RUTİN AKTİVİTELER TEORİSİ BAĞLAMINDA DİJİTALLEŞEN DÜNYADA SİBER SUÇ MAĞDURLARI*

Serdal FİDAN**

Buket Cansu ULUDAĞ***

ÖZ

Soğuk Savaş döneminde ortaya çıkan internet ile birlikte dünya çapında büyük bir değişim ve dönüşüm süreci yaşanmaya başlanmıştır. İnternetin keşfinin getirdiği dijitalleşme ile birlikte küreselleşme hız kazanmış ve alışılagelmiş olan kültürel yapıların, rutin aktivitelerin, suç ve benzeri olguların da dijitale dönüşümüne yol açmıştır. Suç olgusunun sanal ortama taşınması, mağdurlarını da beraberinde getirmiştir. Bu araştırmada sanal ortama taşınan ve siber suç olarak tanımlanan suçlardan etkilenen mağdurların ortak yönleri araştırılmıştır. Aynı zamanda mağdurların belirli özelliklerinin mağduriyet yaşamalarında etkili olup olmadıkları da araştırılmıştır. Yapılan araştırmanın teorik zeminini Lawrance Cohen ve Marcus Felson'un üzerine çalışmış oldukları Rutin Aktiviteler Teorisi oluşturmaktadır. Araştırmanın mekansal sınırı olarak Bursa ili belirlenmiştir. Çalışma grubu, siber suç mağduriyeti yaşamış olan 20 kişiden oluşmaktadır. Mağdurların yaşadıkları süreci daha iyi anlayabilmek açısından nitel yöntemin tercih edilmiş olduğu bu araştırmada fenomenolojik yaklaşım esas alınmıştır. Araştırma verileri; ölçüt örnekleme tekniği ile belirlenmiş olan 20 katılımcıya yarı yapılandırılmış mülakat yapılarak elde edilmiştir. Elde edilen veriler betimsel analiz tekniği kullanılarak yorumlanmıştır. Bireylerin rutin internet kullanım alışkanlıklarının mağduriyet yaşamalarına sebebiyet vermekte olduğu sonucu elde edilmiştir.

Anahtar Kelimeler: Dijitalleşme, Suç, Siber Suç, Mağdur, Rutin Aktiviteler.

CYBERCRIME CASES IN A DIGITAL WORLD IN THE CONTEXT OF ROUTINE ACTIVITIES THEORY

ABSTRACT

With the internet that emerged during the Cold War period, a great change and transformation process began to be experienced around the world. With the digitalization brought about by the discovery of the Internet, globalization has accelerated and has led to the transformation of conventional cultural structures, routine activities, crime and similar phenomena into digital. The transfer of the crime phenomenon to the virtual environment has brought its victims with it. In this research, the common aspects of the victims who were transferred to the virtual environment and affected by the crimes defined as cybercrime were investigated. At the same time, it was also investigated whether certain characteristics of the victims were effective in experiencing victimization. The theoretical basis of the research is the Routine Activities Theory, which Lawrence Cohen and Marcus Felson have worked on. Bursa province was determined as the spatial limit of the research. The working group consists of 20 people who have been victims of cybercrime. In this research, in which the qualitative method was preferred in order to better understand the process experienced by the victims, the phenomenological approach was taken as the basis. Research data; It was obtained by conducting semi-structured in-depth interviews with 20 participants who were determined by criterion sampling technique. The data obtained were interpreted using the descriptive analysis technique. It has been concluded that the routine internet usage habits of individuals cause them to experience victimization.

Keywords: Digitalization, Crime, Cybercrime, Victim, Routine Activities.

---

* Bu çalışma Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Anabilim Dalında hazırlanmış olan "Dijital Dünyada Etkileşim Formları ve Siber Suç Mağdurları: Bursa İli Örneği" başlıklı yüksek lisans tezinden türetilmiştir.

** Karadeniz Teknik Üniversitesi Edebiyat Fakültesi Sosyoloji Bölümü, E-posta: serdalfidan@ktu.edu.tr, ORCID Numarası: 0000-0001-9862-6375

*** Yüksek Lisans Öğrencisi, Karadeniz Teknik Üniversitesi Edebiyat Fakültesi Sosyoloji Bölümü, E-posta: buketcns132@gmail.com, ORCID Numarası: 0000-0002-5029-4823

Atıf: FİDAN, S., ULUDAĞ, B. C. (2023). "Rutin Aktiviteler Teorisi Bağlamında Dijitalleşen Dünyada Siber Suç Mağdurları", *HABITUS Toplumbilim Dergisi*, (4), 175-210.
Citation: FİDAN, S., ULUDAĞ, B. C. (2023). "Cybercrime Cases In A Digital World In The Context Of Routine Activities Theory", *HABITUS Journal of Sociology*, (4), 175-210.
Başvuru / Received: 01 Mart 2023 / 01 March 2023
Kabul / Accepted: 22 Mart 2023 / 22 March 2023
Araştırma Makalesi / Research Article.

EXTENDED ABSTRACT

With the digitalization that brought by the discovery of the Internet, globalization has accelerated and led to the transformation of the usual cultural structures, routine activities, crime and similar phenomena into digital. The crime of bringing the crime into the virtual environment brought its victims with it. In this research, the common aspects of victims affected by crimes that have been moved to the virtual environment and defined as cybercrime have been investigated. At the same time, it has been investigated whether certain characteristics of victims are effective in experiencing victimization. The theoretical basis of the research is the Theory of routine activities, which Lawrence Cohen and Marcus Felson have worked on. Bursa or Bursa is determined as the spatial limit of the research. The study group consists of 20 people who have experienced cybercrime victimization. In this research, which qualitative method is preferred in order to better understand the process experienced by the victims, the phenomenological approach was taken as the basis. The research data was obtained by semi-structured interviews of 20 participants, which were determined by the criteria sampling technique. The data that obtained were interpreted using descriptive analysis technique. It has been concluded that the routine internet usage habits of individuals cause them to experience victimization.

With the evolving and changing technology, people have computers, smartphones, and so on it can interact in virtual environments where there are no jurisdictions over connected networks via objects and the internet. These networks, which are interconnected and provide a constant flow of information, are manifested as 'cyber space' and pave the way for cybercrime. The use of computers has increased due to the fact that they have decreased in size and appeal to everyone in terms of price, and the increase of traffic on the networks with the fact that smartphones can be connected to the internet has made it difficult to control the malicious uses.

Digitalization has brought many changes and transformations around the world. This new process has led to the digitalization of cultural, educational and criminal phenomena as well as daily routine activities. This situation brought with it the phenomenon of digitalized crime and caused the emergence of cyber crime victims. Since cybercrime is constantly self-

renewing and keeps up with technological developments, the measures taken are valid until a new cybercrime technique is developed. There is a building that can be built for everyone.

Cybercrime is defined as the actions that occur with the misuse of computers and the internet, carried out against computers, etc., or against individuals who are users. It is also defined as information crimes, but crimes committed with tools such as telephone are defined as cyber crimes.

After the second World War, the increase in crime rates has revealed the aim of preventing crimes. As a result, there was a divergence in the perspectives of investigating the source of the crime, and for the first time, the idea that the crime can be prevented by focusing on the mechanisms and elements of the crime Felson's theory of routine activities.

The theory of routine activities deals with the impact of the routine of individuals in their daily lives on the occurrence of crime and victimization. It is known that the theory is derived from Amos Hawley's "Theory of Human Ecology", which researches the effect of temporal factors, stating that human behavior does not differ only spatially in the environments in which communities exist. Therefore, it is stated that the reason why this theory is fundamentally different from other criminological theories is due to its origins.

In addition to this, in line with the data; it has been pointed out that there is a fear of stigmatization of cyber crime victims. This made it difficult to reach the participants during the interview process. There have been individuals who do not want to participate in an interview about the cybercrime victimization they have experienced. They thought that they would share. The participants had the same thought. They will be questioned and questioned for the duration of the trial. It was observed that because of these thoughts, participants did not share the victimization that they experienced with their surroundings. It turned out that not sharing with their environment caused them to be psychologically unable to get support and they were lacking in awareness about what to do for the struggle. It was also observed that the participants, who were afraid of hearing from their families and their surroundings, did not make any applications to the official institutions despite their financial losses.

As a result of the victimization that experienced by the participants, it was pointed out that there were inactions such as do not apply to official institutions and do not fight. It has emerged that the fear of being stigmatized has a negative effect on their legal pursuit of their rights. At the same time, as many of the participants heard from their surroundings, they did not think that they could get results even if they applied. The 5 participants who submitted the

application did not receive any results yet. In this case, it can be said that the participants experienced a secondary victimization during the struggle process. Therefore, there is a general perception that participants will not get a legal result. Since this common consciousness will also affect other cyber crime victims, awareness should be made about this issue.

In line with the data; in addition to the belief that there may be worse in the participants and that they were saved with their experiences, fatalism tendencies were observed. They will be treated as if they had suffered the loss of life. In fact, it turns out that they are trying to affirm the victimizations that occur as a result of their carelessness with the tendencies of polyanism and fatalism.

Despite the victimization, it has emerged that there are no significant changes in users' internet usage habits. Therefore, the fact that the routine internet usage habits that cause them to experience victimization do not change increases the likelihood of victimization for the second time. It has emerged that daily routine activities carried out via the Internet are directly related to cybercrime victimization. As a result, since participants experience victimization because of these routine activities, it can be inferred that the victim is the cause of the crime itself. It has been concluded that the role of the victim in cybercrime is an effective factor.

In line with the data obtained, the participants stated that as a solution proposal, the passwords of the user accounts should be strengthened and constantly updated, that they should be cautious against unknown sites and applications, that personal information and card information should not be shared anywhere or should be shared with care.

In general, the participants stated that should not be entered unknown sites on the Internet, which has a complex structure to protect against cyber crime victims, that cookies or permissions should not be accepted, that personal information or card information should not be shared. They commented on the need to pay attention to card information sharing, especially in internet shopping. On the other hand, it was stated that the virus program should be used and the passwords should be constantly updated by choosing strong. None of the participants commented on the reduction of internet usage time. They have made holistic interpretations on the main idea that the internet should be used because it is a part of everyday life, but they should be more careful. In addition, the legal struggle should not be ignored, the necessary applications should be made. The grievances experienced in terms of the development of cyber crime methods and process should not remain a dark number.

Cybercrime victimization is generally seen to be processed through social media accounts and it has been concluded that measures should be increased and users should be made aware of it. Today, it has been observed that victimizations have emerged in line with the desire to be seen and known by sharing information about individuals and themselves. In addition, the desire to make easy money leads to virtual investments or games of chance and leads to high losses. Especially in men, while such victimization is in question, there are moral victimizations or shopping-based victimizations in women. In relation to this, women's reservations about investment, cautious behavior and insecurities can be attributed to the reason, while men's desire to gain more prevails. In the male participants who have experienced victimization due to virtual investment, the behavior of continuing to make virtual investments through other sites has been observed. This situation is seen that every site is not reliable and they have an approach that does not bother to make virtual investments in reliable sites. In short, it has been concluded that the routine internet usage habits of individuals cause them to experience victimization.

GİRİŞ

Günümüzde her alanda karşılaşılmakta ve kullanılmakta olan internetin ortaya çıkışını, 1969 yılında Arpanet'in icat edilmesine dayandırabilmek mümkündür. Spesifik olarak; Amerika Birleşik Devletleri ve Sovyet Sosyalist Cumhuriyetler Birliği arasında ortaya çıkan Soğuk Savaş döneminin bir ürünü olduğu söylenebilir. İki ülke arasındaki askeri ve ideolojik bu rekabet; gizli, hızlı ve kesintisiz bir iletişim arayışı içerisine girilmesine sebep olarak internetin ortaya çıkmasına zemin hazırlamıştır. İlk olarak askeri haberleşme amacıyla kullanılmaya başlanmış olsa da zamanla önce akademi tarafından kullanılarak bilgi alışverişinde kolaylıklar sağlamış, daha sonra kullanımı genele yayılmıştır. Yaygın bir şekilde kullanılmaya başlaması 1991 yılında geliştirilen World Wide Web sayesinde mümkün hale gelmiştir (Akyeşilmen 2018: 25; Brenner 2010: 14-20). Doğal olarak internet kullanıcısı sayısı da artmıştır. Soğuk Savaş endişelerinin ve gerginliğinin uzaklaşmaya başladığı 1996 yılında, bireyler ya da gruplar tarafından; kişisel, bilimsel vb. her tür amaç ile kullanılan bilgisayar ağ sayısı 20 milyona ulaşmış, yatay iletişimin ve dijitalleşmenin temel taşını oluşturmuştur (Castells 2008: 8).

Kavram olarak sayısallaştırma (digitization) ve dijitalleşme (digitalization) genel olarak literatürde birbirinin yerine kullanılmaktadır. Fakat aralarında analitik bir ayrım bulunmaktadır. Sayısallaştırma; özellikle bilgisayar aracılığıyla, elde bulunan verileri dijitalleştirmek amacıyla yapılan bir işlem olarak gerçekleşmektedir (Brennen ve Kreiss 2016: 1-2). Başka bir açıdan

bakıldığında; dijital teknoloji, kelimelere ya da harflere sayılar kadar ihtiyaç duymamaktadır (McLuhan 1994: 80).

