalışmalarda veri sızıntısı tespitinde yüksek oranda doğru sonuçlar elde edilebilen ve daha iyi biçimsel ve anlamsal analiz yapılabildiği için içerik tabanlı analiz tekniklerinden biri olan istatistiksel analizin tercih edildiği görülmüştür. Bazı çalışmalarda ise belirsiz veri desenine sahip hassas veriler veya veriler üzerindeki modifikasyon ataklarına karşı istatistiksel analizle beraber anahtar kelime eşleme yönteminin kullanıldığı saptanmıştır. Özellikle kasti veri sızıntısı vakalarında ise tespit yapabilmek amacıyla istatistiksel analizin yanında parmak izi eşleme yönteminin tercih edildiği görülmüştür. Veri sızıntısı tespiti ve önlenmesi konusuna yeni bir yaklaşım sunmayı amaçlayan çalışmaların ise analiz tekniği olarak bağlam tabanlı yöntemi tercih etmesi ise en belirgin farklılık olarak karşımıza çıkmaktadır. Ayrıca bağlam tabanlı analizi kullanan çalışmalarda gizli olmayan bir dokümandaki gizli bilginin tespit edilebilmesi de bu çalışmaların diğer bir amacı olarak saptanmıştır.

Veri sızıntılarının önüne geçmek için kullanılan erişim kontrolü, şifreleme, devre dışı bırakma ve farkındalık gibi yaklaşımlar ise literatürde (Al-Sanabani, 2016; Alneyadi vd., 2016; Shabtai vd., 2012) bahsi geçen önleme yöntemleri olarak görülmektedir. Çalışmamız kapsamında incelenen makalelerde veri sızıntısının hem tespiti hem de önlenmesine odaklanan çalışmaların analiz tekniği olarak yine içerik tabanlı yaklaşımı kullandığı görülmüştür. İncelenen çalışmalarda geliştirilen sistemlerin performanslarının test edilmesi konusunda veri sızıntısı tespitinde kullanılan analiz tekniğine uygun olacak şekilde farklı birçok ölçütün kullanıldığı tespit edilmiştir.

Yaptığımız bu çalışmanın hedefi güçlü bir bilgi güvenliği sisteminde bulunması gereken DLP sistemini her yönüyle ele almaya çalışarak bu alanda yapılacak olan çalışmalara ışık tutabilmektir. Günümüz teknolojisi her ne kadar gelişmiş ve güçlü güvenlik sistemleri için katkı sağlıyor olsa da tek başına DLP sistemlerinin yeterli olamayacağı ve DLP sistemleri için hala var olan bir takım engel ve zorlukların olduğu görülmektedir. Özellikle bilgi güvenliğinde en zayıf halka olan insan faktörüne karşı bu sistemlerin de yetersiz kaldığı ortaya çıkmıştır. Yine de uygulanacak protokollerin ve güvenlik sistemlerinin doğru bir şekilde planlanması özellikle kurumsal bilgi güvenliği konusunda riskleri en aza indirmeyi sağlamaktadır. Bununla birlikte çalışanların veri güvenliği konusunda bilgi sahibi olması, bilinç ve farkındalık seviyelerinin verilecek eğitimlerle artırılması ile planlı ve rastgele denetimlere tabi tutulup bilgilerinin ölçülmesi diğer önemli bir faktördür ve yaptığımız çalışmanın buna katkı sağlayacağı değerlendirilmektedir.

Son olarak yaptığımız bu çalışmada veri sızıntısı tespit sistemlerinde kullanılan analiz tekniklerinin verinin durumuna, tipine göre değişkenlik gösterdiği tespit edilmiştir. Sadece bir tekniği kullanan bir sistemin tüm veri sızıntılarının tespitinde yetersiz kaldığı görülmüştür. Bu sebeple gelecekte bu alanda yapılabilecek çalışmalar; birden fazla tespit yönteminin entegre edildiği

veri sızıntısı tespit sistemlerinin geliştirilmesine odaklanmalıdır. Ayrıca odaklanılması gereken bir diğer konu ise verilerin aynı kalmayıp sürekli değişime uğramasıdır. Bu durum DLP sistemlerinde tanımlanan protokollerin sürekli değiştirilip güncellenmesine sebep olmaktadır. Bu konuda bağlam tabanlı, içerik tabanlı ve içerik etiketleme yaklaşımlarında yapılan biçimsel analize ek olarak verileri anlamsal bazda inceleyecek ve sürekli kendi kendini güncel tutabilecek bir yaklaşımın geliştirilmesine ihtiyaç vardır. Böyle bir yaklaşımın geliştirilmesinde makine öğrenmesi ve derin öğrenme algoritmalarının DLP sistemleriyle beraber kullanılmasının yüksek oranda başarı sağlayabileceği öngörülmektedir. Bu kapsamda yapılacak yenilikçi çalışmalar DLP sistemlerinin güvenlik kapasitelerinin gelişmesinde önemli katkı sağlayacaktır.

KAYNAKÇA

Al-Sanabani, H. (2016). *Eklentiler Kullanarak Veri Kaybını Engelleme.* (Yüksek Lisans Tezi), Sakarya Üniversitesi, YÖK Ulusal Tez Merkezi.

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2015). *Detecting data semantic: a data leakage prevention approach.* Paper presented at the Trustcom/BigDataSE/ISPA, 2015 IEEE.

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. *Journal of Network and Computer Applications, 62*, 137-152.

Başak, C. D. (2016). Veri Sınıflandırılması ve Hassas Verinin Sızdırılması. Retrieved from https://www.platinbilisim.com.tr/TR/Medya/SiberBulten/siber-bulten-agustos-2016

Breitinger, F., & Baggili, I. (2014). File detection on network traffic using approximate matching.

Canbay, Y., & Sağıroğlu, Ş. (2016). Veri Kaçağı Tespitinde Yeni Bir Yaklaşım. *Savunma Bilimleri Dergisi, 15*(1), 149-177. doi:2148-1776

Canbay, Y., Yazici, H., & Sagiroglu, S. (2017). *A Turkish language based data leakage prevention system.* Paper presented at the Digital Forensic and Security (ISDFS), 2017 5th International Symposium on.

Cost of a Data Breach Study: Global Overview. (2018). Retrieved from https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

Farrell, C. (2017). *Looking Under the Rock: Deployment Strategies for TLS Decryption.* (Master), The SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/dlp/paper/38240

Global Data Leak Report 2017. Retrieved from https://infowatch.com/report2017

Gugelmann, D., Studerus, P., Lenders, V., & Ager, B. (2015). Can content-based data loss prevention solutions prevent data leakage in Web traffic? *IEEE Security & Privacy, 13*(4), 52-59.

Gupta, K., & Kush, A. (2017). A Review on Data Leakage Detection for Secure Communication. *International Journal of Engineering and Advanced Technology (IJEAT), 7*(1).

Gupta, V. (2013). *File detection in network traffic using approximate matching.* Institutt for telematikk.

Hauer, B. (2015). Data and information leakage prevention within the scope of information security. *IEEE Access, 3*, 2554-2565.

Hemalatha.N.C, Somasundaram.R, & Thirugnanam, M. (2016). Privacy Preserving Data Leak Detection in Large Scale Organizations. *International Journal of Future Innovative Science and Engineering Research (IJFISER), 2*(2). doi:2454- 1966

Huang, X., Lu, Y., Li, D., & Ma, M. (2018). A novel mechanism for fast detection of transformed data leakage. *IEEE Access, 6*, 35926-35936.

Katz, G., Elovici, Y., & Shapira, B. (2014). CoBAn: A context based model for data leakage prevention. *Information Sciences, 262*, 137-158.

Kaur, K., Gupta, I., & Singh, A. K. (2017). *A Comparative Evaluation of Data Leakage/Loss prevention Systems (DLPS).* Paper presented at the Proc. 4th Int. Conf. Computer Science & Information Technology (CS & IT-CSCP), Dubai, UAE.

Kleene, S. C. (1951). *Representation of events in nerve nets and finite automata*. Retrieved from

Liu, Y., Corbett, C., Chiang, K., Archibald, R., Mukherjee, B., & Ghosal, D. (2009). *SIDD: A framework for detecting sensitive data exfiltration by an insider attack.* Paper presented at the 2009 42nd Hawaii International Conference on System Sciences.

Matthee, M. H. (2016). *Tagging Data to Prevent Data Leakage (Forming Content Repositories)*. Retrieved from SANS Institute InfoSec Reading Room:

Mogull, R., & Securosis, L. (2007). Understanding and selecting a data loss prevention solution. *Technicalreport, SANS Institute*, 27.

Oğuz, B., & Cevahir, H. K. (2010). BT Yönetiminde Bilgi Sızıntısı ve Ağ Tabanlı Çoklu Protokol Bilgi Sızıntısı Engelleme.

Pesen, M. M. (2015). DLP'de İçerik Analizi Yöntemleri. Retrieved from https://www.sibergah.com/veri-guvenligi/veri-sizintisi-onleme/dlp-de-icerik-analizi-yontemleri/

Ren, L. (2013). DLP Systems: Models, Architecture and Algorithms. Retrieved from https://www.researchgate.net/publication/304080339_DLP_Systems_Models_Architecture_and_Algorithms

Securosis, L. (2010). Understanding and Selecting a Data Loss Prevention Solution. *Securosis, LLC,[Online]. Available: https://securosis. com/assets/library/reports/DLP-Whitepaper. pdf*.

Shabtai, A., Elovici, Y., & Rokach, L. (2012). *A Survey of Data Leakage Detection and Prevention Solutions*. In P. N. Stan Zdonik, Shashi Shekhar (Series Ed.) (pp. 92). doi:10.1007/978-1-4614-2053-8

Shapira, Y., Shapira, B., & Shabtai, A. (2013). Content-based data leakage detection using extended fingerprinting. *arXiv preprint arXiv:1302.2028*.

Shu, X., Yao, D., & Bertino, E. (2015). Privacy-preserving detection of sensitive data exposure. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 10*(5), 1092-1103.

Shu, X., Zhang, J., Yao, D. D., & Feng, W.-C. (2016). Fast detection of transformed data leaks.

Soumya, S. R., & Smitha, E. S. (2014). Data Leakage Prevention System By Context Based Keyword Matching And Encrypted Data Detection. *International Journal of Advanced Research in Computer Science Engineering and Information Technology, 3*(1), 375-384.

T.C. Resmi Gazete, Kişisel Verilerin Korunması Kanunu, 6698 C.F.R. (7 Nisan 2016).

Tahboub, R., & Saleh, Y. (2014). *Data leakage/loss prevention systems (DLP).* Paper presented at the Computer Applications and Information Systems (WCCAIS), 2014 World Congress on.