Dijitalleşmenin gelişmesine paralel olarak bu süreç Dijital çağ; Bilgi çağı. Enformasyon çağı veya Post modern çağ olarak da ifade edilmekte olup, toplumların geçmişten günümüze kadar sahip oldukları bilgi birikimlerinin teknoloji aracılığıyla çoğaltılması ve paylaşılması ile karakterize edilmiş olan bir çağ olarak anılmaktadır. Dijital çağda yaşanmakta olan gelişmeler ile birlikte gündelik yaşam pratiklerinde, eğitimde, ekonomide ve hatta toplumların kültürlerinde bile farklılaşmalar meydana gelmiş bulunmaktadır (Sarıyar 2019: 20; İşliyen 2019: 408). İnternet teknolojisi yazılı, görsel ve işitsel kültürü aynı sistem içerisinde bütünleştirmesiyle birlikte iletişimin karakterini tümüyle değişime uğratmış bulunmaktadır. İletişimin de kültürü doğrudan doğruya şekillendirebilen bir yapıya sahip bulunmasından dolayı toplumlarda bir kültürel değişime sebep olması kaçınılmaz olmuştur. Kültürün yanı sıra dijitalleşme, birçok olgunun değişim ve dönüşümünde etkili bir faktör olarak yer almıştır (Castells 2008: 440).

Dijital Çağda Suçun Dönüşümü

Siber Suçlar

Dünyanın her yerinde insanlar bir araya gelerek toplumları oluşturmaktadır. Bir arada ve düzen içerisinde yaşayabilmek için ise ortak değerler temelinde kural ve normlara ihtiyaç duyulmaktadır. Çünkü toplumsal düzen, bunu bozabilecek her türlü eylemi yasaklayan kurallar olmadan var olamamaktadır. Bu kural ve normlar; dinsel, hukuksal, geleneksel, ahlaki vb. birçok formda belirlenebilmektedir (Güçlü ve Akbaş 2016: 28-29; Brenner 2010: 9). Aynı zamanda bu normlar toplumdan topluma ve yaşanılan çağa göre değişim gösterebilmektedir. Dolayısıyla düzen içerisinde yaşamak isteyen her toplum, üyelerinin bu kurallara uymasını beklemektedir fakat zaman zaman ihlaller söz konusu olabilmektedir. Ortaya çıkan bu ihlaller 'sapma' olarak adlandırılmaktadır. Gerçekleşen sapkın davranış aynı zamanda toplumda yürürlükte olan ceza yasalarına da aykırı ise 'suç' olarak nitelendirilmektedir (Yüksel 2017: 4-5; İçli 2007: 1). Başka bir deyişle; kamusal otoritenin müdahale etmesini gerekli kılan, kanunen açıkça yasaklanmış olan ve cezai yaptırımı bulunan eylemler suç olarak, toplumsal kural ve normlara aykırı olan fakat hukuki alanda herhangi bir yasaklılığı ve yaptırımı bulunmayan eylemler ise sapma olarak ifade edilmektedir (Dolu 2012: 34). Bu durumda; gerçekleştirilen her sapkın davranış bir suç olarak nitelendirilememektedir fakat suç teşkil eden birçok eylem aynı zamanda sapma olarak da değerlendirilebilmektedir (Bal 2013: 14).

Kavram olarak suç, her ne kadar olumsuz bir nitelik taşıyor gibi gözükse de toplum için olumlu fonksiyonları da bulunmaktadır. Gerçekleştirilen eylemin bir suç olarak nitelendirilmesi ve cezalandırılması durumu toplumda var olan normların belirginleşmesine ve istenmedik davranışların gündeme gelerek fark edilmesine imkân vermektedir. Dolayısıyla bireyler bu istenmedik davranışları gerçekleştirmekten kaçınarak, kural ve normları benimsemeye özen göstermektedir. Bunun yanı sıra; toplumsal kurallara uymayan ve suçlu davranışlarda bulunan bireylere karşı gösterilen ortak tepkiler vb. nedeni ile suçun toplumsal dayanışmayı güçlendirdiği savunulmaktadır. Bu bağlamda bir toplum içerisinde işlenen suç türleri ve oranları, toplumsal yapı içerisindeki sorunların açığa çıkmasında yardımcı bir rol oynamaktadırlar (Güney 2008: 12; Kılıç 2007: 35).

Gelişen ve değişen teknoloji ile birlikte insanlar bilgisayar, akıllı telefon vb. nesneler ve internet aracılığı ile birbirine bağlı ağlar üzerinden yargı sınırlarının olmadığı sanal ortamlarda etkileşimde bulunabilmektedir. Birbirine bağlı olan ve sürekli bilgi akışını sağlayan bu ağlar 'siber uzay' olarak tezahür edilmekte ve siber suçların yolunu açmaktadır (Kundi ve Nawaz 2014: 3). Günümüzde gerçekleştirilen siber saldırıların birçoğu fiziksel dünyadaki suçların siber uzaya göçünü temsil etmektedir. Siber uzay, suçluların geleneksel suçları yeni yollar ile işlemek için kullanmaya başladıkları bir araç haline gelmiş bulunmaktadır (Brenner 2010: 10). Bilgisayarların boyut olarak küçülmüş olması ve fiyat olarak herkese hitap ediyor olması sebebi ile kullanımı artmış, akıllı telefonların da internete bağlanabiliyor oluşu ile birlikte ağlar üzerindeki trafiğin artışı kötü amaçlı kullanımların kontrolünü zorlaştırmıştır (Akdağ 2009: 22).

Siber suç; bilgisayarın ve internetin kötüye kullanılması ile birlikte ortaya çıkan, bilgisayara vb. araçlara karşı ya da kullanıcısı olan bireye karşı gerçekleştirilen eylemler olarak ifade edilmektedir. Bilişim suçları olarak da anılmakta fakat bilişim suçları telefon gibi araçlar ile işlenen suçları da içermesi ve daha kapsamlı olması sebebi ile internet ağları kullanılarak siber uzayda işlenen suçlar, siber suçlar olarak tanımlanmaktadır (Budak 2015: 5-6). Nasıl işleneceklerinin kolay öğrenilebilmesi, neden oldukları potansiyel zarara kıyasla daha az kaynak gerektirmeleri, fiziksel olarak bir ortamda bulunmadan işlenebilir olmaları ve yasalar ile açık ve net şekillerde yasaklanmayarak yasa dışı kabul edilmeyen noktalarının bulunması gibi faktörler ile fiziksel suçlardan farklılaşmaktadır (Kundi ve Nawaz 2014: 2; Özüdoğru 2010: 9). Bunun yanı sıra siber suçlar; işleniş biçimleri, görülme sıklığı, karşılığında uygulanan yaptırım oranları vb. faktörler açısından farklılık gösterse de ulusal ve uluslararası ortak bir sorun olarak değerlendirilmektedir (Smith vd. 2015: 3). Siber suçlar, herhangi bir demiryolunun durdurulabilmesine, yanlış sinyaller ile uçak ve tren gibi araçların yönlendirilebilmesine, bir

ülke için önemli olan politik, askeri, ekonomik vb. verilerin başkalarının eline geçebilmesine sebep olabilmektedir. Aynı zamanda her türlü e-medya üzerinde yanlış bilgiler verilebilmesine ya da gizli bilgilerin yayılabilmesine, hedef alınan sistemlerin saniyeler içerisinde çökebilmesine de sebep olabilecekleri için geleneksel suçlara oranla daha büyük zararlara da yol açabilmektedirler (Das ve Nayak 2013: 142). Örneğin; 20 Eylül 2001 yılında dünyanın en işlek sekizinci limanı olan Teksas'taki Houston Limanı'na bir siber saldırı düzenlenmiş ve sistem çökertilerek, gemilerin giriş çıkışından demirlemesine kadar tüm süreci barındıran veri tabanlarına erişim engellenmiştir. Saldırıyı başlatan bilgisayarın İnternet Protokolü (IP) adresi belirlenerek saldırganın adresi bulunmuş, hedefinin aslında bir başka ülkedeki bilgisayar sistemi olduğu gerçeği ortaya çıkmıştır. Saldırı sonucunda çözümsüz problemler ortaya çıkmamış olsa da sistemdeki güvenlik açıklarını kapatmak gerekliliğini göstermiştir (Brenner 2010: 104-106).

Tüm siber suçlar hem bilgisayar, akıllı telefon vb. araçları hem de kullanan kişiyi mağdur olarak içermektedir. Bu durum hangisinin ana hedef olduğuna bağlı olarak değişmektedir. Hedef birey olduğunda bilgisayar gibi teknolojik aletler hedefe ulaşmak için kullanılan bir araç niteliği taşımaktadır. Bu tarz siber suçlar genellikle daha az teknik bilgi gerektirmektedir çünkü verilen zarar daha çok psikolojik ve soyut olmaktadır. Suçlu kişi tarafından elde edilen bilgiler doğrultusunda bireylerin zayıflıkları ve veri mahremiyetleri istismar edilmektedir. Öte yandan bilgisayar benzeri aletlerin hedef olarak seçilmesi durumu ise teknik bilgi gerektirmektedir ve bu suçlar bilgisayar ve internetin ortaya çıkması ile birlikte varlık kazandıkları için diğerlerine oranla yeni kabul edilmektedir. Günümüzde internetin hayatın bir parçası haline gelmiş olması bu tarz suçların her gün ve sayısızca işlenmesine fırsat vermiş bulunmaktadır (Dashora 2011: 241).

Geleneksel suçlarda, işlenecek her suç türü için farklı araçlar ve ortamlar gerekmekte olsa da siber suçlarda failin internete bağlı bir bilgisayarının olması yeterli görülmektedir (Brenner 2010: 170). Bunun yanı sıra geleneksel suçlar ve siber suçlar arasındaki farklılıklar belirtilecek olunduğunda; öncelikle siber suçların kapsamını belirlemenin ve bir çerçevesini oluşturabilmenin teknolojinin sürekli gelişmeye devam etmesi sebebi ile daha güç olduğu ifade edilebilmekte, teknik bilgi gerektirmektedir (Ermeydan 2018: 11). Anlık, zaman ve mekân kavramlarından bağımsız gerçekleştirilebilmektedirler. Dolayısıyla siber suçlara müdahale edebilmenin geleneksel suçlardan daha zor olduğu sonucuna varılabilmektedir. Geleneksel suç mağdurlarından farklı olarak siber suç mağdurlarında; çevrelerinin tepkisinden çekinmek, damgalanmaktan huzursuzluk duymak, çevresindekilerin güvenini zedelemekten korkmak,

güvenlik birimlerine ve ceza sistemine yeterince güvenmemek, kanunları bilmemek gibi nedenlerden ötürü şikâyetçi olmaktan kaçınmaları söz konusu olmaktadır. Siber suçların sadece bireyi ya da bir grubu etkiliyor olmasının yanı sıra bir toplumu tehdit edebilme potansiyelinin bulunması sebebi ile bu tarz suçların önlenmesinde kurumlar arası ve hatta uluslararası iş birliğinin gerekli olduğuna değinilmektedir (Akarslan 2011: 14-15; Peker 2010: 33).

Siber suçlarda delil toplama faaliyetlerinin fiziksel suçlara oranla daha zor olduğu kabul edilmektedir. Fiziksel suçlarda bir olay yeri bulunabiliyor olması delil toplama için bir mekân sunabilirken; siber suçların zaman ve mekândan bağımsız olması, sonuçlarının başka ülkedeki bireyleri ya da toplumu vb. etkileyebiliyor olması sebebi ile delil toplamayı zorlaştırmaktadır. Yasal boşlukların bulunması ve anonimlik oluşturabilmesi sebebi ile de bireyler siber suçlara yönelebilmektedir. Geliştirilen savunma önlemleri her geçen gün teknolojideki ilerlemeler sebebi ile ortaya çıkan yeni bir siber suç tekniği ile aşılabileceğinden dolayı, teknolojinin sürekli takibi ve savunmaların da teknik bilgiler ile sürekli güncellenmesi gerekmektedir (Taşçı ve Can 2015: 231).

Mağdur

Mağdur kavramı genel olarak; dolaylı ya da doğrudan olacak şekilde haksızlığa uğramış olan, zarar görmüş ya da acı çekmiş olan kişi şeklinde tanımlanabilmektedir (Katoğlu 2012: 658-660). Hukuki açıdan ise suçun pasif nesnesi olarak kabul edilmekte ve işlenen suç karşısında zarar gören suç kurbanı olarak tanımlanmaktadır (Akcan 2014: 3969). 20. yüzyıla kadar işlenen suçlarda genellikle faile odaklanılmış ve mağdur boyutu yeterince ele alınmamıştır. Suçu açıklamada mağdur kavramına da ilgi duyulmaya başlanması ve "20. yüzyılın son çeyreğinde Avrupa devletlerinde mağdur haklarının gelişmesi ile birlikte 01.06.2005 tarihinde yürürlüğe giren 5271 sayılı Ceza Muhakemesi Kanunu ile mağdur hakları hatırlanmış ve mağdur yönünden birçok yeni düzenleme hayata geçirilmiştir". Bunun yanı sıra "…aynı tarihte yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nda onarıcı adalet modelinin en önemli aktörü olan mağdurun haklarına önem verilerek birçok müessese mevzuata dahil edilmiştir". Böylelikle mağdur ve mağdur haklarına yönelik önemli adımlar atılmış olmaktadır (Aykara ve Özkan 2017: 145; Seçkin 2020: 621-622). Ayrıca, suç olgusu içerisinde unutulmuş ve yeterince önemsenmemiş aktör olan mağdur, eylemlerinin suç oluşumunu ve sonucunu etkilemesi dolayısıyla anahtar aktör niteliği kazanmıştır (Güngör 2019: 202; Wolhuter vd. 2009: 1-2).

20. yüzyılın sonlarında kriminolojinin alt dalı olan ve mağdurları sosyal, psikolojik, hukuki açılardan incelemekte olan 'Mağdur Bilim (Victimology)' in önem kazanmaya başladığı görülmektedir. Viktimoloji; mağduriyetin tekrarlanmaması, mağdur ve fail arasındaki ilişki, mağdurdun suç sonrasındaki problemleri ve hukuki hakları vb. başlıkları konu edinmektedir. Ortaya çıkan suç olgusunda öncelikli olarak mağdur ile fail arasındaki ilişkiyi ve mağdurun suç sonrası davranışlarını araştıran Viktimoloji, özellikle mağdurun suçun meydana gelmesindeki rolüne odaklanmaktadır (Sokullu Akıncı ve Dursun 2016: 5-6). Mağdurlar suçun ve suçlunun tespit edilmesinde önemli bir rol oynamakta; suç ile ilgili normal şartlarda elde edilmesi güç olan bilgilere ve delillere ulaşmayı kolaylaştırmaktadırlar (Polat ve Gül 2010: 1293-1294).

Çalışmanın ana konusu olan siber suç mağduriyeti bireyin; şahsi bilgisayarına yetkisiz erişim, izni ve bilgisi dahilinde olmadan bilgisayarına dosya eklenmesi, silinmesi ya da içeriklerin değiştirilmesi, kötü amaçlı yazılımların bulaşması sonucu veri kaybı, mahremiyet ihlali, kişisel verilerin ve kredi kartı vb. gizli bilgilerin sızdırılması sonucu yaşadığı maddi ve manevi kayıplar olarak tanımlanabilmektedir (Ngo 2011: 777). Gelişen teknolojinin olumlu etkilerinin yanı sıra beraberinde getirdiği; siber dolandırıcılık, siber zorbalık, sexting, nefret söylemi, çocuk pornografisi, mahremiyeti kötüye kullanma vb. siber suçların varlığı hayatın bir parçası olmuş durumdadır. İnternet teknolojisinin getirdiği yeniliklerin denetiminin yetersiz olması durumu mağduriyetler için temel oluşturmaktadır. Bu denetimsizlik, siber suç alanındaki hukuki boşluk ve internetin sağladığı anonimlik siber suç eylemleri gerçekleştirme potansiyeline sahip bireyler için zemin hazırlamaktadır (Karaca vd. 2021: 178-182).

Rutin Aktiviteler Teorisi

Suçun kaynağı ve nedenleri her çağda ve her toplumda çeşitli faktörlere odaklanılarak açıklanmaya çalışılmıştır. 1940'lı yıllardan öncesinde suç teorileri suçun kaynağını doğaüstü güçlerde, insan genetiğinde ve bireylerin cezadan kaçabilmek adına yaptıkları rasyonel tercihlerde aramışlardır. Fakat meydana gelen İkinci Dünya Savaşı'ndan sonra suç oranlarında artışların görülmeye başlanması, suçları önleyebilme amacını ortaya çıkarmış bulunmaktadır. Bunun sonucunda suçun kaynağını araştırmaya yönelik bakış açılarında bir farklılaşma meydana gelmiş ve ilk kez suçun işlenme mekanizması ile unsurları üzerinde durularak, suç olgusunun engellenebileceğine dair düşünceler Lawrance Cohen ve Marcus Felson'un yaptıkları bir çalışmada 'Rutin Aktiviteler Teorisi' ile savunulmuştur (Birceviz 2019: 25; Ngo ve Paternoster 2011: 775-776).

Rutin aktiviteler teorisi bireylerin gündelik yaşamlarındaki rutinlerinin suçun ve mağduriyetin oluşumuna olan etkisini konu edinmektedir (Cohen ve Felson 1979: 32-33; Yar 2005: 412). Teorinin; toplulukların bulundukları ortamlarda insan davranışlarının yalnızca mekansal olarak farklılıklar göstermediğini belirterek, zamansal faktörlerin etkisini araştıran Amos Hawley'in "İnsan Ekolojisi Teorisi"nden türemiş olduğu bilinmektedir (Branic 2016: 1). Dolayısıyla bu teorinin diğer kriminolojik teorilerden temelde farklı olmasının sebebinin kökenlerinden kaynaklı olduğu ifade edilmektedir. Çünkü daha önceki teorilerin hiçbirinde zaman faktörünün suça etki eden bir olgu olduğu kabul edilmemiştir. Rutin aktiviteler teorisi ise suçun mekân ile ilişkisinin yanına zaman faktörünü de ekleyerek daha kapsamlı bir açıdan incelenebilmesine olanak sağlamış bulunmaktadır (Clarke ve Felson 2008: 3). Sonuç olarak suç olgusunu her açıdan ele alabilmek ve açıklayabilmek amacıyla suçun tam olarak nasıl, nerede ve ne zaman meydana geldiğine odaklanmaktadır (Felson ve Eckert 2018: 17).

Rutin aktiviteler teorisine göre; suç oranlarını etkileyebilecek doğrudan ve temaslı bir suçun oluşabilmesi için üç asgari unsur bulunmaktadır. Bunlar; güdülenmiş yani motive olmuş bir suçlunun varlığı, uygun hedeflerin bulunması ve suça karşı yeterli ya da yetenekli koruyucuların bulunmaması olarak ifade edilmektedir (Cohen ve Felson 1979: 589; Clevenger vd. 2018: 37-38). Aynı zamanda teori, karşısına çıkacak en uygun fırsatları değerlendirmek için bekleyen potansiyel suçlunun varlığını peşinen kabul etmesi yönüyle de diğer teorilerden farklılaşmaktadır (Dolu 2012: 129). Potansiyel suçlu, herhangi bir nedenle motive olmuş ve suç işleyebilecek herhangi birisidir dolayısıyla işlemesi muhtemel suç için kendisine kişi veya nesne olarak bir hedef belirlemektedir. Yeterli koruyucuların bulunmaması durumunda ise suçlu eylemini gerçekleştirebilmekte ve mağduriyet durumu ortaya çıkmaktadır (Clarke ve Felson 2008: 1-3). Bu üç unsurun bir araya gelmesi ile suçun ortaya çıkması muhtemel olduğu gibi, herhangi birinin eksikliğinin ise suçun oluşumunu engelleyebileceği ifade edilmektedir (Branic 2016: 1-2). Felson; teorideki suçun oluşumu için gerekli olarak belirtilen üç asgari unsurun suçluları motive eden şeylerin neler olduğunu, suçluların herhangi bir şekilde engelleyebilecek faktörlerin olup olmadığını tam olarak açıklayamadıklarından dolayı yetersiz kaldıklarını düşünmüştür. Bu sebeple suçluların eylemlerini gerçekleştirmelerini önleyebilecek olan koruyucuların olması dışında kalan engelleyici faktörlere odaklanarak 'tutucular' adı altında dördüncü bir unsur eklenmesi gerektiğini savunmuştur (Dolu 2009: 12).

Ortaya çıkışından bir süre sonra rutin aktiviteler teorisinin genellikle sokak suçlarını açıklamada daha başarılı olduğu fakat nicel araştırmalarda kesin bir suç mekanizması ve sonuç ortaya koyamayabileceği düşünülmüş ve diğer suçların da açıklanabilmesi amacıyla 'Fırsatlar

Teorisi' ile bağdaştırılarak açıklama gücü yüksek bir model geliştirilmeye çalışılmıştır. Bunun yanı sıra, teorinin kapsamını genişletebilmek bağlamında 'Rasyonel Tercihler Teorisi' ile de bütünleştirilmesi amaçlanmıştır. Böylelikle, geliştirilen teori daha geniş alanda suçların açıklanabilmesine imkân vermiş bulunmaktadır (Birceviz 2019: 25-26).

Bulgular

Katılımcıların Özellikleri ve İnternet Kullanım Alışkanlıkları

Araştırma kapsamında, etik kurul ve valilik izinleri çerçevesinde Bursa ilinde ikamet eden 20 siber suç mağduru ile yarı yapılandırılmış mülakat gerçekleştirilmiştir. Katılımcılara ilk olarak kendilerinden bahsetmeleri ve ikinci soru olarak günlük internet kullanım sıklıkları ile amaçları sorulmuştur. Verilen cevaplar çerçevesinde katılımcıların özelliklerinin yer aldığı tablo oluşturulmuştur.

Tablo 1: Siber Suç Mağduru Katılımcı Özellikleri

KATILIMCI	CİNSİYET	YAŞ	EĞİTİM DURUMU	MESLEK	GÜNLÜK İNTERNET KULLANIM SÜRESİ
K1	Erkek	25	Lisans	Yazılım Geliştirme Uzmanı	5 saat ve üzeri
K2	Erkek	40	Ön Lisans	Bilgi İşlem Birimi Müdürü	5 saat ve üzeri
K3	Kadın	38	İlköğretim	Ev Hanımı	2 saatten az
K4	Kadın	32	Lise	İşçi	5 saat ve üzeri
K5	Erkek	28	Lisans	Donanım Uzmanı	5 saat ve üzeri
K6	Kadın	40	Ön Lisans	Muhasebeci	5 saat ve üzeri
K7	Kadın	26	Lisans	Hemşire	2 ile 5 arası
K8	Erkek	30	İlkokul	İşçi	5 saat ve üzeri
K9	Erkek	30	Ön Lisans	Teknisyen	5 saat ve üzeri
K10	Erkek	27	Lisans	Askeri Personel	2 ile 5 arası
K11	Erkek	30	Lisans	Öğretmen	2 ile 5 arası
K12	Kadın	26	Lisans	Hemşire	2 ile 5 arası
K13	Kadın	24	Lisans	Hemşire	5 saat ve üzeri
K14	Kadın	23	Ortaokul	İşçi	5 saat ve üzeri
K15	Kadın	29	Lisans	Yazılım Geliştirme Uzmanı	5 saat ve üzeri
K16	Erkek	37	Lise	İşçi	5 saat ve üzeri
K17	Erkek	33	Lisans	Polis memuru	5 saat ve üzeri
K18	Kadın	27	Lisans	Mimar	5 saat ve üzeri
K19	Erkek	37	Yüksek Lisans	Yönetici	5 saat ve üzeri
K20	Kadın	34	Lisans	Öğretmen	5 saat ve üzeri

Katılımcılar arasında ortaokul, lise, ön lisans, lisans ve yüksek lisans mezunları bulunmaktadır. Katılımcıların eğitim durumları incelendiğinde; siber suç mağduriyeti yaşamanın eğitim durumu ile bağdaştırılamayacağı söylenebilmektedir. Bu durum siber suç tekniklerinin eğitim düzeyi fark etmeksizin herkese hitap eden yapılarının olduğunun bir

göstergesi olarak kabul edilebilir. Katılımcıların mesleki farklılıkları incelendiğinde; diğer katılımcılara oranla siber suçların teknikleri hakkında daha fazla bilgi sahibi olan yazılım geliştirme uzmanlarının dahi siber suç mağduriyeti yaşamış oldukları göze çarpmaktadır. Dolayısı ile siber suç mağduriyeti yaşama potansiyelinin meslek ile ilişkilendirilemeyeceği yorumu yapılabilmektedir. Rutin aktiviteler teorisi bu sebepler ile her bireyi potansiyel mağdur olarak kabul etmektedir, çünkü siber suçlar belirli özeliklere sahip olan bireylerde değil toplumun genelinde gözlemlenebilmektedir.

Elde edilen verilerden yola çıkılarak siber suç mağduriyeti yaşamanın cinsiyete dayalı olmadığına kanaat getirilmiştir. Kadın ve erkek katılımcılar arasında internet kullanım süresinde dikkate değer bir farklılık gözlemlenmemiştir. Süre çerçevesinden bakıldığında bir fark gözlemlenmemiş olsa da mülakat süreçleri dikkate alındığında kadın ve erkekler arasında internet kullanım amaçlarının değişkenlik gösterdiği saptanmıştır. Dolayısı ile cinsiyet faktörünün, mağduriyet yaşanan siber suç çeşidi üzerinde etkili olduğu sonucuna varılmıştır. Kısacası günlük internet kullanım süresindeki artışın mağduriyet potansiyelini genel olarak arttırdığı ve internet kullanım amaçlarındaki farklılıkların da mağduriyet çeşidini şekillendirdiği ortaya çıkmıştır.

Cinsiyete bağlı olarak internet kullanım sıklığı detaylı şekilde incelenecek olduğunda; erkek katılımcıların 8'i, kadın katılımcıların ise 7'sinin internet kullanım süresinin 5 saatin üzerinde olduğu görülmektedir. Kadınların erkeklere oranla internet kullanım sürelerinde neredeyse fark olmadığı belirtilebilir. Dolayısı ile katılımcıların %75'inin günün 5 saat ve üzerini internet kullanımı ile geçirdikleri ifade edilebilir. Bu durum internette geçirilen sürenin artmasının siber suç mağduriyeti yaşamada etkili bir faktör olduğu sonucunu içermektedir. Rutin aktiviteler teorisinin ele almış olduğu zaman faktörünün önemi siber suçlarda belirgin roldedir. İnternette geçirilen sürenin artması, dikkatsizce yapılabilecek tıklamalara zemin hazırlamaktadır. Geçirilen sürenin azalması ya da daha dikkatli internet kullanımı sonucunda mağduriyetlerde azalma görülebilir. Öte yandan; kullanım sürelerinde fark olmamasına rağmen kadın ve erkeklerin internet kullanım amaçlarındaki farklılıklar mülakat sorularına verdikleri cevaplardan daha net bir şekilde anlaşılabilmektedir.

> "Çalışma saatlerinde bilgisayar üzerinden kullanıyorum, çalışma saatleri dışında da ekstra yapmam gereken işlerim var ise yine bilgisayar üzerinden devam ediyorum. Onun dışında sosyal medya, film, dizi o tarz işler için de cep telefonumu kullanıyorum. E-ticaret kullanıyorum sıklıkla, alışveriş olarak kullanıyorum. Bir de geçtiğimiz aylarda bir bitcoin denemem olmuştu. Merak ettim girdim, cüzi bir miktar oynadım hevesimi aldıktan sonra da çıktım. Pek ilgimi çekmedi. Oyun için de kullanıyorum" (K1, 25, Yazılım geliştirme uzmanı).