Trieu, L. Q., Tran, T.-N., Tran, M.-K., & Tran, M.-T. (2017). *Document Sensitivity Classification for Data Leakage Prevention with Twitter-Based Document Embedding and Query Expansion.* Paper presented at the 2017 13th International Conference on Computational Intelligence and Security (CIS).

GOOGLE TRENDS KUDUZ TARAMA VERİLERİ İLE KUDUZ HASTALIĞI MİHRAK VE FREKANS VERİLERİ ARASINDAKİ İLİŞKİNİN ANALİZİ

***

ANALYSIS OF THE RELATIONSHIP BETWEEN RABIES GOOGLE TRENDS DATA AND RABIES OUTBREAK AND FREQUENCY DATA

DOI: 10.33461/uybisbbd.633414

Berrin ŞENTÜRK*

Öz

Bu çalışmada "Kuduz" anahtar kelimesi kullanılarak, 01.01.2005-30.06.2019 tarihleri arasındaki Google Trends internet tarama verileri ile aynı dönem Uluslararası Salgın Hastalıklar Ofisi Kuduz mihrak verileri kullanılarak il düzeyinde mihrak sayıları, hastalığın yıllar itibariyle görülme sıklığı ve Google Trends verilerinde alt bölge olarak bildirilen iller arasındaki ilişki araştırılmıştır. Çalışmada bölgelerin belirlenmesinde frekans dağılımı içinde en çok yer alan il sayıları dikkate alınmıştır. Oran analizi yöntemi ile yapılan değerlendirmelerde; mihrak sayısı, frekans dağılımı ve alt bölge için büyükten küçüğe doğru yapılan sıralama ile ilk 25, 15 ve 10 il değerlendirilmiştir. Google Trends verilerinde aramaların %52 oranında (13/25 İl), %66,6 (9/15 İl) ve %80 (8/10 İl) oranında hastalığın frekans dağılımında en çok sayıda yer alan illerin bulunduğu bölgelerde gerçekleştiği tespit edilmiştir. Elde edilen çalışma bulguları Google Trends veri sıralamasının hastalık koruma ve kontrolünde kullanımının önemini ortaya koymuştur.

***Anahtar Kelimeler**: Google eğilimleri, Kuduz, Mihrak.*

Abstract

In this study, using "rabies" keyword, 2005-2019 Google Trends internet search data and the same period International Office of Epidemic Diseases using outbreak rabies data, provincial outbreak numbers, incidence of disease by years and Google Trends data as a sub-region It was investigated. In the study, the number of provinces in the frequency distribution was taken into consideration in determining the regions. In the evaluations made by ratio analysis method; outbreak, frequency distribution and ranking from top to bottom in the lower region, the first 25, 15 and 10 provinces were evaluated. According to Google Trends data, 52% (13/25 Provinces), 66,6% (9/15 Provinces), and 80% (8/10 Provinces) searches took place in regions with the highest number of provinces in the frequency distribution of the disease. The findings of the study revealed the importance of using Google Trends data ranking in disease prevention and control.

***Keywords:** Google Trends, Rabies, Outbreak.*

*Doç. Dr. Samsun, Ondokuz Mayıs üniversitesi, Veteriner Fakültesi, Hayvancılık Ekonomisi ve İşletmeciliği Anabilim Dalı, bsenturk@omu.edu.tr
ORCID: 0000-0002-0455-9341

Geliş Tarihi / Received: 15.10.2019
Kabul Tarihi / Accepted: 25.12.2019

1. GİRİŞ

Kuduz hastalığı ölümle sonuçlanan yüksek maliyetli bir hastalıktır (Shwiff vd., 2018). Hastalık büyükbaş hayvanlar içinde önemli bir endişe kaynağıdır(Jemberu vd., 2013). Diğer yandan kuduz insanlar içinde günümüzde hala tehdit oluşturan hastalıklar arasında yer almaktadır (Hampson vd., 2015; Wallace et al., 2016). Kuduz hastalığı oluşturduğu doğrudan ve dolaylı etkilerle yerel ve ulusal ekonomiler için önemli ekonomik kayıp kaynağı olmaya devam etmektedir (Regea, 2017). Dünyada olduğu gibi Türkiye'de de kuduz hastalığı popülerliğini yitirmeyen hastalıklar arasında yer almaktadır. Bu nedenle günümüz dünyasının önemli veri kaynağı olan internet bu konunun araştırılmasında yarattığı olanaklarla yakın gelecekte giderek artan bir öneme sahip olacaktır. İnternet kaynaklı bilginin en önemli özellikleri büyük miktarda bilgi içermesi ve bu bilginin akışının zamanında olmasıdır. İnternet kaynaklı bilgi kullanımı konusunda hayvancılık sektörü ile doğrudan ilişkili tüketici davranışlarının web tabanlı yaklaşımlarla tahmini (Goel vd., 2010), Google Trends'le Influenza (Dugas vd., 2013) ve arama motorları kullanılarak Dang Hummasının insidensinin tespiti (Althous vd., 2011)uluslararası düzeyde yapılan çalışmaların yanı sıra Türkiye'de yapılmış tüketicilerin harcama niyetlerinin öngörülebilir olup olmadığını ve sağlık hizmetleri alanında Google arama trendlerinin araştırıldığı çalışmalar da mevcuttur (Zeybek ve ark., 2018; Yıldız, 2018).

Bu çalışmada il düzeyinde hastalık mihrak verileri, hastalığın yıllar itibariyle görülme sıklığı verileri ve Google Trends kuduz arama terimi ile elde edilen alt bölge verilerinin bulundukları, iller ve bulundukları bölgelere göre, gruplanmış ve hastalığın 1., 2., 3., olarak tanımlanan bölge ile 4. Bölge olarak tanımlanan bölgede bulunma olasılığı oran analizi ile belirlenerek hastalık koruma ve kontrolünde bölgesel mücadele programlarında bu bölgelere yönelik internet kullanım olanaklarının da dahil edildiği yöntemlerle mücadelesi önerilmiştir. Çalışma bulguları, hastalık koruma ve kontrolünün geleceğinin iletişim teknolojileri yönünde konusunda önemli işaretler vermektedir.

2. MATERYAL VE METOT

Bu çalışmada Google Trends ve Uluslararası Salgın Hastalıklar Ofisi verileri kullanılmıştır. Google Trends uygulamasında Türkiye'nin kuduz arama terimine ilişkin veriler 11 Ekim 2019 Tarihinde Saat 19.00 'da alınmıştır. Google Trends (Trends Google, 2019) ve Uluslararası Salgın Hastalıkları Ofisi (Wahis, 2019) Türkiye'nin kuduz hastalığı mihraklarına ait 01.01.2005-30.06.2019 zaman serisi verileri kullanılarak, aynı tarih aralığında il düzeyi verileri bölge düzeyine dönüştürülmüş ve veriler arasındaki ilişki oran analizi ile hesaplanmıştır.

Çalışmada kullanılan terimler ve yöntem

Alt bölgeye göre ilgi alanı: Terimin belirtilen zaman aralığında en popüler olduğu il görülmektedir. Popülerliğin belirlenmesinde değerler 0-100 arasında bir ölçekte hesaplanıp, 100 en yüksek popüler konum 0 değeri ise bu terim için yeter veri olmamasını ifade etmektedir.

İlgili konular: Terimi arayan kullanıcının aynı zamanda aradıkları konuları gösterirken en popüler konular popülerliğin belirlenmesinde kullanılan 0-100 arasında bir ölçekte hesaplanmaktadır.

Arama motorunda seçilen konu başlıkları

Kuduz:

1. Arama terimi: Kuduz
2. Zaman içinde gösterilen ilgi (1 Ocak 2005-30 Haziran 2019)
3. Alt bölge olarak ilk 25, ilk 15 ve ilk 10 il verilmiştir.
4. Çalışmada 01.01.2005-30.06.2019 aralığına ait Uluslararası Salgın Hastalıklar Ofisi (Office International Epizooti= OIE) Kuduz mihrak sayısı hücre verileri iller düzeyinde(15 yıl)

Microsoft Excel programında bir araya getirilerek il düzeyinde toplam mihrak sayıları ve hastalığın görülme sıklıkları hesaplanmıştır. Çalışma verileri en yüksek mihrak değerinden en düşük mihrak değerine göre ve en yüksek il frekansından (sıklık) en düşük il frekansına göre sıralanmıştır.

5. 81 il düzeyinde yapılan hesaplamalar sonucu hastalığın görülme sıklığının 12 yıl ve üzerinde olduğu 25 il değerlendirmeye alınmıştır.

6. Çalışmada illerin bulunduğu bölgeler Doğu Anadolu Bölgesi 1, Ege Bölgesi 2, Marmara bölgesi 3 ve diğer bölgeler 4 olarak tanımlanmıştır. Bu tanımlamada frekans dağılımı içinde en çok yer alan il sayıları esas alınarak 1. Bölge (11 İl), 2. Bölge (5 İl), 3. Bölge (2 il) geri kalan 4 ilin bölgesinin frekansı 2'nin altında olduğundan diğer olarak tanımlanmıştır. Çalışmada ilk 25, 15 ve 10 ilin tanımlı 3 bölgede bulunma oranı, mihrak sayıları, frekans dağılımı ve Google Trends alt bölgesinde bulunma oranları verilmiştir.

Çalışmada basit ve kolay anlaşılabilir bir değerlendirme ölçütü olarak kullanılan oran analizi yöntemi kullanılmıştır. Finansal değerlendirmelerde kullanılan oran analizi yöntemi bu çalışmaya uyarlanmıştır (KPMG, 1996).