> "2 ile 5 saat arası kullanırım. Sosyal medya kullanırım. Alışveriş yapıyorum evet alışveriş de yapıyorum hatta kripto işi de yapıyorum yani sanal para üzerinden şeyler yapıyorum. Oyun da oynuyorum yani internetin her şeyinden yararlanıyorum. Telefonu daha çok kullanıyorum" (K11, 30, Öğretmen).
>
> "İnterneti günlük olarak 5 saatten fazla yani kullandığım oluyor tabi. Yani artık kullanmayan yok zaten sosyal medyayı da biz de kullanıyoruz. Sosyal medyayı kullanıyorum genelde haberleri falan takip ediyorum ne olmuş ne bitmiş onları öğrenmek için takip ediyorum yani günlük olarak. Alışveriş için pek kullanmıyorum. Oyun oynuyorum telefonumda indirdiğim oyunlar var onları oynuyorum. Bitcoin için de kullanıyordum sanal yatırım olarak yani" (K16, 37, İşçi).
>
> "Genel olarak tabii ki sosyal medya için kullanıyorum herkes kadar ben de. Oyun pek oynamam aslında ama bazen kafamı dağıtmak için oynadığım oluyor. Günde 5 saatten fazla internet kullandığıma eminim tabi ama hiç ölçmemiştim, ölçeceğim. Sanal yatırım için kullanıyorum, günümüzün dijital parası ben kullanmayan olduğunu da düşünmüyorum var ise de yakın zamanda eminim herkes kullanacak zaten. Alışveriş pek yapmam aslında ama bazen yaptığım oluyor" (K19, 37, Yönetici).

Yukarıda verilen, erkek katılımcıların kullanım amaçlarını içeren yanıtlarının yanı sıra kadın katılımcıların yanıtları da aşağıdaki gibidir. İnternet kullanım amaçlarında farklılıklar bulunduğu kadar ortak amaçların da var olduğu göze çarpmaktadır.

> "Günlük ortalama 8 saat internet kullanıyorum. Bunun yaklaşık 2.5, 3 saate yakın kısmını iş amaçlı yani işim gereği kullanıyorum. Yaklaşık 1 saatini, bu 1 saatin üzerine hiç çıkmadı, sosyal medya için kullanıyorum. Bunun dışında sadece araştırma amaçlı. Çok alışveriş yapmayı sevmiyorum. Şöyle sevmiyorum; hani günümüz şartları gereği çok fazla dolandırıcılık, o tarz şeyler olduğu için çok fazla sevmiyorum. Ama yine de kullanıyorum. Hemen hemen şu anda vaktimin çoğunu, yani internet bazlı vaktimin çoğunu telefon üzerinden yapıyorum" (K6, 40, Muhasebeci).
>
> "Yani, işim gereği interneti aktif olarak kullanıyorum aslında. Bu sebeple günlük 5 saatten fazla kullandığımı söyleyebilirim. Hani genelde araştırma ve sosyal medya, internet alışverişi, youtube için kullanıyorum. Telefon ve bilgisayar ile internet erişimimi sağlıyorum" (K15, 29, Yazılım geliştirme uzmanı).
>
> "İnterneti günlük olarak 5 saatin üzerinde kullanıyorumdur. Sosyal medya ve alışveriş için zaten hepimiz kullanıyoruz artık. Dijital çağın getirilerinden biri bu diyebiliriz. Bunun yanında dizi ya da film izlemek için de kullanıyorum fakat genellikle vaktim araştırma ile geçiyor. Makale okumaları ve gündemin takibi gibi şeyler vaktimin çoğunu alıyor diyebilirim. Belki günde 8 saati bile buluyordur internet kullanımım" (K20, 34, Öğretmen).

Erkek katılımcılar interneti; sosyal medya, oyun ve sanal yatırım için daha çok kullandıklarını belirtmişlerdir. Kadın katılımcılar ise sosyal medya, alışveriş ve araştırma için daha çok kullandıklarını belirtmişlerdir. Kulanım amaçları farklılaşmış olsa da sosyal medya kullanımı tüm katılımcılarda ilk sırada yer almaktadır. K20 sosyal medya için "Zaten internet hatta sosyal medya artık resmen günümüzün uyuşturucusu gibi, telefonlarımızda sabah katlığımızda bile sosyal medya hesaplarımızı kontrol ediyoruz." yorumunda bulunmuştur. Ona göre internet ve sosyal medya günümüzde bağımlılık içeren bir alışkanlığa sebep olmuştur. Tüm katılımcıların sosyal medya kullanımı ve hatta sosyal medya hesapları üzerinden

mağduriyet yaşamış olmalarına rağmen kullanmaya devam eden katılımcıların bulunması günümüzde sosyal medyanın vazgeçilmesi zor bir alışkanlığa dönüştüğünün kanıtı olarak da değerlendirilebilir.

Genel olarak bakıldığında; internet kullanım amaçları arasında sosyal medya kullanımının, alışveriş amaçlı kullanımın ve sanal yatırım için kullanımın ilk üç amacı oluşturduğu görülmektedir. Sosyal medya kullanımı tüm katılımcılarda söz konusu iken alışveriş amaçlı kullanımın daha çok kadınlarda, sanal yatırım amaçlı kullanımın ise daha çok erkeklerde olduğu ifade edilebilmektedir. Dolayısı ile sosyal medya kaynaklı mağduriyetlerden sonra; kadınlarda alışveriş temelli mağduriyet, erkeklerde ise sanal yatırım temelli mağduriyetlere daha sık rastlanmaktadır.

Temkinli Olma ve Önlem Alma

Katılımcılara; internet üzerinden kendilerine ait ne tür bilgileri hakkında paylaşımlar yaptıkları, internet ve uygulama kullanımları sırasında talep edilen bilgileri paylaşırken dikkatli olup olmadıkları sorulmuştur. Katılımcıların tümü sosyal medya kullandığından fotoğraf ve video paylaşımlarında bulunduklarını dile getirmişlerdir. Katılımcıların %50'si herhangi bir web sitesi veya link aracılığı ile kendisinden bilgi talep edildiğinde doldururken dikkatli davrandığını, gerekli görmediği bilgileri paylaşmadıklarını iletmişlerdir. Telefona indirilen uygulamalarda ise talep edilen izinlere onay verirken dikkatli davrandığını katılımcıların sadece %45'i ifade etmiştir.

> "Tabi sosyal medyada fotoğraf falan paylaşıyoruz. Orda hani çok hani özel bilgimiz değil, yarı özel bilgileri paylaşıyoruz. Telefon numaramı paylaşıyorum. Kimlik bilgilerimi sosyal medyada paylaşmam, ona dikkat ediyorum. Son zamanlarda Whatsapp üzerinden bir kişisel bilgileri kullanım olayı çıkmıştı, orada da artık bir Whatsapp'ta da yazmamaya çalışıyoruz ama tabi unutuyoruz arada. Kaçırdığımız oluyor arada. Genelde uygulamayı o an kullanıp hemen faydalanma yönünde eğilim gösterdiğimiz için indirilen uygulamalarda istenen izinlere onlara pek dikkat etmiyoruz" (K2, 40, Bilgi işlem birimi müdürü).

> "Fotoğraf, video arada paylaşıyorum. Kimlik ve kredi kartı bilgilerimi, adres bilgilerimi paylaşmıyorum. Güvenlik önlemi açısından paylaşmıyorum. Bilmediğim uygulamaları kabul etmiyorum, onay vermem ama bildiğim uygulama, hani kullanmış olduğum daha önce güvenilirliğine emin olduğum uygulamalar için izin veriyorum ama onun dışında bilmediğim bir uygulamaya izin vermiyorum. Alışveriş yaptıktan sonra kartı internet alışverişine kapatıyorum" (K4, 32, İşçi).

> "Sosyal medya kullandığım için tabi illaki fotoğraf, video falan paylaşımlarım oluyor. Kimlik bilgilerimi paylaşmıyorum sadece. Onun dışında diğer bilgileri ister istemez paylaşıyoruz yani işte konumdur, kredi kartıdır, iletişimdir vs. paylaştığımız ya da işte kaydettiğimiz oluyor. Uygulamaları da zaten izin vermezsen kullanamıyorsun ki o yüzden hani gerçekten gerekli bir uygulama ise benim için, izinleri veriyorum çok da dikkat ettiğimi söyleyemem o konuda" (K9, 30, Teknisyen).

Katılımcıların sosyal medya kullanımında ve fotoğraf video gibi paylaşımlar yapmakta sorun görmedikleri sonucuna varılmıştır. Bunun yanı sıra kimlik ve kart bilgilerini paylaşma durumu söz konusu olduğunda daha dikkatli davrandıkları ve kendilerince birtakım önlemler almaya çalıştıkları gözlemlenmiştir. Akıllı telefonlara indirilen uygulamaların mikrofon, kamera, galeri, kişiler vb. özelliklere ve dosyalara erişim taleplerinde ise temkinli olmaya çalıştıkları dikkat çekmiş fakat indirilen uygulamalar, talep edilen izinler verilmediği taktirde çalışmadığı için kişisel bilgilerin paylaşımı ve erişimlerine onay vermek durumunda kaldıkları gözlemlenmiştir. Rutin aktiviteler teorisi çerçevesinden bakıldığında bu ve benzeri temkinsizlik içeren internet kullanım davranışları ile birlikte potansiyel mağdurun suçun oluşumuna zemin hazırladığı söylenebilir. Dolayısı ile suçun oluşumunda üçüncü unsur olarak potansiyel bir suçlunun da ortaya çıkması ile suç olgusu gerçekleşmektedir.

Katılımcıların verdikleri cevaplar incelendiğinde; K2 sosyal medya kullandığını ve fotoğraf paylaşımında bulunduğunu belirtmesinin yanı sıra kimlik bilgilerinin paylaşımında ise temkinli davrandığını dile getirmiştir. K4'te sosyal medya konusunda K2 ile benzer düşüncelere sahip olmasına rağmen farklı olarak kredi kartını internet üzerinden kullandığında önlem olarak işlem sonrasında kartını internet harcamalarına kapattığını beyan etmiştir. Aynı zamanda kimlik bilgilerini, adres bilgilerini ve kart bilgilerini paylaşmadığını ifade etmiştir. İndirdiği uygulamalarda ise daha önce kullanmış olup olmadığına, güvenilir olup olmadığına dikkat etmeye çalıştığını söylemiştir. Kart bilgilerini internet alışverişinde pratik olması sebebi ile internet tabanlı uygulamalarda kayıtlı tutmakta olduğunu bildiren K7, indirdiği uygulamalarda ise kullanımını zorunlu görmediğinde talep edilen izinleri onaylamadığını fakat izin vermediği takdirde uygulamaları kullanamadığı için bazı uygulamalarda onay vermek durumunda kaldığını ifade etmiştir. K9'da bu konuda K7 ile aynı fikirde olup, sadece kimlik bilgilerini paylaşmadığını fakat iletişim, adres, kredi kartı gibi bilgilerini paylaşmakta olduğunu iletmiştir. Tam tersi şekilde K15 ise izinler ve bilgi paylaşımı konusunda temkinli davrandığını, internet harcamalarını kendince bir önlem yöntemi olarak gördüğü sanal kart ile yapmakta olduğunu ve hatta günlük harcama limitinin bulunduğunu ifade ederek, akıllı telefonlara indirilen uygulamaların amacı dışında bilgilere ulaşmak istemesinin dikkat edilmesi gereken bir durum olduğunu savunmuştur. Son olarak K17'nin de K9 gibi kişisel bilgilerini ve kart bilgilerini paylaşmaktan çekinmediği göze çarpmaktadır.

Yapılan mülakatlarda katılımcılara dördüncü soru çerçevesinde; siber suç mağduriyeti yaşamadan önce çevrelerinde bu tarz mağduriyetlere şahit olup olmadıkları, siber suç hakkında daha önce herhangi bir bilgilerinin bulunup bulunmadığı ve bunun sonucunda herhangi bir

önlem alma eylemleri gerçekleştirip gerçekleştirmedikleri sorulmuştur. Üç katılımcı dışında diğer katılımcıların daha önce siber suçlar hakkında bilgi sahibi oldukları ve çevrelerinden de duydukları ifadelerine rastlanmıştır. Daha önce siber suçlar hakkında herhangi bir şey duymadıklarını belirten katılımcılar ise eğer duymuş olsalar ve konu hakkında biraz bilgileri olsa daha dikkatli olabileceklerini bildirmişlerdir.

> "Hayır, açıkçası daha önce iç duymamıştım. Çevremde de yaşanmamıştı bir benim başıma geldi. Ya gerçekten o kadar üzüldüm, çok üzüldüm… Ne yapacağımı ben de bilemedim. Daha önce duysam belki ne yapacağımı bilirdim. Bilgili birisi vardı çevremde bizi de o yönlendirdi yetkililere başvurmamız için yoksa siber suçlar diye bir birim olduğunu da öyle çok bilmiyordum" (K3, 38, Ev hanımı).

> "Ben yaşadım, ben yaşadığım için yaşamadan önce duymamıştım. Duymamıştım dediğim zaten üniversitedeydim. Üniversitede bundan 5 yıl önce bu kadar yaygın mıydı bilmiyorum ama daha yeni yeni yaygınlaştığı dönemdi herhalde bana denk geldi. Benden sonra duyduklarım oldu. Yani çevremden ilk ben tecrübe ettim. Benden sonra duydum yani. Duymadığım için önlem de alamamıştım" (K11, 30, Öğretmen).