Hastalığın 1.2.ve 3. bölge mihrakta görülme oranı (%) = Hastalığın 1.2.3. bölgede mihrakta görüldüğü il sayısı/ Toplam il sayısı

Hastalığın 1.2.ve 3. bölgede görülme yoğunluğu (frekans=sıklık) oranı (%) = Hastalığın 1.2.3. bölgede yoğun görüldüğü il sayısı/ Toplam il sayısı

Google Trends verilerinde 1.2.ve 3. Bölgede kuduz arama teriminin alt bölgede aranma oranı (%) = Google Trends'te kuduz arama teriminin alt bölgede arandığı il sayısı/ Toplam il sayısı

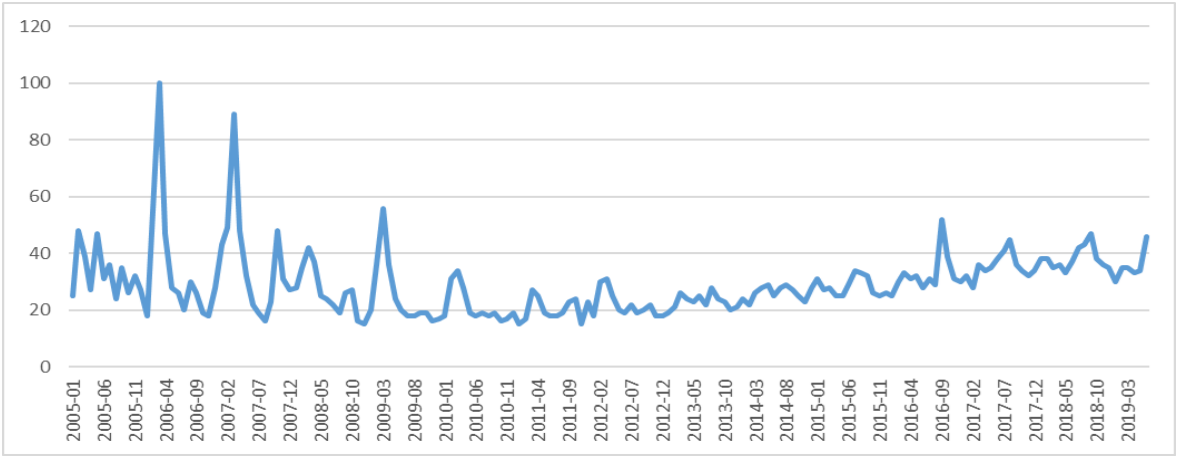
7. Yıllar itibariyle iller düzeyinde hastalığa ait toplam mihrak verileri ve frekanslar ile Google Trends kuduz arama verisi arasında iller düzeyinde bir ilişkinin olup olmadığı araştırılmıştır.

8. Çalışmada Google Trends verilerinde kuduz arama terimine ilişkin artış gösteren ilgili konu ve ilgili sorular konu hakkında geliştirilecek hastalık yönetim politikalarının tartışılması amacıyla verilmiştir.

9. Çalışmada son olarak elde edilen veriler dikkate alınarak hastalık anahtar kelimesi kullanılan durumlarda konulara ilişkin algı düzeyinin ve doğru bilginin erişimine olanak sağlayacak web tabanlı uygulamaların geliştirmesi ve ileriye dönük uygulanabilecek politikalar tartışılmıştır.

3. BULGULAR

Kuduz arama terimine ait Google Trends verilerinde zaman içinde meydana gelen değişimler şekil 1'de verilmektedir.



Kaynak: 11.10 2019 Tarihli Google Trends Verileri

Şekil 1. Google Trends verilerinde zaman içinde Kuduz arama terimine gösterilen ilgi

Kuduz arama terimini arayan insanların bu terimle ilgili konu başlıklarında ve ilgili sorularında ilk sıralarda bulunan alan seçimleri Tablo1'de sunulmuştur.

Tablo 1. Google Trends verilerinde Kuduz arama teriminde ilgili konular ve ilgili sorular

o	**İlgili konular**	**İlgili sorular**
	Köpek-Hayvan	Köpek
	Kedi-Hayvan	Kuduz Belirtileri
	Belirti-Konu	Kuduz Aşısını Kim Buldu
	İnsan-Primat	Kuduz Hastalığı
	Yan etki-Konu	Kuduz Aşısı

Kaynak: 11.10.2019 tarihli Google Trends Verileri

Çalışmada incelen yıllar için Kuduz vakaları mihrak sayıları ve hastalığın görülme sıklığı büyükten küçüğe göre 25 il dikkate alınarak sıralanmıştır. Google Trends verilerinde alt bölge olarak tanımlanan il sıralamasında ilk 25 il içerisinde yer alan iller alt bölge de alınan puanlarda dahil edilerek illerin bulundukları bölgeler belirlenmiş ve Tablo 2'de sunulmuştur.

Tablo 2. Kuduz vakalarının mihrak, görülme sıklığı ve Google Trends'de alt bölge puanlarına göre il sıralamasından bölge tespiti

No	İl	Mihrak	Bölge	İl	Sıklık	Bölge	İl	Alt bölge	Bölge
1	İzmir	386	2	Elâzığ	15	1	Ardahan	100	1
2	Şanlıurfa	316	4	Balıkesir	15	3	Ağrı	83	1
3	Balıkesir	235	3	Diyarbakır	15	4	Kars	65	1
4	Diyarbakır	235	4	İzmir	15	2	İzmir	58	2
5	Erzurum	228	1	Malatya	15	1	Osmaniye	56	4
6	Aydin	175	2	Manisa	15	2	Muş	55	1
7	Ağrı	150	1	Şanlıurfa	15	4	Giresun	51	4
8	Konya	147	4	Aydın	14	2	Çanakkale	51	3
9	Elâzığ	134	1	Bitlis	14	1	Yalova	51	3
10	Manisa	133	2	Erzincan	14	1	Uşak	50	2
11	Van	102	1	Erzurum	14	1	Çankırı	49	4
12	Hatay	95	4	Gaziantep	14	4	Isparta	48	4
13	Çanakkale	93	3	Hatay	14	4	Aydın	47	2
14	Bingöl	91	1	Tunceli	14	1	Edirne	47	3
15	Adana	90	4	Ardahan	13	1	Niğde	46	4

16	İstanbul	90	3	Bingöl	13	1	Yozgat	46	4
17	Malatya	86	1	Bursa	13	3	Balıkesir	46	3
18	Kars	83	1	K. Maraş	13	4	Kırklareli	46	3
19	Gaziantep	75	4	Kars	13	1	Aksaray	45	4
20	Iğdır	73	1	Mardin	13	4	Amasya	45	4
21	Erzincan	64	1	Van	13	1	Muğla	45	2
22	K. Maraş	63	4	Adıyaman	12	4	Rize	45	4
23	Mardin	61	4	Denizli	12	2	Çorum	45	4
24	Ankara	59	4	Iğdır	12	1	Düzce	45	4
25	Ardahan	56	1	Muğla	12	2	Kastamonu	43	4

Kaynak: 11.10.2019 Tarihli Google Trends ve OIE verileri

Tablo verileri kullanılarak yapılan oran analizi sonuçlarına göre; ilk 25 il dikkate alındığında bu illerin yüksek mihrak sayısına sahip bölgelerde %64'ünün (16/25 İl) bulunduğu hesaplanmıştır. Hastalığın görülme sıklığı (frekans) verileri incelendiğinde ise %75'inin (18/25 İl) yüksek frekansa sahip illerin bulunduğu ilk üç bölgede yer aldığı, Google Trends alt bölge illerinin taranma verilerinde ise bu oran %52 (13/25 İl) olarak tespit edilmiştir.

İlk 15 il dikkate alınarak yapılan hesaplamalarda, illerin %66,6'sının (10/15 İl) yüksek mihrak sayısına sahip bölgelerde bulunduğu hesaplanmıştır. Hastalığın görülme sıklığı dikkate alındığında illerin %73,3'ü (11/15İl) yüksek frekansa sahip illerin bulunduğu bölgelerde bulunmaktadır. Google Trends alt bölge verilerinde bu oran %66,6'tır (10/15 İl). İlk on il için yapılan hesaplamalarda %70'ilin (7/10 İl)yüksek mihrak sayısına sahip bölgelerde, %80'inin (8/10) yüksek frekansa sahip illerin bulunduğu bölgelerde, yüksek aranma oranına sahip illerin ise Google Trends alt bölge verilerinde oranının %80 (8/10 İl) olduğu belirlenmiştir.

4. SONUÇ ve TARTIŞMA

Kuduz hastalığının koruma ve kontrolü için temel fon kaynağı kamu harcamalarıdır. Hastalık yönetiminde Google Trends verileri kullanılarak hastalık koruma ve kontrolüne katkı sağlayacak politikalar geliştirilmesinin yanı sıra internet olanakları ile hastalığın kontrolüne yönelik bilgilendirmelerin ve eğitimlerin yapılması da mümkündür. Böylece kamu kaynaklarının etkin kullanım olanağı yaratılacaktır. Bu nedenle öncelikle Google Trends verileri kullanılarak hastalığa ilişkin verilerle bu veriler arasında bir bağlantı olup olmadığı araştırılmıştır.

Google Trends verileri Kuduz terimi aramalarının çalışma periyodunda Nisan 2006 ve Mart 2007'de artış gösterdiğini göstermektedir. Bu durumun belirtilen ay ve yıllarda basında Kuduz'a ilişkin çıkan haberlere bağlı olduğu düşünülmektedir. "Çorum'da Kuduz Paniği" başlıklı haber bağlamında Google Trends verileriincelendiğinde,22.08.2019 - 31.08.2019 tarihleri arasında alt bölgeye göre ilgi alanı iller sıralamasında, Çorum ili 90 ölçeği ile 2.sırayı almıştır(https://www.klimik.org.tr › 2019/08/24 › corumda-kuduz-panigi; https://www.aksam.com.tr › Yaşam). Bu durum internette "arama terimi" taramalarında yazılı basının etkisini de ortaya koymaktadır.

Çalışmada kuduz hastalığının 15 yıllık epidemiyolojik zaman serisi verileri ile uzun dönem Google Trends verileri arasındaki ilişki analiz edilerek verilerin uzun dönem sonuçları ile hastalık arasındaki ilişki değerlendirilmiştir. Diğer yandan, Çorum örneği, kısa dönem hastalık verileri ile de

il ve bölge için internet ortamında aynı dönemde kamunun bilgilendirme amaçlı reklamlarının ve linklerinin kullanılması vasıtasıyla hastalık yönetiminde etkinliğin artması sağlanabileceğini düşündürmektedir.

Google taramalarında ilgili konu ve sorulara ilişkin arama yapanların genel olarak konu bağlamında arama yaptıkları görülmektedir (Tablo 1). Hastalıktan koruma tedbirlerine ilişkili bilgi ve reklamlar bu durum dikkate alınarak geliştirilmelidir.

Çalışmada kuduz hastalığı Uluslararası Salgın Hastalıklar Ofisi mihrak sayıları ve hastalığın frekans verileri ve Google Trends verilerinin Alt Bölge tanımı içinde yer alan illerin bulundukları bölgeler belirlenmiştir. Google Trends verileri alt bölge olarak sırasıyla 25, 15 ve 10 il için sıralanmıştır. Bu sıralamalarda %52 (13/25 İl), %66,6 (10/15İl), %80 (8/10İl) oranında hastalığın mihrak sayılarının ve frekans dağılımlarının yüksek düzeyde tespit edildiği bölgelerde arandığı tespit edilmiştir. Çalışma sonuçları dikkate alındığında hastalık yönetiminde bölge esas alınarak politika oluşturmanın önemini ve uzun dönem Google Trends verilerinin hastalık kontrolünde bölge bazlı politika oluşturmada yararlanılabilecek önemli bir kaynak olduğunu düşündürmektedir.

Google araştırma verileri büyük popülasyonlardan sağlamaktadır. Bileşik Devletlerde influenza aktivitesini tespit etmek amacıyla 2003-2007 yılları arsı verilerin değerlendirildiği çalışmada influenza salgınında alınması gereken önlemlerde yerel medya bilincinin arttırılması önerilmektedir (Ginsberg vd., 2009). Bu çalışma da hastalığın görülme sıklığı ve mihrak sayısının yoğun olduğu bölgelerde medya olanaklarının ivedilikle hayata geçirilmesinin önemini bir kez daha ortaya koymuştur. Kuduz hastalığının farkındalığını arttırmak amacıyla kuduz anahtar sözcüğü kullanıldığında doğru bilgilere ulaşımın sağlandığı resmi link verilerine ulaşımın sağlanması, bilginin içeriğinin kısa, anlaşılır ve etkin olarak planlanması, hedefe ve hedef kitleye uygun planlanması sağlanmalıdır. Diğer taraftan konu hakkında küçük anketlerle bu bilgileri almak isteyen kişilerin yaş bilgileri edinilerek gelecek dönemler için yaş gruplarına göre etkili olabilecek teknikler geliştirilmelidir. Google Trends verilerinin hayvan sağlığı koruma ve kontrolüne yönelik yakın gelecekte iyi kullanılırsa önemli avantajlar yaratacağı düşünülmektedir. Bu doğrultuda yakın gelecekte bu yönde önemli çalışmaların yapılacağı ve kısa orta ve uzun vade Google Trends verilerinin dikkate alındığı farklı hastalık verilerinin araştırıldığı çalışmaların giderek önem kazanacağı düşünülmektedir. Yakın geleceğin diğer sosyal medya olanakları kullanımı açısından da fırsat yaratabileceği araştırmacılara açısından göz önünde tutulmalıdır.

Sonuç olarak bu çalışma, salgın hastalıklar konusunda Türkiye açısından Google Trends verilerinin kullanımının önemli bir fırsat olarak önümüzde durduğunu göstermiştir. Bu olanağın kullanılmasının yakın geleceğin hayvan hastalıkları koruma ve kontrolünün politikalarının geliştirilmesinde hem çağın olanaklarından yaralanma hem de hastalıklarla etkin mücadelede il düzeyinde verilerle bölgesel mücadele programlarının geliştirilmesinde insana kolay erişim açısından önemli fırsatlar yaratacağını ortaya koymaktadır.

KAYNAKÇA

Althouse Bm, Ng Yy, Cummıngs Dat. (2011). Prediction of Dengue Incidence Using Search Query Surveillance. PLoS Negl Trop Dis 5(8), e1258. doi:10.1371/journal.pntd.0001258.

Dugas Af, Jalapour M, Gel Y, Levın S, Torcaso F, Igusa T, Rothman Re. (2013). Influenza Forecasting with Google Flu Trends, Plos One, 8(2), e56176

Gınsberg J, Mohebbı Mh, Patel Rs, Brammer L, Smolınskı Ms, Brıllıant L. (2009). Detecting Influenza Epidemics using Search Engine Query Data, Nature 457, 1012 –1014.

Goel S, Hofman Jm, Lahaıe S, Pennock Dm And Watts Jd. (2010). Predicting consumer behavior with Web search, PNAS, 107 (41), 17486–17490.

Google Trends. (2019). Google Trends (https://Trends.Google.com.tr/Trends/explore?date=2005-01-01%202019-06-30&geo=TR&q=kuduz).

Hampson K, Coudevılle L, Lembo T, Sambo M, Kıeffer A, Attlan M, Barrat J. Aet al., (2015). Global Alliance for Rabies Control Partners for Rabies Prevention. PLoS Negl Trop Dis. 9(4), e0003709.

Jemberu Wt, Molla W, Almaw G, Alemu S. (2013). Incidence of Rabies in Humans and Domestic Animals and People's Awareness in North Gondar Zone, Ethiopia. PLoS Negl Trop Dis 7(5): e2216. doi:10.1371/journal.pntd.0002216.

Kpmg Peat Marwıck Llp. (1996). "Financial Ratio Analysis Project," Final Report, US Department of Education.

Regea G. (2017). Review on Economic Importance's of Rabies in Developing Countries and Its Controls, Arch Prev Med, 2(1): 015-021.

Shwıff Sa, Brown Vr, Dao Tt, Elser J, Trung Hx, Tıen Nn, et al., (2018). Estimating the economic impact of canine rabies to Viet Nam 2005–2014. PLoS Negl Trop Dis 12(10): e0006866.

Wahıs (2019). Wahis interface, country information, disease information, Turkey, Rabies, https://www.oie.int/wahis_2/public/wahid.php/Countryinformation/Countryhome (Erişim 1.10 2019)

Wallace Rm, Etheart Md, Doty J et al., (2016). Dog-Mediated Human Rabies Death, Haiti, Emerg Infect Dis, 22(11),1963–1965. doi:10.3201/eid2211.160826.

Yıldız MS. (2018). Google Search Trends: An Application For Health Services Related Queries ın Turkey, International Journal of Health Management and Strategies Research, 4(2): 168-179.

Zeybek Ö,Uğurlu E, Yuceoglu B. (2018). Google arama trendi verileriyle tüketicilerin harcama niyetleri öngörülebilir mi? Çevirim içi perakende sektörü uygulaması, 19. Uluslararası Eyi Sempozyumu (17-20 EKİM 2018).

Makale Türü: Araştırma Makalesi
Paper Type: Research Paper

INSTAGRAM'DAKİ INFLUENCER'LARIN TAKİPÇİLER ÜZERİNDEKİ ETKİSİ*

***

THE EFFECT OF INFLUENCERS IN INSTAGRAM ON FOLLOWERS

Selçuk KIRAN*
Cansu YILMAZ**
İlkim Ecem EMRE***

DOI: 10.33461/uybisbbd.637155

Öz

Web 2.0 teknolojilerinin gelişmesiyle sosyal medya araçları ortaya çıkmış ve bu araçlar günlük yaşantımızın önemli bir parçası haline gelmişlerdir. Sosyal medyanın kullanıcılar üstündeki etkisi artmaya başladıkça, görüşleri izleyicileri tarafından dikkate alınan "Influencer" olarak adlandırılan kişiler göze çarpmaya başlamışlardır. Influencer'ların kitlelerle hızlı ve etkili iletişimi markaların da dikkatini çekmiş ve markalar ürünlerini veya hizmetlerini daha geniş kitlelere ulaştırmak için Influencer'ların sosyal medyadaki gücünü kullanmaya yönelmişlerdir. Bu iş birlikleri günümüzün en önemli pazarlama faaliyetlerinden biridir ve "Influencer Marketing" olarak adlandırılmaktadırlar. Bu çalışma Instagram'daki Influencer'ların takipçileriyle aralarındaki ilişkileri ölçmek amacıyla yapılmıştır. Araştırmada, veri toplamak için anket yapılmıştır. Anket formu öğrencilere elektronik ortamda gönderilmiş ve 282 katılımcı ile gerçekleştirilmiştir. Anket ile toplanan veriler SPSS programı ile analiz edilmiştir. Çalışmanın bulgularına göre, cinsiyet ve eğitim seviyesi faktörlerinin Instagram'da takip edilen alanlarla ilişkisi olduğu, cinsiyetin satın alma kararları üzerinde etkili olduğu ve Instagram'da geçirilen zaman ile ürün satın alma arasında bir ilişki olduğu sonuçlarına ulaşılmıştır. Elde edilen sonuçların kurumlara, Instagram üzerinde hedef kitlelerine göre yapacakları Influencer seçiminde faydalı olacağı düşünülmektedir.

Anahtar Kelimeler: *Sosyal Medya, Instagram, Sosyal Medya Pazarlaması, Influencer Marketing.*

Abstract

With the development of Web 2.0 technologies, social media tools have emerged and social media tools have become an important part of our daily lives. As the influence of social media on users begins to increase, it has emerged people called "Influencer" whose views are taken into account by particular followers. The rapid and effective communication of influencers with followers has begun to attract attention by brands, and brands have begun to use the power of influencers on social media to deliver their products or services to wider audiences. These collaborations are one of the most important marketing activities of today and are called "Influencer Marketing". This study was conducted to measure the relationship between influencers on Instagram and their followers. Survey method was used to collect data. The questionnaire was sent to students electronically and conducted with 282 participants. The data collected by using questionnaire were analyzed with SPSS. According to the findings of the research, it is found that, gender and education level factors are related to the areas followed in Instagram, gender has an effect on purchasing decisions, and there is a relationship between time spent on Instagram and product purchase. It is thought that the obtained results will be useful for the institutions while selecting influencers according to the target followers on Instagram.

Keywords: Social Media, Instagram, Social Media Marketing, Influencer Marketing.

* Bu çalışma, lisans programı bitirme ödevi olarak sunulmuştur.

* Dr. Öğr. Üyesi, Marmara Üniversitesi, İşletme Fakültesi, İşletme Enformatiği Bölümü, selcuk.kiran@marmara.edu.tr
ORCID: 0000-0001-6088-2701
** * Marmara Üniversitesi, İşletme Fakültesi, İşletme Enformatiği Bölümü, cnsylmz95@gmail.com
ORCID: 0000-0001-7144-4627
*** Arş. Gör., Marmara Üniversitesi, İşletme Fakültesi, İşletme Enformatiği Bölümü, ecem.emre@marmara.edu.tr
ORCID: 0000-0001-9507-8967

Geliş Tarihi / Received: 23.10.2019
Kabul Tarihi / Accepted: 17.12.2019

1. GİRİŞ

Teknolojinin gelişmesiyle birlikte internet günümüzün en yaygın ve en etkili iletişim aracı haline gelmiştir. İnternet kullanımının artmasıyla birlikte hem sosyal alanlarda hem de iş hayatında alışkanlıklar değişmeye başlamış ve eş zamanlı olarak hayatımıza yeni kavramlar girmiştir; bu kavramlardan biri de sosyal medyadır.