Çevresinde siber suç mağduriyeti yaşanmadığını ve kendisinin başına geldiğinde de ne yapacağını bilemediğini ifade eden K3, ne kadar üzüldüğünü ve birileri kendisini yasal başvurular için yönlendirene dek siber suçlar ile ilgilenen ayrı bir birimin bile olduğunu bilmediğini dile getirmiştir. K10 ise 5 yıl önce siber suçların belki de şimdiki kadar yaygın olmadığı için duymamış olabileceğini ve duymuş olsa önlem almış olabileceğini iletmiştir. K14 ise "Ben bu olayı yaşamadan önce etrafımda böyle bir olay yaşayan olmadığı için herhangi bir önlem alma gereği de duymadım açıkçası" sözleri ile daha önce çevresinde bu tarz bir mağduriyet yaşayan kişiler bulunmadığını ve bu sebeple de önlem alma gereği duymamış olduğunu belirtmiştir. Bu sebeple yaşanılan mağduriyetlerin çevredekiler ile paylaşılması, bu ve benzeri durumlarda bireylerin çevrelerini bilinçlendirmesi gerektiği empoze edilmelidir. Durumsal Suç Önleme Yaklaşımı bağlamında değerlendirildiğinde; yaşanılan mağduriyetler konusunda çevrenin bilinçlendirilmesi potansiyel mağdur olan diğer internet kullanıcılarının temkinli davranmalarına ve rutin internet kullanım alışkanlıklarına etki edeceğinden, suç olgusunun oluşumunu engelleyebileceğinden ya da olasılığını düşürebileceğinden dolayı önem arz etmektedir. Öte yandan diğer katılımcılar ise daha önce çevrelerinde siber suç mağduriyetleri duymuş olmalarına rağmen önlem almadıklarını ya da kendileri yaşayana kadar önlemin ne kadar gerekli olduğunun farkına varmadıklarını dile getirmişlerdir.

> "Onunla ilgili şöyle; etrafımda kripto parası ile ilgilenen bir çevre var hemşire grubundan onların aracılığı ile duyduğum şey para kaybına yönelik. Nasıl oluyor bilmiyorum. Bayağı sıfıra inenler falan olmuş ama nasıl oluyor içeriğini bilmiyorum yani. Ben de kullanmadığım için önlem alma gereği de duymadım herhangi bir şeye karşı" (K12, 26, Hemşire).

> "Daha önce illa duyuyorduk zaten meslek gereği de mutlaka arkadaşlar söz ederken duyduğumuz oluyordu. Yani önlem, bilmiyorum hani şifreleri güçlü yapınca bir şey olmaz, önlem olur diye düşünüyorsun aslında. Ama tabi bu da tartışılır yani acaba gerçekten koruyucu mu diye. Daha da etkili önlemler almak gerekiyormuş demek ki" (K17, 33, Polis memuru).
>
> "Aslında daha önceden de duymuştum, sadece o an yakın çevrende olmadığı için mi desem önemsemediğin için mi desem önlem alma gereksinimi duymuyorsun. Önlem almamıştım ben de açıkçası. Çünkü yani bence önlem alsan da değişmiyor ki zaten. A şeklinde olmazsa B şeklinde mağduriyet yaşayabilirsin yine, bunun garantisi yok" (K18, 27, Mimar).

Katılımcıların verdikleri cevaplar incelendiğinde K12'nin kendisinin kullanmamakta olduğu sanal yatırım uygulamalarına istinaden siber suç mağduriyetlerini duyduğu fakat bu alanda herhangi bir işlem yapmamasından kaynaklı olarak önlem alma gereksinimi hissetmemiş olduğu göze çarpmaktadır. Benzer şekilde K16'nın da mağduriyet süreçleri hakkında çevresinden bilgi almış olduğu fakat önlem konusunda herhangi bir eylem gerçekleştirmemiş olduğu görülmektedir. Kullanıcı şifrelerini güçlü olarak oluşturmasının yeterli bir önlem olacağını düşündüğünü ileten K17 ise daha etkili önlemlerin alınması gerektiğine dikkat çekmiştir. Bunun yanı sıra K18 önlem alınsa dahi siber suç tekniklerindeki farklılıklardan dolayı farklı bir şekilde mağduriyet yaşanabileceğini savunmuştur. K19'un beyanı ise kendisinin başına gelmeyeceğini düşünmesi nedeniyle önlem alma gereksinimi duymadığı doğrultusunda olmuştur.

Genel olarak bakıldığında, internetin günlük yaşamı kolaylaştırmasından ötürü, katılımcıların rutin internet kullanım aktiviteleri sırasında temkinli olmadıkları ve dikkatli davranmadıkları sonucu çıkarılmıştır. Dolayısı ile uzun saatler internet kullanımı gerçekleştiren bireylerin temkinli olmaması durumu karşılaşılacak siber suçları ve mağduriyet olasılığını yükseltmektedir. Bunun yanı sıra günümüzde sıklıkla kullanılan kamuya açık internet erişim ağları da motive olmuş siber suçlular için fırsatlar doğurmaktadır. Rutin Aktiviteler Teorisi açısından, bu fırsatlar potansiyel suçluları motive etmekte ve diğer unsurların da hazır bulunması sebebi ile siber suç mağduriyeti oluşumuna sebep olmaktadır. Temkinli olunmaması durumunda, kamuya açık olan internet erişim ağları kişisel veriler için tehdit oluşturmaktadır. Birceviz (2019: 59) de yaptığı bir çalışmada kamuya açık internet erişim ağlarının kullanımının günlük rutin haline geldiğini ve bu ağlarda geçirilen vaktin artması ile siber suç mağduru olma riskinin artması arasında doğrudan bir ilişki olduğunu saptamıştır. Kamuya açık olan bu ağlara bağlanıldığında kart bilgileri, kimlik bilgileri gibi önem arz eden bilgilerin kullanılmaması gerektiği iletilmektedir.

Damgalanma Korkusu ve Mücadele Süreci

Toplumun hoş görmediği bir davranış sonucu damgalanma olgusu insanlık tarihi boyunca var olagelmiştir. Toplumdan topluma farklı şekillerde tezahürü mümkün olsa da bireylerde bir korku oluşturmuştur. Toplumdan dışlanacaklarını ya da damgalanacaklarını düşünen bireyler toplumun hoş görmediği eylemlerden kaçınmaya çalışmışlardır fakat bu elbette her zaman mümkün olamamaktadır. Damgalanma çekincesine istinaden katılımcılara yaşadıkları siber suç mağduriyetini çevreleri ile paylaşıp paylaşmadıkları, ilgili birimlere başvuruda bulunup bulunmadıkları sorulduğunda çoğunluğun cevabı damgalanmaktan çekindiklerine yönelik olmuştur. Günümüzde bu tarz suçlar ile mağdur olmak halk arasında cahillik, aptallık olarak nitelendirilmekte ve dikkatsizlik sonucu gibi algılanmakta olduğundan, mağduriyet yaşayan bireyler bu durumu çevreleri ile paylaşmakta çekince göstermektedir. Keza mülakatlar sırasında katılımcıların verdiği cevaplardan da damgalanma korkusunun ne kadar baskın olduğu gözlemlenmiştir. Bunun yanı sıra mülakat yapılmasını reddeden mağdurların ise birçoğunun yaşadığı mağduriyetin tekrar duyulmasından ve damgalanmaktan çekindiği için katılımcı olmak istemedikleri sonucuna varılmıştır. Katılımcıların ise verdiği cevaplardan damgalanma korkusunun mağduriyet süreçlerinde ne derece etkin bir faktör olduğu çıkarımı yapılabilir.

> "Kimse ile paylaşmadım, sadece ailem biliyor süreci birlikte yaşadığımız ve atlatmaya çalıştığımız için. Çünkü herkes "Sende mi inandın, nasıl dolandırıldın, bu kadar aptal olamazsın" gibi cümleler kuracaklardı eminim. Hiç dinlemek istemedim. Yaşayana kadar ben de böyle değerlendiriyordum. Yaşayınca görüyorsun hiç de öyle olmadığını aslında. Yadırgayacaklardı, eleştireceklerdi o yüzden paylaşmak istemedim" (K9, 30, Teknisyen).

> "Nasıl tarif edeyim ki yani öyle bir his yok tarif edebileceğim. Bir yandan korkuyorsun paran gitti diye. Bir yandan da üzgünsün, streslisin, endişelisin, çaresizsin de aslında. Kimseye de anlatamıyorsun falan zaten o çok kötü. Kendi kendine yiyip bitiriyorsun kendini ki nasıl çözeceğim bu işi diye" (K17, 33, Polis memuru).

> "Çevremden kimse ile paylaşmadım. Resmi kurum dışında ilk defa seninle paylaşıyorum diyebilirim. Yani öyle bir şey ki eşimle bile paylaşmadım. Bir damgalanma korkusu söz konusu evet. Çekince diyelim biz ona hatta. Kötü düşünüp, eleştirip kendi kendilerine yargılayacaklarından kimse ile paylaşmamayı seçtim" (K19, 37, Yönetici).

Yaşadıkları mağduriyet sürecini çevreleri ile paylaşmaktan çekinen katılımcılardan K4 karşılaştığı durumun kendisi ile özdeşleşmediğini, normal şartlarda bu tarz eylemlerde bulunmayan ve böyle bir mağduriyet yaşayabileceği düşünülmeyen birisi olması dolayısı ile çevresinin kendisini yargılayacağı düşünmüş olduğunu dile getirmek istemiştir. Yine aynı şekilde K8 de yadırganacağından koktuğu için çevresi ile paylaşmakta zorlandığını ifade etmiştir. K9 ise mağduriyet yaşamadan önce bu tarz durumları yadırgadığını fakat kendisi

yaşadıktan sonra bakış açısının değiştiğini belirtmiştir. K12 yaşadığı mağduriyeti paylaştığı taktirde kendisi ile dalga geçileceğini düşündüğü için paylaşmamış olduğunu söylemiştir. K13, kimse ile paylaşamadığı ve çevresinden duyulmasından çekindiği için resmî kurumlara da başvuru yapmamış olduğunu belirtmektedir. Resmi kurumda görev yapan K17'nin de yaşadığı durumu kimse ile paylaşmamayı seçtiği dikkat çekmektedir. K19'un ise statüsünden kaynaklı olarak damgalanma çekincesi olduğu gözlemlenmiştir. Sonuç olarak; damgalanma korkusunun mağduriyet sürecindeki mücadelede olumsuz etki eden bir role sahip olduğu görülmektedir. Bireylerin damgalanmaktan korktukları için mücadele girişiminde bulunmamalarının söz konusu olabileceği gözlemlenmiştir.

Öte yandan çevrelerini bilinçlendirmek amacı ile çekinmeden yaşadıkları mağduriyeti paylaşan katılımcılar da bulunmaktadır. Yazılım geliştirme uzmanı olan K1; "Çevremdeki herkes ile paylaştım onların da başına gelirse diye önlemlerini alsınlar diye. Tabi ki haliyle tekrar mağduriyet yaşama endişemiz var ama bu da artık hayatımızın bir parçası olduğunu düşünüyorum ben." sözleri ile yaşadığı mağduriyet sürecini çevresi ile paylaştığını ifade etmiştir. Bunun yanı sıra siber suçların ve getirdiği mağduriyetin artık günlük yaşamın bir parçası oldukları yorumunda bulunmuştur. Günlük yaşamda, dijitalleşme ile birlikte nasıl ki rutin aktiviteler ve alışıla gelmişlikler değişim ve dönüşüme uğradı ise aynı şekilde günlük yaşamın bir parçası olan suç olgusu da dijitalleşme ile yeniden üretilerek dijital çağdaki yeni yaşam pratiklerinin arasında gündelik hayatın bir parçası olmuştur. Benzer şekilde K2'de teknolojik olarak sürekli gelişimlerin söz konusu olduğu günümüzde siber suçların ve mağduriyetlerinin sürekli karşılaşacağımız bir durum olduğunu ve daha dikkatli olunması gerektiğini belirtmektedir. Siber suçlarda sürekli olarak yeni teknikler geliştirilmeye devam ettiği için bireylerin bilinçlendirilmesi gerektiğini ve önlem almaları gerektiğini ifade etmektedir.

> "Çevremle tabii ki paylaştım çünkü herkesi bilinçlendirmek lazım bu konuda. Önceden sadece virüs vardı virüs ile uğraşıyorduk, şimdi fidye çıktı. Daha neler çıkacak bilmiyoruz. Daha dikkatli olmaya mecburuz yani, bunu yapmaya mecburuz. Hani bu işte, bu işin nasıl emniyetini alıyorsak nasıl ki sunucularımızı kapalı bir odada tutuyorsak fiziksel olarak bir emniyetini alıyorsak, bu şekilde de almaya mecburuz yani" (K2, 40, Bilgi işlem müdürü).

Katılımcılara mağduriyet sürecinde resmî kurumlar ile mücadele edip etmedikleri, herhangi bir şikâyette bulunup bulunmadıkları sorulmuş; şikâyette bulunanların herhangi bir sonuç alamadıkları ve şikâyette bulunmayanların ise herhangi bir sonuç alamayacaklarını düşündükleri gözlemlenmiştir. Dolayısı ile bu durum akıllarda siber suç mağduriyetinde resmî kurumlara başvurmanın anlamsız olduğunu, resmî kurumların bu alanda yetersiz olduğunu ve

başvurulsa dahi sonuç alınamayacağı düşüncelerini doğurmaktadır. Diğer yandan, yaşadıkları mağduriyet karşısında resmî kurumlara başvuruda bulunan ve buna rağmen sonuç alamamış olan katılımcıların ikinci bir mağduriyet yaşadıkları yorumunda bulunulabilir. Başvuruda bulunmuş olan katılımcıların bu süreç hakkında 'yıpratıcı', 'uzun süren' şeklinde sıfatlarla tanımlamalarda bulundukları görülmektedir.