Bireyler sosyal medya aracılığıyla duygu ve düşüncelerini paylaşmakta, yeni fikirler üretebilmekte ve bu fikirler üzerinde tartışabilmektedir. Bunun yanı sıra insanlar, sosyal medya platformlarında kendi kişisel bilgilerini, çeşitli fotoğrafları ve videoları paylaşabilmektedirler. Sosyal medyanın insanlara sunduğu bir başka önemli özellik ise kullanıcıların, içerikleri kendi istekleri doğrultusunda hem üreten hem de tüketen bireyler olmalarına imkân vermesidir. Bir başka ifadeyle sosyal medya, kullanıcıların rolünü aktif ve katılımcı bireyler olmaları yönünde değiştirmektedir. Sosyal medyanın, kullanıcılarının katılımına olanak sağlayan yapısı, belki de aktif izleyici kavramının ilk defa, anlamını bu kadar bulmasını sağlamaktadır. Kullanıcılar; kendi eğilimleri, gereksinimleri, istekleri ve ilgi alanları doğrultusunda, tüketmek ya da paylaşmak ve katılımda bulunmak istedikleri içerikleri seçerek ve hatta içerikleri üreterek sosyal medya platformlarını kullanmaktadırlar (Koçak, 2012). Bu platformların yayılması ile birlikte tüketiciler üzerindeki etkisi de günden güne artmaktadır. Sosyal medya araçlarında kitleleri etkileme gücü bulunan, takipçileri tarafından otorite ya da bilirkişi kabul edilen kişilerle birlikte "Influencer" kavramı ortaya çıkmıştır. Influencer'lar; sosyal medyada belirli bir takipçi kitlesine sahip olan, takipçi kitleyi fikir ve önerileri ile etkileme güçleri bulunan, kanaat önderi olarak kabul edilen kişilerdir.

Bu çalışmada, Instagram'daki Influencer'ların tüketici davranışları üzerindeki etkisinin ölçülmesi amaçlanmıştır. Bu doğrultuda 18 yaş ve üzerindeki Instagram kullanıcılarına anket yapılmış ve anket sonuçları tanımlayıcı istatistik yöntemleri ki-kare testi ve t-test kullanılarak analiz edilmiştir.

2. GELENEKSEL PAZARLAMADAN DİJİTAL PAZARLAMAYA

Amerikan Pazarlama Derneği (AMA) pazarlama kavramını şu şekilde açıklamıştır (American Marketing Association (AMA), 2017; marketingdersleri.blogspot.com, 2015): *"Pazarlama; alıcılar, tüketiciler, ortaklar ve geniş boyutuyla toplum için değer ifade eden ürünlerin geliştirilmesi, dağıtımı, mübadelesi ve ilgili gruplarla iletişim kurulmasını sağlayan bir dizi işlemler ve kuruluşlardan oluşan bir faaliyettir."*

Klasik pazarlama kavramı, bir ürün ve hizmetle ilgili mevcut pazarların korunması, zamanla genişletilmesi ve yeni pazarların oluşturulması anlamına gelmektedir. 20. yüzyılda teknolojinin gelişip internetin hayatımıza girmesiyle birlikte pazarlamanın anlamında da değişim başlamıştır. İnternet, mesafeleri azaltmış, bilgi akışını hızlandırmış ve yeniliklerin anında hedef kitlelere ulaşmasını sağlamıştır. Bu sebeple işletmeler, geleneksel pazarlama yöntemlerini bırakıp, sanal dünya üzerinden pazarlama yapma faaliyetlerine ağırlık vermeye başlamışlardır. Bu yeni yöntem daha geniş bir hedef kitlesine ulaşma imkânı sağlayıp, maliyetleri düşürme fırsatı sunmuştur (Mert, 2018).

Dijital pazarlama, işletmeler ile müşterilerin hızlı bir şekilde birebir iletişim kurmalarını sağlamıştır. İşletmeler, dijital ortamdaki araçlar üzerinden, müşterilerin ürün ve/veya hizmetlerle ilgili geri bildirimleri doğrultusunda nasıl bir strateji izlemeleri gerektiğini belirlemeye başlamışlardır. İlk başlarda e-posta üzerinden sağlanan dijital pazarlama, bugün sosyal medya araçlarıyla birlikte daha etkili bir şekilde kullanılmaktadır.

Sosyal medya kullanıcılarının içerik oluşturma sürecine aktif olarak dâhil olmasıyla moda, film, spor, seyahat gibi alanlarda sunulan görüşler internette hızla yaygınlaşmıştır. Kullanıcıların sosyal ağlara girmelerinin nedenleri; başkaları ile kolay iletişim kurma, güncel olayları takip etme, bilgi edinme ve sosyalleşme beklentisidir. Bu sebeple sosyal ağlar kısa sürede geniş bir alana yayılmış ve pazarlama açısından önemli bir yere gelmişlerdir (Mert, 2018). Sosyal medyada hızlı geri dönüşlerin alınması, çeşitli yorumların herkes tarafından görülebilmesi, bir ürün veya hizmetle ilgili içeriklere kolayca ulaşılabilmesi, tüketicinin satın alma kararını etkilemektedir. Sosyal medya pazarlaması işletmelerin itibar ve marka değerini arttıran bir etken olarak kabul edildiği gibi, zaman, para tasarrufu ve hızlı geri bildirim sağladığından işletmeler açısından da büyük önem taşımaktadır (Yanar ve Yılmaz, 2017).

Bireylerin deneyimlediği bir ürün ya da hizmetle ilgili düşüncelerini pazarlama amacı gütmeden başka kişilere aktarmasına "*ağızdan ağıza pazarlama*" (Word of Mouth Marketing, WOMM) denir. Bu kavram 1960'larda literatüre girmiş olsa da insanlık tarihi kadar uzun bir geçmişe sahiptir. Bireyler yakın ilişki içinde olduğu kişilerden gelen bilgileri daha güvenilir ve daha doğru bulurlar ve bu bilgiler, bireylerin düşünceleri, duyguları ve davranışları üzerinde önemli bir etki yaratır. Bir şey satma amacı olmayan bir arkadaş, akraba veya komşunun, bir ürün ya da hizmet hakkındaki fikirleri bireylere daha fazla güven vermektedir (Yavuzyılmaz, 2015). İnternetin kullanımının artmasıyla birlikte bireyler daha çok kişiyle zamandan ve mekândan bağımsız olarak bilgi alışverişinde bulunmaya başlamışlardır. Tüketiciler internette yapılan ağızdan ağıza iletişim sayesinde, bir ürün veya hizmet hakkında yapılan yorumlara, forumlar, e-postalar ve sosyal medya araçları aracılığıyla kolaylıkla ulaşabilir hale gelmişlerdir. Bunun yanında internet aracılığıyla ürün ve hizmetler hakkında karşılaştırmalı bilgi sunan kaynaklara da ulaşabilmektedirler. Geleneksel ağızdan ağıza iletişimde, bu iletişimin başlatıcıları olan kanaat önderleri, fikirlerini tüketicilere yüz yüze aktarmaktadırlar. Teknolojinin gelişmesiyle birlikte ağızdan ağıza iletişim de yeni bir anlam kazanmış ve sosyal medya araçları sayesinde belirli bir kitleyi etkileme gücüne sahip olan kişiler, fikirlerini daha geniş kitlelere duyurma şansı elde etmişlerdir. Bu sebeple günümüzde ağızdan ağıza iletişimin en yoğun ve etkili yaşandığı yer sosyal medyadır. Eskiden etki alanı çevresindeki kişi sayısıyla sınırlı olan tüketiciler, bugün sosyal medya sayesinde milyonlarca kişiye tek tıkla ulaşabilmektedir. Ağızdan ağıza iletişim faaliyetlerinin sosyal medyada artmasıyla literatüre "*elektronik ağızdan ağıza pazarlama"* eWOM (electronic Word of Mouth) kavramı da eklenmiştir.

Instagram, Kevin Systrom ve Mike Krieger tarafından 2010 tarihinde ücretsiz bir fotoğraf paylaşım uygulaması olarak kurulmuştur. Önceleri Apple işletim sistemi için geliştirilen bu uygulama daha sonra Android işletim sistemi için de kullanılabilir hale getirilmiş ve kısa sürede birçok kullanıcıya ulaşmıştır. 2012 yılında Facebook'un Instagram'ı satın almasıyla birlikte kullanıcı sayısında büyük miktarda bir artış olmuştur. Bu artış sonucunda işletmeler, Instagram'ı pazarlama amaçlı bir platform olarak görmeye başlamışlardır. Markalar, Instagram üzerinden hesap açabilmekte, etiket (hashtag) kullanarak görünürlüklerini ve beğeni sayılarını arttırabilmekte, yüksek takipçisi olan hesaplara reklam verebilmekte ve takipçilerini markayla ilgili paylaşım yapmaya teşvik edebilmektedirler (Aslan ve Ünlü, 2016). Instagram, maliyeti düşük, etkileşim gücü yüksek bir platform olduğu için küçük işletmeler için önemli bir satış ve tanıtım aracı olarak görülmektedir. Instagram'da işletmeler ürünlerinin bilgilerini ve görsellerini paylaşarak bir anda geniş kitlelere ulaşmaya başlamışlardır. Özellikle doğru etiketleme yöntemiyle yapılan paylaşımlar, hedef kitle arasında hızla yayılabilmektedir. Kullanıcılar ilgi alanlarına giren ürün veya hizmeti satan işletmelerin profillerine bakarak ürün hakkında bilgiye ve ürünün görsellerine ulaşabilmektedirler (Yılmazsoy, 2019). İlgi çekici gönderiler, işletme hesabının kalitesi ve ürün hakkında doğru bilgilendirme, Instagram'dan yapılan pazarlamanın hedefine ulaşmasını etkileyen faktörlerdir. Bu sebeple Instagram reklamcılığı son yıllarda hızlı bir yükseliş içerisindedir.

Sosyal medyada güçlü bir takipçi kitlesi olan, öneri ve fikirleriyle takipçi kitlesinin davranışlarını etkileyen veya değiştiren kişilere "*influencer*" denir (Sevinç, 2018). Influencer'lar

takipçi sayılarına göre mikro ve makro olmak üzere ikiye ayrılırlar. Mikro Influencer terimi daha az takipçi sayısına sahip olanlar için kullanılır. Takipçi sayısı markalar için önemli bir ölçüt olsa da mikro Influencer'ların takipçileri ile arasındaki iletişim ve etkileşim daha güçlüdür. Bu yüzden markalar için önemlidirler. Makro Influencer ise yüksek takipçi sayısına sahip Influencer'lar için kullanılır. Bu kişiler sosyal iletişim ağlarında daha geniş bir kitleye hitap ederler. Makro Influencer'ların markalar tarafından tercih edilme sebepleri erişim gücü ve görünürlük yaratma imkânlarıdır. Pinghelsinki, markaların doğru etkiyi yaratacak kişilerle iş birliği yapması için Influencer'ların sahip olmaları gereken özellikleri; ürün veya hizmet hakkında bilgi sahibi olmaları, ürüne veya hizmete ilgi duymaları, seçilen alanda uzman ya da bilirkişi olmaları, hangi tür paylaşımla dikkat çekeceklerini bilmeleri, gerekli etkileşimi sağlayacak takipçi sayısına sahip olmaları, ticari iş birliğine uygun olmaları ve yapılacak çalışmaya gereken önemi verip, iyi iş birliğine uygun olmaları şeklinde özetlemiştir (Aktaş, 2018).