> "Bunun için de siber suçlara gittim, gerekli bütün formları doldurdum, bu bana yazılı mesaj atan kişilerin birebir hepsine ulaşıldı, onların raporu tutuldu. Mahkemeye vermek istediğimi hani söyledim fakat çok iddialı konuştular konu ile alakalı, işte polisler çok uğraşırsınız dediler bize yani bir seneye öyle sonuçlanamaz kim bilir kaç sene sürer dediler öyle anlamsızlığa kadar götürdüler, ben de çok peşinde durmama kararı aldım… Vazgeçirdiler, destekçi olmadılar, yapabiliriz açabiliriz hakkınızı arayın gibi bir şey söylemediler. Kim bilir ne kadar sürer arkadaşım dedi bir sene de sürer on sene de sürer dedi. Sürse de senin eline hiçbir şey geçmez, bu tarz konuştular" (K3, 38, Ev hanımı).
>
> "İşte resmi kuruma başvurduk ama sonuç yok yani daha. Ama eşim sağ olsun çok destek oldu yani yadırgamadı ama bir daha olursa kesin boşarım dedi onun korkusu var işte bizde de şimdi, tabi çocuk da olunca artık hataya yer yok yani. Sonuçlanmasını da hala bekliyoruz. Bu gidişle bir sonuç alabilecek miyiz onu da bilmiyorum. Siber suçlarda çalışan arkadaşım nadiren sonuçlandığını söylüyor" (K17, 34, Polis memuru).
>
> "Başvuruda bulundum, arkadaşım ile sürekli irtibat halindeyim takip ediyor davayı. Umudum yok aslında açıkçası sonuç çıkacağına dair de işte meblağ yüksek olduğu için bir umut diye başvuru yapıyorsunuz" (K19, 37, Yönetici).

Katılımcılar içerisinden K3, K7, K9, K17 ve K19 siber suç mağduriyetleri sonucunda resmî kurumlara başvuru yapmış fakat henüz sonuç alamamışlardır. Bu sürecin olumlu şekilde sonuçlanacağına dair inançları gözden geçirildiğinde katılımcıların yaşadıkları mağduriyetin çözüme kavuşacağına inanmadıkları gözlemlenmiştir. K3 başvurusunu yaptıktan ve gerekli incelemeler yapıldıktan sonra dava açmak istediğini ilettiğinde kendisini orada çalışan memurların sonuç alamayacağını ve çok uzun süre uğraşacağını ileterek vazgeçirdiklerini aktarmıştır. K7, çevresinde sonuç alamaya siber suç mağdurlarının bulunduğunu ve kendisinin de sorununun çözüme kavuşacağı konusunda emin olamadığını ifade etmiştir. K9 ise kart bilgilerinin ele geçirilmesinden dolayı yaşadığı siber suç mağduriyeti sonucu 300 bin Türk lirası tutarındaki kaybına yönelik açtığı davadan herhangi bir sonuç alamadığını ve bunun sonucunda ödemek zorunda kalmış olduğunu belirtmiştir. K17, sonuç alıp alamayacağından emin olamadığını iletmekte ve K19'un açıklaması da bunu destekler niteliktedir. Resmî kurumlara başvuruda bulunarak mağduriyetlerini gidermeye yönelik arayışta bulunan katılımcıların bu başvurulardan herhangi bir sonuç alamayacaklarına yönelik inançları olduğu gözlemlenmektedir. Bu durum hem siber suçların yeni yeni yasalarda yer alması ile hem de tespit edilmesi güç olan iz ve kanıtlar içermesi ile ilişkilendirilebilir. Fakat gerçek şu ki; siber su mağduriyeti yaşamış olan bireyler üzerine istatistiksel bir çalışma yapılmak istendiğinde birçok kişi karanlık sayı olarak kalacaktır. Bu durum öncelikle bireylerin resmî kurumlara

başvurmaya yönelik çekincesinden ve ikinci olarak da sonuç alamayacaklarına dair inançlarından kaynaklanmaktadır. Çevrelerinde artan siber suç mağduriyetleri karşısında sonuç alamamış olan bireylerin de artış göstermesi diğerleri için olumsuz birer örnek teşkil etmektedir.

Katılımcılardan bazıları ise yaşadığı mağduriyet sonucu resmî kurumlara başvurmama sebebini çevresindeki bireylerin konu hakkında yaptıkları olumsuz yorumlar ile ilişkilendirmişlerdir. Sonuç alamayacağını söyleyen yakınları dolayısıyla başvuruda bulunmadıklarını iletmişlerdir. Bu durum bireylerin çevrelerinden etkilendiğinin bir göstergesi olarak kabul edilebilir. Katılımcıların, yukarıda çevreleri tarafından damgalanmaktan koktuklarına yönelik verilen söylemleri ile aşağıdaki söylemler bütüncül olarak incelendiğinde çevre etkeninin siber suç mağduriyeti sürecindeki güçlü rolü göze çarpmaktadır.

> "Şikâyet etmedik. Çünkü ben araştırdım bir sonuç çıkmadı. Yani bazı arkadaşlarıma sordum, yurt dışında olduğu için hiçbir şey yapılamaz Türkiye'den. Çünkü verdikleri numara, dekontlar vs. hepsi yurt dışı üzerinden ilerliyor. Hani onlar da şey diyor; biz sizi dolandırmadık, siz şu meblağı yatırsanız biz zaten parayı yollayacağız size. Onların da o açıklaması olduğu için hiçbir şekilde yasal olarak bir şey yapılmıyor, adamların şirketi yasal gözüküyor. Yaptırımı olacağını düşünmediğim için resmî kurumlarla mücadele etmedim" (K4, 32, İşçi).
>
> "Türkiye'de bazı şeyler gerçekten çok çözümsüz. Yani bizim adalet sistemimiz açıkçası çok adil bir ortamda çalışmıyor. Mağdursunuz ve mağduriyetinize hiçbir şekilde çözüm sağlayamıyorsunuz… Yani açıkçası kendinize olan kızgınlık zaten bunları perçinliyor. Birkaç kişiye sordum polis arkadaşlardan da sordum hatta ya abla çözüm sağlayamazsın, koşturduğunla kalırsın boş ver gitsin dediler açıkçası böyle kaldı" (K6, 40, Muhasebeci).
>
> "Açıkçası çevremden duyduklarım doğrultusunda herhangi bir sonuç alamayacağımı düşündüm. Hani o sebeple de başvurma gereği duymadım. Yani benim açımdan daha yıpratıcı olacaktı takibi falan. Sonuç da alabileceğin kesin değil, o yüzden başvuru yapmamayı tercih ettim diyebiliriz" (K20, 34, Öğretmen).

Katılımcılardan K4, arkadaşları ile görüşmüş ve mağduriyetinin sonuçlanamayacağı konusunda duyumlar almış olduğu için yasal başvuruda bulunmamıştır. Aynı zamanda yaptırımı olacağını düşünmediğini de dile getirmiştir. K6 yine aynı şekilde resmî kurumlara başvurmama sebebini etrafından herhangi bir çözüm sağlanamayacağı yorumları duymasına bağlarken aynı zamanda sonuç alamayacağına karşı olan düşüncesini de adalet sitemi ile ilişkilendirmiştir. Adalet sistemi içerisinde bu tarz suçların henüz tam olarak yer edinmemesinden kaynaklı bir boşluk olduğunu ifade etmek istemiştir. K20 ise çevresinden duydukları doğrultusunda hem sonuç alamayacağını düşündüğünden hem de sürecin yıpratıcı olmasından endişe ettiğinden başvuruda bulunmadığını ifade etmiştir. Dolayısı ile siber suç mağduriyeti yaşamış olan bireylerin çevresinden yapılan yorumları dikkate aldıkları, herhangi bir yaptırım uygulanmayacağı ve sonuç alamayacaklarına yönelik inançlarının baskın

gelmesinden dolayı yasal başvurulardan çekindikleri gözlemlenmektedir. Bu durumda, yaşanılan siber su mağduriyetine karşı sonuç almış olan bireylerin bu süreci çevreleri ile olumlu şekilde paylaşmasının önemi ortaya çıkmış olmaktadır. Bireylerin bu tarz paylaşımlarda bulunmasına yönelik teşvik edici bilgilendirmeler yapılması gerekmektedir.

Diğer katılımcılar ise direkt olarak herhangi bir sonuç alabileceklerine inanmadıkları için hiçbir yasal başvuruda bulunmadıklarını ve mücadeleye girişmediklerini iletmişlerdir. Siber suçların tespitinin güçlükler içermesi davaların sonuçlanamamasında ya da uzun süre içerisinde sonuçlanmasında en büyük etkeni oluşturmaktadır. Fakat bu durumun katılımcılar üzerinde sanki davalarda çözüm sağlanmasına yönelik çalışmaların yapılmadığı yönünde bir hissiyat doğurduğu gözlemlenmiştir.

> "Evet, yani kendi şirket içinde çözdük, çözdüğümüz şekil ödemeyi yaptık kendilerine. O zamanlar hani bu konuda ilgilenen bir emniyet birimi de bilmiyorum yoktu herhalde, yeni yeni başlanmıştı siber suç gibi. Çok da bilgimiz yoktu açıkçası varsaydı da ilk olduğu için. Meblağ çok yüksek olmadığı için kendi içimizde hallettik ama tabi yüksek meblağlarda bir şey olsaydı o zaman daha resmi ya da resmi hani ne kadar faydası olabilir tartışılır ama en azından başvuru yapardık diye düşünüyorum" (K2, 40, Bilgi işlem müdürü).

> "Yani bu durum beni hem maddi hem manevi açıdan açıkçası yıprattı. Dediğim gibi; site sahte olduğu için benim gibi kandırılan çok kişi olmuş. Hani polise de gitsem, siber suçlara da gitsem yani çok üstüne düşüleceğini zannetmiyorum bu konunun. Bu sebeple gitmedim ben de açıkçası. Arkadaşlarıma anlattım, en azından dedim ben mağdur oldum onlar mağdur olmasın. Çevremi bilinçlendirmeye çalıştım. Yasal süreç izlemedim. Şu an bankaya olan kredi borcumu ödüyorum" (K8, 30, İşçi).

> "Kimseye de başvurmadım yani başvursan ne olacak sonuç alamazsın ki. Başvuranlara sorun bakayım kim sonuç almış parasını geri almış. Peşinde koşulmaz yani zaten hemen sizi suçluyorlar oynamasaydın diye" K16, 37, İşçi).

Katılımcılardan K2 yaşanılan siber suç mağduriyeti döneminde henüz bu suçlara yönelik herhangi bir işlem yapılıp yapılmadıklarından emin olmadıkları ve bilmedikleri için resmî kurumlara başvuruda bulunmadıklarını ve sorunu kendi içlerinde çözmeye çalıştıklarını iletmiştir. K5 ise resmî kurumlara başvuruların bu tarz suçlar için sonuçlandırılmasının düşük ihtimalde olduğunu düşündüğünü beyan etmiştir. K8, yaşadığı mağduriyeti resmî kurumlara bildirdiği taktirde ilgilenileceğini düşünmediğinden dolayı başvuruda bulunmadığını aktarmıştır. K10 herhangi bir başvuru yapmadan kendisinin çözmeye çalıştığını ifade ederken, K16 ise sonuç alamayacağından emin olduğu için yasal yollara veya resmî kurumlara başvurmamış olduğunu dile getirmiştir. Dolayısı ile yaşanılan mağduriyetler karşısında bireylerin kendilerince çözüm üretmeye çalıştıkları ve resmi yollara tam anlam ile güvenemedikleri saptanmıştır. Bunun en büyük sebebinin ise siber suçlar ile yasal mücadele konusunda katılımcıların bilgi eksikliğinin olduğu gözlemlenmiştir. Aynı zamanda çevreden

fazlası ile etkilenme, damgalanma korkusu, yeterince araştırmama gibi faktörlerin de bulunduğu dikkat çekmiştir.

Olumlama Yaklaşımı ve Kadercilik

Bireyler yaşadıkları kötü deneyimleri olumlama ihtiyacı duymaktadırlar. Yapılan mülakatlarda katılımcılardan yaşadıkları siber suç mağduriyetinden söz etmeleri istendiğinde; daha kötüsü de olabilirdi, yaşanacağı varmış, kader, kısmet gibi kelimelerin sıkça kullanıldığı gözlemlenmiştir. Dolayısı ile katılımcıların yaşamış oldukları mağduriyet sürecini olumlamaya[**] çalıştıklarından söz edilebilir. Olumlama yaklaşımı; olumsuz bir durumu pozitif düşünceler ile olumlu şekilde yeniden kurgulamak olarak tasvir edilebilir. Katılımcıların tümünde bu davranışın hâkim olduğu gözlemlenmiştir. Bu davranışa etki eden en büyük faktörün ise damgalanma korkusu olduğu yorumu yapılabilir.

> "Sonuç aslında alamadık hani bizi memnun eden tarafı şu sonuç kısmı; şifrenin yüzde yetmiş, yüzde seksen oranında çalışması ve şöyle bir durum var hani aldığınız şifre çözücü dosya, şifrelenen dosyaları eski haline getiren dosya yüzde yüz verimde çalışacak diye bir garanti de yok. Hani parayı ödemiş olmak sorunu tamamen çözmüş olduğunuz anlamına da gelmiyor. Geri döndürebildiğimiz yüzde yetmiş oldu. Yüzde yirmilik, yüzde otuzluk bir kayıp oldu mesela. Şifrelendiği zaman bazı dosyalar geri dönüşebiliyor bazısı dönüşmüyor yani yapısı bozuluyor. O sebeple geri döndürülmesi sıkıntı oluyor. Daha kötüsü de olabilirdi. Dosyalar hiç çalışmayabilirdi mesela" (K2, 40, Bilgi işlem müdürü).
>
> "Benim için tecrübe oldu bu. Tecrübeyi en azından ben yaşadım, şimdi benden hariç duyuyorum televizyonlarda büyük paralar kaptıranlar oluyormuş falan. En azından ben çok az para kaptırarak kurtuldum. Bu şekilde bir tecrübe kazandım. Daha kötüsü de olabilirdi, daha bilinçliyim şu anda… Zararın neresinden dönersek kar mıdır derler yoksa gideceği vardır bu kadar da kâfi oldu tarzında yaklaştım yani" (K11, 30, Öğretmen).
>
> "Genelde zaaf olarak adlandırabiliriz bilmiyorum o an bir düşünemiyorsunuz sanki yani tutulup kalıyordunuz ve yanlış karar veriyorsunuz. Pişman oldum tabii ki sonradan çok fazla ve üzüldüm çünkü para kaybım vardı fakat ders oldu bu bana. Daha fazla da kaybım olabilirdi ama en azından bununla kurtuldum diye düşünüyorum yani bir nevi tecrübe kazanmak için para ödedim gibi düşünüyorum aslında" (K15, 29, Yazılım geliştirme uzmanı).