Artan rekabet koşulları birçok firmayı pazarlama alanında yenilikler yapmaya itmektedir. Firmalar, rakip firmalara karşı avantaj sağlamak için tüketiciye ulaşabilecekleri en etkili kanalları belirleme ihtiyacındadırlar. Sosyal medyada yapılan ağızdan ağıza pazarlama sayesinde firmalar zaman ve mekân gibi etkenler olmaksızın geniş bir tüketici kitleye ulaşabilmektedir. Sosyal medya araçlarında kitleleri etkileme gücü bulunan, takipçileri tarafından otorite ya da bilirkişi kabul edilen kişilerin, hitap ettiği kitlenin satın alma davranışını etkileme gücünü kullanarak pazarlama stratejisi yapmasına "*Influencer Marketing*" denir. Influencer marketing kavramının Türkçe literatürde oturmuş bir karşılığı olmadığı, bu kavramın çeşitli kaynaklarda fenomen pazarlaması, nüfuz pazarlaması, hatırlı pazarlama ya da etkileyen pazarlaması olarak kullanıldığı belirtilmektedir (Saltık Yaman, 2018). Diğer bir deyişle Influencer marketing, sosyal medya kanallarında yüksek takipçi sayılarına sahip Influencer'ların paylaşımlarıyla bir ürün ya da hizmet hakkındaki deneyimlerini takipçilerine aktarmasıdır.

McCracken (1989)'a göre bir ünlünün markaya olan katkısı o ünlünün sahip olduğu kültürel anlamların ilk önce ünlünün tanıtımını yaptığı markalı ürün ya da hizmete aktarılması, oradan da o ürün ya da hizmeti satın alan tüketiciye taşınması ile ortaya çıkmaktadır. Bu yaklaşıma "*anlam transfer modeli*" denir ve pazarlamada ünlü kullanımının temelini oluşturur. Bu yaklaşıma göre pazarlamacılar; sosyal medyanın ortaya çıkışıyla birlikte tüketicilerin hayatına giren yeni ünlü türü olan Influencer'lar ile iş birliğine gittiklerinde o kişinin sahip olduğu imaj ve özdeşlik ilişkilerini markalarına taşıma amacı güderler.

Influencer ve marka iş birlikleri çeşitli şekillerde olabilir. IAB (Interactive Advertising Bureau, 2018) Influencer Pazarlama Raporu'nda, markaların Influencer'larla çalışma şeklini, ücretli, ürün karşılığı ve etkinliğe davet olmak üzere 3 kategoride incelenmektedir. Reklam veren, influencer ile belirli bir paylaşım sayısı veya paylaşım başına ücret şeklinde "ücretli" iş birliğine gidebilir; yapılacak reklam kampanyası çerçevesinde Influencer'lara ücretsiz markalı ürün gönderip Influencer'ların bu ürünlerle ilgili içerik paylaşımı yapmasını teşvik edebilir. Bunların yanı sıra, Influencer'ı markanın düzenlediği bir etkinliğe davet ederek, ücret karşılığı ya da gönüllü olarak bu davetle ilgili paylaşımda bulunmasını sağlayabilir. Markalar bu iş birliklerinin yanı sıra bu bireylerle farklı iş birliği stratejileri de izlemektedirler. Bu stratejiler markanın amacına göre şekillenmektedir. Bu stratejiler marka elçiliği, ürün yerleştirme ve etkinlik yorumlatma şeklinde üç kategoriye ayrılmaktadır. Marka elçisi, uzun süreli bir ilişki çerçevesinde markanın kimliğini ücretli olarak temsil eden kişidir. Balasubramanian (1994)'e göre ürün yerleştirme, markalı bir ürünün sinema ve televizyon programlarının içine planlı ve göze çarpmayacak şekilde yerleştirmesiyle izleyiciyi etkilemeyi amaçlayan paralı ürün mesajlarıdır. Dijital ortamlara göre değerlendirildiğinde ise, markalar ürün yerleştirmeyi çeşitli web sitelerinde, oyunlarda ve çeşitli sosyal ağlarda kullanmaktadır. Instagram'da ürün yerleştirme, markanın kullanıcıların ürettiği içerikle birleştirilmesi olarak tanımlanmaktadır. Markalar tarafından düzenlenen ürün tanıtım etkinliklerinin amacı ise, Influencer'lar arasında markanın tanınırlığını arttırmak ve onları marka hakkında

bilgilendirmek olarak özetlenebilir. Bu etkinliklerin amacı esasen, markayı Influencer'ların gündemine sokmak, onların da yorum yaparak marka hakkında takipçilerine yönelik gönüllü içerik üretmesini sağlamaktır.

3. YÖNTEM

Bu çalışmada veri toplama aracı olarak anket formu kullanılmıştır. Anket soruları 18 yaş ve üzerindeki Instagram kullanıcıları tarafından çevrimiçi bir ortamda (Google Forms) cevaplandırılmıştır. Araştırma 282 katılımcı ile gerçekleştirilmiş ve yapılan anketlerin hepsi analizlere dâhil edilmiştir. 0,05 örnekleme hatasına göre bulunması gereken katılımcı sayısı 246'dır (Yazıcıoğlu ve Erdoğan, 2004) ve anketle ulaşılan katılımcı sayısı bunu sağlamaktadır. Anket soruları Peltekoğlu & Tozlu (2018) ve Yanar & Yılmaz (2017)'nin çalışmalarındaki sorular örnek alınarak oluşturulmuştur.

Araştırmada kullanılan anket farklı bölümlerden oluşmaktadır. İlk bölümde katılımcıların demografik özellikleri ile internet ve Instagram kullanım alışkanlıklarını öğrenmeye yönelik sorular bulunmaktadır. İkinci bölümde kullanıcıların Instagram'da takip ettikleri alanlara yönelik sorular yöneltilmiştir. Son bölümde ise katılımcıların Instagram'daki Influencer'ları takip etme sebepleri, tüketicilerin satın alma kararına ilişkin değerlendirmeler ve Instagram'daki Influencer'lara duyulan güven ile ilgili Likert tipi sorular sorulmuştur. Çalışma kapsamında hipotezler oluşturulmuş ve bu hipotezler SPSS kullanılarak test edilmiştir. Verileri analiz etmek için tanımlayıcı istatistik yöntemleri, güvenilirlik analizi, ki-kare testi ve t - testi yapılmıştır.

4. BULGULAR

Çalışmanın bu kısmında; tanımlayıcı istatistikler, ki-kare testi, güvenilirlik ve t-testi sonuçları paylaşılmıştır.

4.1.Tanımlayıcı İstatistikler

Çalışmaya katılan kişilerin cinsiyetini, yaşını, eğitim durumunu, medeni durumunu, aylık gelirini, gün içerisinde internette geçirdiği zamanı, Instagram'da geçirilen zamanı, ne kadar süredir Instagram hesabına sahip olduğunu, hangi hesapları takip ettiği ve son bir yılda Instagram'da Influencer'lar tarafından tanıtılan bir ürünü satın almasına yönelik soruların yanıtları incelenmiştir (Tablo 1).

Tablo 1: Demografik Özellikler ile İnternet ve Instagram Kullanım Alışkanlıkları ile İlgili Bulgular

Demografik Özellikler	**N**	**%**		**N**	**%**
Cinsiyet			**Gün içerisinde internette harcanan zaman**		
Kadın	189	%67	0-3 saat	125	%44,3
Erkek	93	%33	3 saat üzeri	157	%55,7
Yaş			**Instagram'da gün içerisinde geçirilen zaman**		
18-24	210	%74,5	1 saatten az	99	%35,1
25 yaş ve üzeri	72	%25,5	1 saat ve üzeri	183	%64,9
Eğitim Seviyesi			**Ne kadar süredir Instagram hesabına sahipsiniz?**		

Lise ve altı	91	%32,3	0-3 yıl	88	%31,2
Lisans ve üzeri	191	%67,7	3 yıldan fazla	194	%68,8
Medeni Durum			**Son bir yılda Instagram'da Influencer'lar tarafından tanıtılan bir ürünü satın aldınız mı?**		
Bekar	232	%82,3	Hayır	237	%84
Evli	50	%17,7	Evet	45	%16
Gelir Düzeyi					
0-1500 TL	148	%52,5			
1500 TL üzeri	134	%47,5			

Yapılan analiz sonuçlarına göre bu çalışmaya katılan 282 katılımcının %67'si kadın, %33'ü erkektir. Yaşa göre dağılım incelendiğinde katılımcıların %74,5'i 18-24 yaş arasında, %25,5'i yaş ve üzerindedir. Katılımcıların eğitim seviyesine bakıldığında %32,3'ü lise ve altı, %67,7'si lisans ve üzeri eğitim almıştır. Çalışmaya katılanların %82,3'ü bekar, %17,7'si evlidir. Anket katılımcılarının aylık gelirine bakıldığında %52,5'i 1500 TL altı, %47,5'i ise 1500 TL ve üzerinde aylık gelire sahip olduklarını belirtmişlerdir (Tablo 1).

İnternet kullanım sıklığı incelendiğinde, katılımcıların %44,3'ünün gün içerisinde 0-3 saat, %55,7'si 3 saat ve üzeri internette vakit geçirdiği görülmüştür. Katılımcıların Instagram kullanım sıklığını incelendiğinde ise, %35,1'inin gün içerisinde 1 saatten az, %64,9'unun 1 saatten fazla Instagram'da zaman harcadığı görülmüştür. Katılımcıların %31,2'si 3 yıldan az ,%68,8'i 3 yıl ve üzeri süreler ile Instagram hesabına sahiptir. Son olarak katılımcıların son bir yılda Instagram'da Influencer'lar tarafından tanıtılan bir ürünü satın alma sıklığına bakıldığında, %84'ü "hayır", %16'sı "evet" cevabını vermiştir (Tablo 1).

4.2. Ki-Kare Testlerine Ait Bulgular

İki kategorik değişken arasında anlamlı bir ilişki olup olmadığını incelemek için ki-kare testi uygulanır ve bu testte önemli olan Pearson-Chi Quadrat değerinin 0,05'ten küçük olmasıdır (Yazıcıoğlu ve Erdoğan, 2004). Bu değer 0,05'ten küçük ise, iki değişken arasında bağımlı bir ilişki olduğu söylenir ve hipotez kabul edilir. Bu bölümde; cinsiyet, yaş ve eğitim seviyesi ve Instagram'da geçirilen zaman faktörlerine bağlı olarak yapılan test bulgularına yer verilmiştir.

H_1:Cinsiyet ile son 1 yılda Instagram'da Influencer'lar tarafından tanıtılan bir ürünü satın alma arasında ilişki vardır.