Katılımcılardan K2, yaşadığı mağduriyet için daha kötüsünün de olabileceğini dile getirmiştir. K11 de benzer şekilde daha kötüsünün de yaşanabileceğini fakat zararın neresinden dönülürse kar olduğunu belirtmiş ve yaşadığı mağduriyetin kendisi için tecrübe kazandırmış olduğunu, artık daha bilinçli olduğunu ifade etmiştir. Yaşadığı maddi kayıptan daha fazlasının da söz konusu olabileceğini ileten K15, bu durumun kendisini tecrübelendirdiğini ve tecrübe kazanmak için para ödemiş bulunduğunu düşünerek kendisini rahatlattığını bildirmiştir.

[**] Olumlama kavramı; halk arasında polyannacılık olarak da bilinen, her kötü durumun iyi tarafına odaklanmayı veya yaşanılan olumsuz durumu olumlu gibi aksettirmeyi tasvir edebilmek amacı ile kullanılmıştır.

Anlatılar dikkate alındığında katılımcıların yaşadıkları siber suç mağduriyetini olumlama çabasında oldukları görülmektedir. Bu durumun bir nevi, kendilerine mağduriyet yaşamış olmayı yakıştıramamalarından da kaynaklı olduğu fark edilmiştir. Öte yandan, diğer katılımcıların cevaplarından yaşadıkları mağduriyeti kaderciliğe dayandırdıkları gözlemlenmiştir. Yaşanılan durumun ellerinde olmadığını, yaşanacak olduğu için ve kendilerinin kaderlerinde böyle bir mağduriyet yaşamak olduğundan dolayı yaşamış olduklarını beyan etmeye çalışmışlardır. Aslında bu yaklaşımdan yine damgalanmaktan ne kadar korktukları ve suçu kadere attıkları sonucu çıkartılabilmektedir. Kısaca damgalanma korkusunun bireylerin yaşanılan mağduriyete karşı olan yaklaşımlarına etki ettiği ifade edilebilir. Bu yaklaşıma istinaden aşağıda, yaşadıkları mağduriyeti kadercilik ile ilişkilendiren katılımcıların verdikleri cevaplardan örnekler paylaşılmıştır.

> "On beş, yirmi bin liraya kadar bir kaybım oldu maddi olarak. Psikolojik olarak hiç söylemiyorum. Manevi olarak daha kötü etkiledi. Tecrübe oldu diye düşünüyorum. Nasipte bu varmış, olacağı varmış oldu yani" (K4, 32, İşçi).

> "Tabi maddi olarak kayıp yaşamak üzdü. Tabi insan kendini aptal yerine konmuş gibi hissediyor böyle bir durumda, nasıl böyle bir şeye inandığımı ben de anlayamadım açıkçası. Ani ve dikkatsizliğime denk gelen bir şey oldu. Olacağı varmış diyelim. İyi oldu, tecrübe kazandık diyelim. Tecrübe kazanmak için yaşayacağımız varmış demek ki" (K13, 24, Hemşire).

> "Uzun süre beni zorladı tabi maddi kayıp yaşamış olmak ama biraz da kader aslında, yaşayacağımız varmış. Büyük bir tecrübe oldu mu derseniz evet tecrübe oldu onu da zaten yaşamadan öğrenemezsiniz ki. Tecrübe gibi düşünüyorum ben bu talihsizliği. Kader, kısmet diyorum" (K20, 34, Öğretmen).

Katılımcılardan K4 yaşadığı durumun nasibinde olduğunu, benzer şekilde K6 ise yaşadığı maddi kayıptan dolayı bunun kendisinden zaten çıkacağının var olduğunu ve o sebeple gerçekleşmiş olduğunu beyan etmişlerdir. K9 da diğerleri ile benzer şekilde kader ile ilişkilendirmiş ve yaşadığı bu durumun aynı zamanda kendisine tecrübe kazandırdığını ifade etmiştir. K13 ve K20'de tıpkı K9 gibi yaşadıkları mağduriyetin kendilerine tecrübe kazandırdığını belirterek bu olumsuz durumun kendileri için olumlu olan tarafına işaret etmişlerdir. Kısaca özetlenecek olduğunda; katılımcılar bu ifadeler ile yaşadıkları durumun aslında ellerinde olmadığını, yaşanması gerektiği için yaşanmış olduğunu, yani daha büyük bir güç vesilesi ile meydana geldiğini, iradeleri dışında gerçekleştiğini ve kendi kabahatleri bulunmadığını ifade etmek istemişlerdir. Dolayısı ile şu çıkarımda bulunulabilir; bireyler damgalanmaktan çekindikleri için yaşadıkları siber suç mağduriyetlerini kendi dikkatsizliklerine, rutin internet kullanım alışkanlıklarına ya da bilinçsizliklerine dayandırmak yerine; Rutin Aktiviteler Teorisi'nin savunularının aksine, ellerinde olmayan bir güce dayandırmayı seçerek üzerlerinden sorumluluğu atmaya çalışmaktadırlar. Psikolojik ve bireysel

etkenlerin de var olduğu gerçeği söz konusu olsa da daha önce de ifade edildiği gibi bu yaklaşımlara sebep olan en büyük etkenin damgalanma korkusu olduğu göze çarpmıştır. Sonuç olarak bu çalışmada yaşanılan mağduriyet durumlarında ve bu süreçlerin paylaşımında damgalanma korkusunun mağdurlar üzerindeki etkileri belirgin şekilde ortaya çıkmıştır.

Rutin İnternet Kullanım Alışkanlığına Etkiler

Gündelik yaşam içerisinde rutin eylemlerin birçoğunun gerçekleşmesini sağlayan ve kolaylaştıran internet kullanımından vazgeçebilmek pek de mümkün bir davranış olarak değerlendirilememektedir. Market alışverişinden fatura ödemelerine kadar ve hatta ev temizliğine kadar neredeyse tüm eylemler internet temelinde gerçekleştirilmeye başlanmıştır. Dolayısı ile bu gibi durumlar, internetin gündelik yaşamın vazgeçilmez bir parçası halini almasını sağlamıştır. Yapılan mülakatlarda katılımcılara; yaşadıkları siber suç mağduriyeti sonucunda internet kullanım alışkanlıklarında değişiklikler olup olmadığı sorulmuş, katılımcıların siber suç mağduriyeti yaşamalarına rağmen çoğunlukla internet kullanım sıklıklarında herhangi bir değişim olmadığını ya da sıklık olarak değişmediğini fakat içerik olarak değiştiğini belirttikleri gözlemlenmiştir.

> "İnternet kullanım alışkanlığımda bir değişim olmadı, olaya şöyle bakıyorum yani yolda yürürken cüzdanınız çalındı yine aynı endişeyi duyabilirsiniz ama bu çalınmayacağı anlamına gelmez ama hani kendinizce önlem alırsınız" (K1, 25, Yazılım geliştirme uzmanı).

> "İnternet kullanım süremde en fazla 1 saat oynamıştır… çünkü hala sosyal medyayı kullanıyorum. Hayatın bir parçası diyebiliriz gerçekten çünkü herkes orda insanları takip ediyor kim nerede ne yapıyor gibisinden. Bu çağda birbirimizden bu şekilde haberdar oluyoruz aslında yani" (K7, 26, Hemşire).

> "Ya internet kullanım alışkanlığımda hani pek bir kayıp olmadı öyle söyleyeyim. Tekrar aynı vakti ben internet kullanarak geçiriyorum" (K10, 27, Askeri personel).

İnternet kullanımını azaltmanın gereksiz olduğunu düşünen K1, aynı zamanda önlem olarak internet kullanım sıklığını azaltsa bile bu durumun oluşabilecek herhangi bir siber suç mağduriyetini kesin olarak engelleyeceği anlamına gelmediğini savunmaktadır. Kullanım sıklığında bir değişikliğin söz konusu olmadığını belirten K4 ise internet kullanımındaki amaçlar ile içeriğin değiştiğini ve artık tehlikeli olduğunu düşündüğü bazı sanal ortamlarda eskisi kadar vakit geçirmediğini ifade etmiştir. Yaşadığı mağduriyet sonucu internet kullanım süresinde en fazla bir saat kadar oynama olduğunu dile getiren K7 ise hala sosyal medyayı kullanmaya devam ettiğini ve bunun hayatın bir parçası olduğunu dile getirmiştir. Verilen cevaplardan elde edilen verilere göre katılımcılar internet kullanım sıklıkları ile yaşadıkları siber suç mağduriyetlerini ilişkilendirmemiş, dolayısı ile genel olarak internet kullanım sıklıklarında belirgin bir değişim söz konusu olmamıştır. Aşağıda, internet kullanım

sıklıklarında değişiklik olmasa bile kullanım amaçlarında ve kullanım içeriklerindeki değişimleri aktaran diğer katılımcıların cevaplarından örnekler verilmiştir.

> "Daha çok bu sefer kendimi bilinçlendirmek için daha güzel sitelerde olmaya karar verdim… Belki saat olarak değişmedi ama içerik olarak değişti" (K8, 30, İşçi).
>
> "Herhangi bir değişime sebep olmadı, yine aynı sürede internet kullanımım devam ediyor. Sadece alışveriş yapmamaya dikkat ediyorum böyle ortamlardan. Çünkü internet hayatın bir parçası yani" (K13, 24, Hemşire).
>
> "Instagram kullanımımda bir azalma yaşadım ama hani yine internet kullanımında aynı bir vakit geçirme oluyor. Zaten kısmak mümkün değil ki, her gün kullandığımız bir şey ve neredeyse her işimizi kolaylaştıran bir şey" (K14, 23, Hemşire).
>
> "Aslında kullanım sürem azalmadı, çünkü o olmasa başka bir şey ile o da yoksa başka bir şey ile hep dolduruyorsunuz ki yani geçirdiğiniz vakti. Zaten kullanmadan ne yapabiliriz ki internet yani bu. Hayatımızın içine işledi artık, mümkün değil ki taş devri gibi bir hayat yaşayalım…" (K17, 33, Polis memuru).

Günlük internet kullanım sürelerinde herhangi bir değişiklik olmamasına rağmen kullanım amaç ve içeriğinin değiştiğini belirten K8 kendisini bilinçlendirmek için faydalı olduğunu düşündüğü daha farklı sitelerde zaman geçireceğini belirtmiştir. Katılımcılardan K12; yaşadığı mağduriyet sonrası internet üzerinden alışveriş konusunda henüz kendisini güvende hissetmediğini, kredi kartı bilgilerini paylaşmış olduğu site ve uygulamalardan bu bilgileri kaldırdığını dolayısı ile artık interneti alışveriş için eskisi kadar sık kullanmadığını ifade ederek kullanım amacındaki değişikliği dile getirmiştir. K13 de K12'yi destekler nitelikte yorumda bulunmuş ve aynı zamanda internetin hayatın bir parçası olduğu bu sebeple de kullanım sürelerinde değişiklik olmasının pek mümkün olmadığı düşüncesini paylaşmıştır. K14 de benzer şekilde, internet kullanımını sınırlandırmanın mümkün olmadığını ve günlük hayatı kolaylaştırdığını dolayısı ile her halükârda aynı sıklıkta günlük internet kullanımına devam ettiğini dile getirmiştir. K15 internetin tehlikeli yönlerinin bulunmasına rağmen hayatı kolaylaştırmasından ve artık her yerde var oluşundan dolayı bunu kısıtlayamayacağını, kullanımında herhangi bir değişiklik söz konusu olmadığını ifade etmiştir. K16 diğer katılımcılardan farklı bir cümle kullanarak interneti bağımlılık olarak tanımlamıştır. K17 ise internetin sınırsız imkanlar sunuyor olmasından dolayı herhangi bir amaç için kullanmayı bıraktığında tamamen farklı bir amaç için tekrar kullanmaya başlayacağından internet kullanım süresinde değişim olmadığını ve hayatın içine işlediğini vurgulamıştır.

Katılımcıların anlatıları incelenecek olduğunda; internetin günlük yaşamın bir parçası olduğunu kabullendikleri ve interneti kullanmadan günlük rutin aktivitelerini yerine getiremeyeceklerine inandıkları gözlemlenmiştir. İnternetsiz bir yaşamın mümkün olmadığı ana fikrini ortaya çıkaran veriler doğrultusunda siber suçların ve siber suç mağduriyetlerinin

bireyler tarafından hayatın içerisinde olağan olarak algılanmaya başlandığının, dijital çağın kabullenilmiş bir olgusu olduğunun sonucuna varılmıştır.

Katılımcıların Almış Oldukları Önlemler ve Siber Suç Mağduriyetini Önlemek İçin Önerileri

Katılımcılara yaşadıkları siber suç mağduriyetinden yola çıkarak diğer kullanıcıların mağduriyet yaşamamaları için ne gibi önlemler almaları gerektiğine yönelik soru yöneltildiğinde cevaplar; kişisel bilgilerin ve kart bilgilerinin paylaşılmamasına, şifrelerin güçlü belirlenmesine ve bilinmedik sitelere girilmeyip bilinmedik mesaj ya da maillere bakılmamasına yönelik olmuştur. Önlem amacı ile internet kullanım süresinin azaltılmasına dair herhangi bir söylemde bulunulmamıştır. Bu durum katılımcıların internet kullanım süresini mağduriyet ile ilişkilendirmediklerini, internette geçirdikleri sürenin mağduriyetlerinin temelini oluşturduğunu kabullenmediklerinin göstergesi olarak kabul edilebilir.