Tablo 2'ye bakıldığında Sig.2 değeri 0,00 olup 0,05'ten küçük olduğu için H_1 hipotezi kabul edilmiştir. Yani cinsiyet ile son bir yılda Instagram'da Influencer'lar tarafından tanıtılan bir ürünü satın alma arasında anlamlı bir ilişki olduğu görülmektedir. Yine tabloya bakıldığında kadınların erkeklere göre daha fazla alışveriş yapmış olduğunu görülmektedir.

Tablo 2: Cinsiyet ve Satın Alma

	Erkek		Kadın					
	Adet	**Beklenen**	**Adet**	**Beklenen**	**Pearson**	**Sig.2**	**φ**	**Sig.**
Satın Alma	4	14,8	41	30,2	14,058	0,000	0,000	0,000

H_2: Cinsiyet ile Instagram'da takip edilen alan arasında ilişki vardır.

Tablo 3'e bakıldığında tüm Sig.2 değerleri 0,05'ten küçük olduğu için H_2 hipotezi kabul edilmiştir. Yani cinsiyet ile Instagram'da takip edilen alan arasında anlamlı bir ilişki vardır. Bu tabloda moda, makyaj/güzellik, sağlıklı yaşam, yemek ve kitaplar/dergi alanlarının kadınlar tarafından daha çok takip edildiğini, teknoloji ve spor alanlarının ise erkekler tarafından daha fazla takip edildiğini görülmektedir.

Tablo 3: Cinsiyet ve Instagram'da Takip Edilen Alan

	Erkek		Kadın					
	Adet	**Beklenen**	**Adet**	**Beklenen**	**Pearson**	**Sig.2**	**φ**	**Sig.**
Moda	7	39,2	112	79,8	68,389	0,000	0,000	0,000
Makyaj/Güzellik	4	31,7	92	64,3	54,665	0,000	0,000	0,000
Sağlıklı Yaşam	13	28,4	73	57,6	17,862	0,000	0,000	0,000
Teknoloji	56	31,3	39	63,7	43,710	0,000	0,000	0,000
Yemek	20	40,9	104	83,1	28,428	0,000	0,000	0,000
Spor	66	34,6	39	70,4	67,567	0,000	0,000	0,000
Kitaplar/Dergi	25	34,3	79	69,7	5,958	0,015	0,018	0,015

H_3: Yaş ile Instagram'da geçirilen zaman arasında ilişki vardır.

Tablo 4'e bakıldığında Sig.2 değeri 0,05'ten küçük olduğu için H_3 hipotezi kabul edilmiştir. Yani yaş ile Instagram'da geçirilen zaman arasında anlamlı bir ilişki vardır. Ayrıca 18-24 yaş grubunun Instagram'da daha fazla zaman geçirdiği görülmektedir.

Tablo 4: Yaş ve Instagram'da geçirilen zaman

	18-24 yaş		25 yaş ve üzeri					
	Adet	**Beklenen**	**Adet**	**Beklenen**	**Pearson**	**Sig.2**	**φ**	**Sig.**
1 saatten az	63	73,7	36	25,3	9,414	0,002	0,003	0,002
1 saat ve üzeri	147	136,3	36	46,7				

H_4: Eğitim seviyesi ile Instagram'da geçirilen zaman arasında ilişki vardır.

Tablo 5'e bakıldığında Sig.2 değeri 0,034 olup 0,05'ten küçük olduğu için H_4 hipotezi kabul edilmiştir. Yani eğitim seviyesi ile Instagram'da geçirilen zaman arasında ilişki vardır. Lise ve lise seviyesinin altındaki katılımcıların Instagram'da daha fazla zaman geçirdiği görülmektedir.

Tablo 5: Eğitim Seviyesi ve Instagram'da geçirilen zaman

	Lise ve altı		Lisans ve üzeri					
	Adet	**Beklenen**	**Adet**	**Beklenen**	**Pearson**	**Sig.2**	**φ**	**Sig.**
1 saatten az	24	31,90	75	67,1	4,498	0,034	,45	0,022
1 saat ve üzeri	67	59,1	116	123,9				

H_5: Eğitim seviyesi ile Instagram'da takip edilen alan arasında kısmen ilişki vardır.

Tablo 6'ya bakıldığında tüm Sig.2 değerleri 0,05'ten küçük olduğu için H_5 hipotezi kabul edilmiştir. Yani eğitim seviyesi ile Instagram'da takip edilen zaman arasında ilişki vardır. Eğitim seviyelerine göre takip edilen alanlara bakıldığında eğitim seviyesi düşük olan katılımcıların "Makyaj" alanını daha fazla takip ettiği, eğitim seviyesi yüksek olan katılımcıların ise "Sağlıklı Yaşam" ve "Gezi" alanlarını daha fazla takip ettiği görülmektedir.

Tablo 6: Eğitim Seviyesi ve Takip Edilen Alan

	Lise ve altı		Lisans ve üzeri					
	Adet	**Beklenen**	**Adet**	**Beklenen**	**Pearson**	**Sig.2**	**φ**	**Sig.**
Makyaj	40	31,0	56	65,0	5,881	0,015	0,022	0,011
Sağlıklı Yaşam	20	27,8	66	58,2	4,600	0,032	0,038	0,021
Gezi	29	44,5	109	93,5	15,663	0,000	0,000	0,000

H_6: Instagram'da geçirilen zaman ile son bir yılda Instagram'da Influencer'lar tarafından tanıtılan bir ürünü satın alma arasında bir ilişki vardır.

Tablo 7'ye bakıldığında Sig.2 değeri 0,021 olup 0,05'ten küçük olduğu için H_6 hipotezi kabul edilmiştir. Yani Instagram'da geçirilen zaman ile son bir yılda Instagram'da Influencer'lar tarafından tanıtılan bir ürünü satın alma arasında ilişki vardır. Instagram'da 1 saat ve üzerinde vakit geçirenlerin daha fazla ürün satın aldığı görülmektedir.

Tablo 7: Zaman ve Satın Alma

	1 saatten az		1 saat ve üzeri					
	Adet	**Beklenen**	**Adet**	**Beklenen**	**Pearson**	**Sig.2**	**φ**	**Sig.**
Satın Alma	9	15,8	36	29,2	5,363	0,021	0,026	0,014

4.3.Cronbach Alpha Güvenilirlik Testine Ait Bulgular

Cronbach alpha güvenilirlik testi, likert ölçeği ile hazırlanan soruların cevaplarının tutarlılığını ölçmek için kullanılmıştır. Ölçek; 0,00 ile 0,40 arasında ise güvenli değil, 0,40 ile 0,60

arasında ise güvenilirliği düşük, 0,60 ile 0,80 arasında ise oldukça güvenilir ve 0,80 ile 1,00 arasında ise güvenilirliği yüksek olarak kabul edilmektedir (Yıldız ve Uzunsakal, 2018).

Tablo 8'de katılımcıların; "Instagram'da Influencer'ları takip etme sebepleri", "Tüketici satın alma kararına ilişkin değerlendirmeler" ve "Instagram'da Influencer'lara duyulan güven" ile ilgili 5'li likert ölçeği ile oluşturulan altışar soruya verilen yanıtlara dair Cronbach alpha güvenilirlik testi bulguları yer almaktadır. Buna göre sırasıyla 0,826, 0,892 ve 0,951 değerlerine göre bu sorulara verilen yanıtların iç tutarlılığı yüksektir.

Tablo 8: Güvenilirlik testi bulguları

	Cronbach's Alpha	N
Instagram'daki Influencer'ları Takip Etme Sebepleri	,826	6
Tüketici Satın Alma Kararına İlişkin Değerlendirmeler	,892	6
Instagram'da Influencer'lara Duyulan Güven	,951	6

4.4.t-Testine Ait Bulgular

Bağımsız gruplar için t-testleri normal dağılıma sahip iki grup arasında anlamlı bir fark olup olmadığını öğrenmek için yapılmıştır ve buna göre güvenirlilik 0,05'ten büyük ise iki grup arasında anlamlı bir farkılılık olmadığı sonucu elde edilir (Yazıcıoğlu ve Erdoğan, 2004). Bu bölümde cinsiyet-Influencer takip etme ilişkisi, cinsiyet-tüketici satın alma kararları değerlendirmesi ve eğitim seviyesi-Influencer'lara duyulan güven ile ilgili test bulgularına yer verilmiştir.

H_7: Cinsiyete göre Influencer'ları takip etme sebepleri farklılık göstermektedir.

Varyansların eşit olmadığı ihtimaline dayanarak Tablo 9'a bakıldığında Sig değeri 0,005 olup 0,05'ten küçük olduğu için gruplar arasında anlamlı bir farklılık olduğu görülmektedir. Katılımcıların, kendilerini takip ettikleri kişi ile özdeşleştirip, onu takip etme sebepleri açısından cinsiyetlere göre anlamlı farklılık göstermektedir. İki grup arasında ortalamalara bakıldığında kadınların ortalaması 3,4241'dir.

Tablo 9: Cinsiyet-Takip Etme Sebebi

Grup	N	Ortalama	Standart Sapma	t	Serbestlik derecesi	Sig
Erkek	93	3,055555556	1,113523950241608	-3,278	280	,001
Kadın	189	3,424162257	,752936305350887	-2,884	134,716	,005

H_8: Cinsiyete göre ile tüketici satın alma kararları farklılık göstermektedir.

Varyansların eşit olduğu ihtimaline dayanarak Tablo 10'a bakıldığında Sig değeri 0,012 olup 0,05'ten küçük olduğu için gruplar arasında anlamlı bir farklılık olduğu görülmektedir. Katılımcıların satın alma kararlarını verirken Instagram'dan etkilenmeleri, cinsiyetlere göre anlamlı farklılık göstermektedir. İki grup arasında ortalamalara bakıldığında kadınların ortalaması 3,2495'tir.

Tablo 10: Cinsiyet-Satın Alma Kararı

Grup	N	Ortalama	Standart Sapma	t	Serbestlik derecesi	Sig
Erkek	93	2,931899641577060	1,075146478937344	-2,544	280	,012
Kadın	189	3,249559082892417	,939138534794917	-2,429	162,819	,016

H_9: Eğitim seviyelerine göre Influencer'lara duyulan güven farklılık göstermektedir.

Varyansların eşit olduğu ihtimaline dayanarak Tablo 11'e bakıldığında Sig değeri 0,031 olup 0,05'ten küçük olduğu için gruplar arasında anlamlı bir farklılık olduğu görülmektedir. Katılımcıların Influencer'lara duydukları güven, eğitim seviyelerine göre anlamlı farklılık göstermektedir. İki grup arasında ortalamalara bakıldığında eğitim seviyesi düşük olan katılımcıların ortalaması 3,020'dır.

Tablo 11: Eğitim Seviyesi-Inflencerlara Duyulan Güven

Grup	N	Ortalama	Standart Sapma	t	Serbestlik derecesi	Sig
Lise ve altı	91	3,020146520146520	1,141213120193033	2,168	280	,031
Lisans ve üzeri	191	2,713787085514834	1,093891397496364	2,136	170,559	,034

5. TARTIŞMA & SONUÇ

Tanımlayıcı istatistik yöntemleri ile demografik özellikler, internet ve Instagram kullanım alışkanlıkları analiz edilmiştir. Yapılan analizler incelendiğinde, katılımcıların büyük bir çoğunluğunun kadınlardan ve 18-24 yaş arası kişilerden oluştuğu görülmüştür. Katılımcıların %67,7'si, lisans ve üzeri eğitim almış, eğitim seviyesi yüksek kişilerden oluşmaktadır. Katılımcıların internet ve Instagram kullanım alışkanlıklarına bakıldığında ise %55,7'sinin gün içerisinde 3 saat ve üzeri internette vakit geçirdiği görülmüştür. Bu kişilerin %64,9'u gün içerisinde 1 saat ve üzeri Instagram'da vakit geçirirken, %68,8'inin 3 yıldan fazla bir süredir Instagram hesabına sahip oldukları anlaşılmıştır. Çıkan bir başka sonuç, katılımcıların son 1 yılda, Instagram'da Influencer'lar tarafından tanıtılan bir ürünü %16 oranında satın aldıklarıdır. Bu veriler, anket katılımcılarının günlük yaşantısında aktif bir şekilde internet ve Instagram kullandığını göstermektedir.

Katılımcıların demografik özellikleri üzerinden Instagram karakteristikleri incelendiğinde öncelikli olarak görülen, kişinin cinsiyeti ile takip edilen alanlar arasında anlamlı farklılık olduğu olmuştur. Buna göre kadınlar; moda, makyaj/güzellik, sağlıklı yaşam, kitaplar/dergi alanlarını takip ederken erkekler daha çok teknoloji ve spor alanlarıyla ilgilenmektedir. Bir başka sonuca göreyse takipçinin yaşı ile Instagram'da geçirdiği zaman arasında anlamlı bir ilişki vardır. Yaşı küçük olanlar Instagram'da daha fazla zaman geçirirken yaşı büyük olanlar daha az geçirmektedirler; bu da küçük olanların teknolojinin içine doğmuş olmaları ve Instagram ile çok daha küçük yaşlarda tanışmış olmalarıyla açıklanabilir. Eğitim seviyeleri açısından yapılan incelemedeyse lise ve lise seviyesinin altındaki katılımcıların Instagram'da daha fazla zaman geçirdiği görülmektedir; bu sonuç lise seviyesindeki kişilerin genelde daha genç oldukları göz önüne alındığında bir önceki sonuçla uyumludur. Eğitim seviyelerine göre takip edilen alanlara bakıldığında ise eğitim seviyesi düşük olan katılımcıların "Makyaj" alanını daha fazla takip ettiği, eğitim seviyesi yüksek olan

katılımcıların ise "Sağlıklı Yaşam" ve "Gezi" alanlarını daha fazla takip ettiği görülmektedir. Buradan eğitim seviyesi yükseldikçe kişilerin bedenin dışından çok bedenin içiyle ilgilendikleri sonucu çıkarılabilir.

Yapılan t-testi ile cinsiyet ve eğitim seviyesine göre gruplar arasında fark olup olmadığı incelenmiştir. Çıkan bulgular cinsiyet ile Influencer'ları takip etme sebepleri arasında anlamlı bir farklılık olduğu sonucunu göstermektedir. Buna göre kadınlar takip ettikleri Influencer'lar sayesinde erkeklere göre kendilerini daha pozitif hissetmektedirler. Bir başka deyişle Influencer'ları takip etmek kadınları erkeklere göre daha olumlu etkilemektedir. Çıkan bir başka sonuç ise katılımcıların kendi eğitim seviyelerinin, Influencer'lara duydukları güven seviyesini etkilediğidir. Buna göre eğitim seviyesi "lise ve altı" olan grup "lisans ve üzeri" olan gruba göre Influencer'lara daha fazla güvenmektedir.

Katılımcıların satın alma ile ilgili kararları ile ilgili olarak yapılan analizlere bakıldığında önemli sonuçlara ulaşılmıştır. Bunlardan ilkine göre takipçinin cinsiyeti ile son bir yılda Instagram'da Influencer tarafından tanıtılan bir ürünü satın alma arasında anlamlı bir ilişki bulunmaktadır. Tam olarak ifade etmek gerekirse, kadınlar son bir yılda Instagram'da Influencer'lar tarafından tanıtılan ürünleri erkeklere göre daha fazla satın almıştır. Bu da Instagram'da kadınlara yönelik yapılan reklam faaliyetlerinin erkeklere göre daha etkili olabileceğini göstermektedir. Ulaşılan bir diğer sonuç ise takipçinin Instagram'da geçirdiği zaman ile son bir yılda Instagram'da Influencer tarafından tanıtılan bir ürünü satın alması arasında anlamlı bir ilişki olduğudur zira Instagram'da bir saat ve üzerinde vakit geçiren bireylerin daha fazla ürün satın aldığı görülmektedir. Diğer bulgulara bakıldığında kadınların erkeklere göre daha fazla alışveriş yapmış olduğu görülmektedir. Satın alma kararı ile ilgili yapılan t-testi sonuçlarına göre ise katılımcıların satın alma kararlarını verirken Instagram'dan etkilenmelerinin, cinsiyetlere göre anlamlı farklılık gösterdiği görülmüştür. Daha net bir ifadeyle kadınlar alışveriş kararlarında erkeklere göre Instagram'dan daha fazla etkilenmektedirler.

Bu çalışmadan elde edilen bulguların, sosyal medya üzerindeki satın alma davranışlarının incelenmesi adına faydalı olabileceği düşünülmektedir. İlerleyen çalışmalarda Instagram'ın diğer sosyal medya araçlarına göre tüketicilerin satın alma kararlarında daha etkili olup olmadığı, Influencer'ların fikirlerinin kişileri hangi alanlarda daha çok etkileyebileceği gibi konularda araştırma yapılabilir. Kişi sayısının arttırılması, yaş gruplarının çeşitlendirilmesi ve daha farklı eğitim seviyelerinden kişilerin çalışmaya katılması ile benzer bir çalışmanın tekrarlanabileceği düşünülmektedir.

KAYNAKÇA

Aktaş A.(2018). Nüfuz Pazarlamasında (Influencer Marketing) Kullanılan Mesaj ve Stratejilere Yönelik İçerik Analizi. Yüksek Lisans Tezi. Bahçeşehir Üniversitesi. İstanbul.

American Marketing Association (AMA). (2017). What is Marketing? — The Definition of Marketing. https://www.ama.org/the-definition-of-marketing-what-is-marketing/, (04.12.2019).

Aslan A., Ünlü D. (2016). "Instagram Fenomenleri ve Reklam İlişkisi: Instagram Fenomenlerinin Gözünden Bir Değerlendirme". Maltepe Üniversitesi İletişim Fakültesi Dergisi 3(2), 41-65.

Balasubramanıan, S.K. (1994). "Beyond Advertising and Publicity: Hybrid Messages and Public Policy Issues". Journal of Advertising 23(4), 29-46.

Interactive Advertising Bureau (IAB.) (2018). "Ifluencer Pazarlaması". www.iabturkiye.org/UploadFiles/Reports/inluencer762018162344.pdf, (04.12.2019).

Koçak, G. (2012). Bireylerin Sosyal Medya Kullanım Davranışlarının ve Motivasyonlarının Kullanımlar ve Doyumlar Yaklaşımı Bağlamında İncelenmesi: Eskişehir'de Bir Uygulama. Doktora Tezi. Anadolu Üniversitesi Sosyal Bilimler Enstitüsü. Eskişehir.

Marketingdersleri.Blogspot.Com. (2015). "Pazarlama Üzerine Araştırmalar: Pazarlama (Marketing) Nedir ?". http://marketingdersleri.blogspot.com/2015/04/pazarlama-marketing-nedir.html, (04.12.2019)

Mccracken G. (1989). "Who Is The Celebrity Endorser ? Cultural Foundations of the Endorsement Process". Journal of Consumer Research 16(3), 310-321.

Mert L. (2018) "Dijital Pazarlama Ekseninde Influencer Marketing Uygulamaları". Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi 6(2), 1299-1328.

Peltekoğlu, F , Tozlu, E . (2018). "Kurumsal Sosyal Sorumluluk Kampanyalarının Dijital Paydaşları" Sosyal Medya Fenomenleri. Erciyes İletişim Dergisi 5 (4) , 285-299.

Saltık Yaman, E. (2018). "Ürün Yerleştirmede Yeni Bir Alan: Influencer Marketing Sosyal Medyada Influencer Annelerin Takipçileri Tarafından Değerlendirilmesine Yönelik Bir Araştırma." 2. Uluslararası İletişimde Yeni Yönelimler Konferansı: Eğlence ve Ürün Yerleştirme, 268-279.

Sevinç, S. S. (2018). "Blogger, Influencer, Fenomen, Instagrammer, Youtuber, Celebrity Nedir? Ne İşe Yarar? Nasıl İstifade Edilir?", http://salihseckinsevinc.com/blogger-influencer-fenomen-instagrammer-youtuber-celebrity-nedir-ne-ise-yarar-nasil-istifade-edilir/, (04.12.2019).

Uzunsakal, E, Yıldız, D. (2018). "Alan Araştırmalarında Güvenilirlik Testlerinin Karşılaştırılması Ve Tarımsal Veriler Üzerine Bir Uygulama". *Uygulamalı Sosyal Bilimler Dergisi* 2(1), 14-28.

Yanar K., Yılmaz G. (2017). "Sosyal Medyanın Satın Alma Öncesi ve Sonrası Tüketici Davranışlarına Etkisi Üzerine Bir Araştırma". Yönetim, Ekonomi ve Pazarlama Araştırmaları Dergisi 1(2), 24-40.

Yavuzyılmaz O. (2015). "Ağızdan Ağıza Pazarlama". Akademik Sosyal Araştırmalar Dergisi (14), 429-448.

Yazıcıoğlu, Y. ve Erdoğan, S. (2004). SPSS Uygulamalı Bilimsel Araştırma Yöntemleri (1. bs.). Detay Yayıncılık, Ankara.

Yılmazsoy B. (2019). "Sosyal Ağların Pazarlama Üzerindeki Etkileri: Instagram Örneği". Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi 7(1), 49-58.