> "Sürekli şifrelerini güncellemeleri, belli sürelerde değiştirmeleri. Belli bilgilerini paylaşmamaları özellikle şifrelerdeki güvenlik sorularını, her yerde aynı şeyleri kullanmamaları… Ama ne yapılabilir yani yüzde yüz hiçbir şey olmuyor. Mutlaka bir yerden yine bir açık çıkacak, yine bir açık kapı bulacaklar yine girecekler ama riski ne kadar düşürebilirsek o kadar iyi" (K2, 40, Bilgi işlem müdürü).

> "Yani resmi olmayan hiçbir sayfa ile kesinlikle bilgilerini, kredi kartı bilgilerini, nüfus bilgilerini kesinlikle paylaşmasınlar. Özellikle bunlardan uzak duruyorum. Hiçbir şekilde kartımı kaydetmiyorum. Hiçbir sitenin resmi bile olsa hiçbir siteye kartımı kaydetmiyorum…" (K4, 32, İşçi).

Bireylerin günlük rutin internet kullanımında, sitelerde ve uygulamalarda mağduriyetlerine yol açabilecek kötü amaçlı detayların yasal olarak devlet tarafından engellenmesi ve çıkartılması gerektiğini ifade eden K1, internet alışverişlerinde de sms doğrulamanın tamamen zorunlu olması gerektiği düşüncesini paylaşmıştır. Bu şekilde doğrulama ile birtakım mağduriyetlerin önüne geçilebileceğine inanmaktadır. K2 ise kullanılan şifrelerin güçlü seçilmesi ve sürekli olarak da güncellenmesi gerektiğini ifade etmiş fakat hiçbir önlemin siber suçlardan korunmak için yeterli olmadığını, sadece olasılığı düşürdüğünü belirtmiştir. K4'te resmi olmayan hiçbir sitede kişisel, kimlik ve kredi kartı bilgilerinin paylaşılmaması gerektiğini, başka bir ülkeden bile bilgilerine erişilebileceğini bu sebeple de tüm kullanıcıların daha dikkatli olmaları gerektiğini vurgulamıştır.

Yaşadığı mağduriyet ile ilişkili olarak K5; "Yani şöyle şunu söyleyebilirim; hiç kimse bir başkasına bu kadar kolay para kazandıramaz. Bunun bilincine ulaştım. Bu tarz şeylerden uzak durmaya dikkat ediyorum yani artık. O yüzden herkes uzak durmalı." yorumu ile siber suç

mağduriyetleri ile kolayca para kaybedilebileceğini ifade etmektedir. Dolayısı ile dikkatli olunması gerektiğini vurgulamaktadır.

> "Dediğim gibi öncelikle bütün kartlarını kesinlikle e ticarete açık bırakmamalılar. Yapacakları alışveriş esnasında kartını zaten on-line üzerinden kartınızı hemen internete açıp hemen kapatabiliyorsunuz sadece 30 saniyelik bir işlem. Bu otuz saniyede işleme onay verdikten sonra hemen kartlarını kapatabiliyorlar. Bunu yapmalarını öneririm akabinde de çok büyük bir problem yaşayacaklarını zannetmiyorum. Ama ara ara yine kart detaylarını mutlaka kontrol etmeliler" (K6, 40, Muhasebeci).

Kart bilgilerinin kaydedilmemesini savunan K6'ya göre, mobil bankacılık sayesinde internet alışverişlerinde alışveriş yaptığı sırada kart kullanımına izin verildikten sonra tekrar iznin kapatılabileceğini ve bu durumun kredi kartı mağduriyetlerinin önüne geçebileceğini iletmiştir.

> "Bunun dışında; kendilerine ait kişisel bilgilerini hiçbir yerde paylaşmamalarını tavsiye ederim. İnsanlar artık gerçekten her şeyi her yerde kullanabilir pozisyona geldikleri için her şekilde dolandırıcılık olabilir. Atıyorum bu illa maddi olmak zorunda değil manevi de olabilir. Yani çok moda mesela instagram da şu anda fake hesaplar açılıyor, kişinin fotoğrafları kullanılıyor bu da bir dolandırıcılık ister istemez o yüzden dediğim gibi kişisel bilgilerimizi paylaşmamalıyız. Ama işte yaptık" (K7, 26, Hemşire).

İnternet kullanımı sırasında tanımadığı birinden mesaj ile link vb. gelmesi durumunda kesinlikle açılmaması gerektiğini ifade eden K11'e göre resmi olmayan, bilinmedik sitelerden ve uygulamalardan kaçınmak gerekmektedir. Aşağıda verilen K14'ün yorumu da K11'in düşüncelerini destekler niteliktedir. K14 aynı zamanda herhangi bir uygulama vb. kayıt isteyen platformlarda zorunlu olmayan bilgilerin doldurulmaması gerektiğini ifade etmiştir.

> "Tabii ki bilmediğim, tanımadığım insanlardan gelen mesajları açmadan önce bir düşünüyorum neden böyle bir şey geldi diye. Buna daha çok dikkat ediyorum onun dışında tabii ki sosyal medya uygulamalarının biraz daha güvenliğe dikkat etmek gerektiğini düşünüyorum. Uygulamayı yapan kişilerinde bu konuda kullanıcıları destekleyecek daha güvenli ortamda sosyal medya kullandırtabilecek tasarımlar yapmaları gerektiğini düşünüyorum. Kişisel bilgileri kaydetmemek gerekiyor, bu konuda daha dikkatli olunması gerekiyor. Zaten birçok uygulamanın girişinde, uygulamaya kayıt esnasında her bilgi istenmiyor isteğe bağlı olmayan bilgilerin verilmemesi gerekiyor bence" (K14, 23, İşçi).

Yazılım geliştirme uzmanı olan K15, güvenilmeyen sitelerden herhangi bir dosya indirilmemesi ve güvenilmeyen uygulamalardan kaçınılması gerektiğini belirtmiştir. Bunun yanı sıra virüs programları kullanılması gerektiğine değinmiştir. Alınacak tüm önlemlerin siber suçlardan tümüyle korumasa bile engelleyebilmesinde öneme sahip olduğunu ifade etmiştir. K17'de siber suçların tespitinin kolay olmamasından söz ederek, internet kullanımında dikkatli olunması gerektiğini vurgulamıştır.

Genel olarak bakıldığında; katılımcılar siber suç mağduriyetlerinden korunmak için kompleks bir yapıya sahip olan internette bilinmeyen herhangi bir siteye girilmemesini, çerezlerin ya da izinlerin kabul edilmemesini, kişisel bilgilerin ya da kart bilgilerinin paylaşılmaması gerektiğini iletmişlerdir. Özellikle internet alışverişlerinde kart bilgisi paylaşımına dikkat edilmesi gerektiği üzerine yorum yapmışlardır. Öte yandan virüs programı kullanılması gerektiği ve şifrelerin güçlü seçilerek sürekli olarak güncellenmesi gerektiği ifade edilmiştir. Katılımcılardan hiçbiri internet kullanım süresinin azaltılması üzerine bir yorumda bulunmamıştır. İnternetin günlük yaşamın bir parçası olması sebebi ile kullanılması gerektiği fakat daha dikkatli olunması gerektiği ana fikri üzerinde bütüncül yorumlamalarda bulunmuşlardır. Bunun yanı sıra yasal mücadele göz ardı edilmemeli, mutlaka gerekli başvurular gerçekleştirilmelidir. Siber suçlar ile mücadele yöntemlerinin ve sürecinin gelişebilmesi açısından yaşanan mağduriyetler karanlık sayı olarak kalmamalıdır.

SONUÇ

Dijitalleşme dünya üzerinde birçok değişim ve dönüşümü beraberinde getirmiştir. Bu yeni süreç beraberinde; kültür, eğitim, suç gibi olguların yanı sıra günlük rutin aktivitelerin de dijitalleşmesine sebep olmuştur. Bu durum dijitalleşen suç olgusu beraberinde getirerek siber suç mağdurlarının ortaya çıkmasına neden olmuştur. Siber suçlar sürekli olarak kendini yenileyen ve teknolojik gelişmelere ayak uyduran bir niteliğe sahip olduklarından alınan önlemlerin geçerlilikleri yeni bir siber suç tekniği geliştirilene kadar sürmektedir. Dolayısı ile herkesi kapsayabilen bir yapıları bulunmaktadır.

İnternet kullanım sürecinde temkinli olma ve önlem alma açısından elde edilen veriler incelendiğinde, katılımcıların bilgi paylaşımlarında yeterince dikkatli davranmadıkları ve çoğunlukla siber suçlara karşı önlem alma eyleminde bulunmamış oldukları sonucu ortaya çıkmıştır. Katılımcıların dikkatsiz olmasının ve önlem konusunda aksiyon almamalarının siber suç mağduriyeti yaşamalarında etkili bir faktör olduğu sonucuna varılmıştır.

Bunun yanı sıra veriler doğrultusunda; siber suç mağdurlarının damgalanma korkusu olduğu dikkat çekmiştir. Bu durum mülakat sürecinde de katılımcılara ulaşmayı zorlaştırmıştır. Yaşadıkları siber suç mağduriyeti konusunda mülakata katılmak istemeyen bireyler söz konusu olmuştur. Paylaştıklarında yadırganacaklarını düşünmüşlerdir. Katılımcılarda da aynı düşünce söz konusu olmuştur. Mülakat süresi boyunca yadırganacakları ve damgalanacakları konusunda yorumlarda bulunmuşlardır. Bu düşünceler sebebi ile katılımcıların yaşadıkları mağduriyeti çevreleri ile de paylaşmadıkları gözlemlenmiştir. Çevreleri ile paylaşmamalarının psikolojik

olarak destek alamamalarına sebep olduğu ve mücadele için ne yapacakları konusunda bilinçlenme durumunda eksik kaldıkları ortaya çıkmıştır. Ailelerinin ve çevrelerinin duymasından çekinen katılımcıların maddi kayıplarına rağmen resmi kurumlara herhangi bir başvuruda bulunmadıkları da gözlemlenmiştir.

Katılımcıların yaşadıkları mağduriyet sonucunda resmi kurumlara başvuruda bulunmama ve mücadele etmeme gibi eylemsizliklerinin bulunduğu dikkat çekmiştir. Damgalanma korkusunun yasal olarak haklarını arayışlarında olumsuz bir etkisinin bulunduğu ortaya çıkmıştır. Aynı zamanda katılımcıların birçoğu çevrelerinden de duydukları üzere, başvuruda bulunsalar bile sonuç alabileceklerini düşünmemiş ve başvuruda bulunmamışlardır. Başvuruda bulunmuş olan 5 katılımcının ise henüz bir sonuç alamamış oldukları görülmüştür. Bu durumda katılımcıların mücadele sürecinde ikincil bir mağduriyet yaşadıkları söylenebilir. Dolayısı ile katılımcılarda yasal bir sonuç alamayacaklarına yönelik genel bir algı oluşmuştur. Bu ortak bilinç yaşanacak diğer siber suç mağduriyetlerine de işleyeceğinden bu konuda bilinçlendirmeler yapılması gerekmektedir.

Veriler doğrultusunda; katılımcılarda daha kötüsünün de olabileceği ve yaşadıkları ile kurtulmuş oldukları inancının yanı sıra kadercilik eğilimleri gözlemlenmiştir. Yaşanılan mağduriyetleri olacağı varmış şeklinde değerlendirdikleri göze çarpmıştır. Aslında dikkatsizlikleri sonucu meydana gelen mağduriyetleri polyanacılık ve kadercilik eğilimleri ile olumlama çabasında oldukları ortaya çıkmaktadır.

Yaşanılan mağduriyetlere rağmen kullanıcıların internet kullanım alışkanlıklarında belirgin değişimler olmadığı sonucu ortaya çıkmıştır. Dolayısı ile mağduriyet yaşamalarına sebep olan rutin internet kullanım alışkanlıklarının değişmemesi durumu ikinci kez mağduriyetlerin yaşanma olasılığını artırmaktadır. İnternet aracılığı ile gerçekleştirilen günlük rutin aktivitelerin siber suç mağduriyetleri ile birebir ilişkili olduğu sonucu ortaya çıkmıştır. Sonuç olarak katılımcılar bu rutin aktiviteler sonucunda mağduriyet yaşadıklarından, mağdurun suça kendisinin sebebiyet vermekte olduğu çıkarımında bulunulabilir. Siber suçlarda mağdurun rolünün etkili bir faktör olduğu sonucuna varılmıştır.

Elde edilen veriler doğrultusunda katılımcılar çözüm önerisi olarak; kullanıcı hesaplarının şifrelerinin güçlendirilmesi ve sürekli olarak güncellenmesi gerektiğini, bilinmedik site ve uygulamalara karşı temkinli olunması gerektiğini, kişisel bilgilerin ve kart bilgilerinin herhangi bir yerde paylaşılmaması ya da dikkat edilerek paylaşılması gerektiğini iletmişlerdir.

Nihai olarak; siber suç mağduriyetlerinin genel olarak sosyal medya hesapları üzerinden işlendiği görülmektedir ve bu alanda önlemlerin artırılması, kullanıcıların bilinçlendirilmesi gerektiği kanaatine varılmıştır. Günümüzde bireylerin sosyalleşme ve kendileri hakkında bilgi paylaşarak görülme, bilinme arzuları doğrultusunda mağduriyetlerin ortaya çıktığı gözlemlenmiştir. Bunun yanı sıra kolay para kazanma arsuzu da sanal yatırımlara ya da şans oyunlarına yönelime sebebiyet vermekte ve yüksek miktarda kayıplara yol açmaktadır. Özellikle erkeklerde bu tarz mağduriyetler söz konusu olurken, kadınlarda manevi mağduriyetler ya da alışveriş temelli mağduriyetler söz konusu olmaktadır. Bunun ile ilişkili olarak kadınların yatırım konusunda çekinceleri, temkinli davranışları ve güvensizlikleri sebep gösterilebilirken erkeklerin daha fazlasını kazanma arzularının baskın geldiği görülmektedir. Sanal yatırım dolayısı ile mağduriyet yaşamış olan erkek katılımcılarda, başka siteler aracılığı ile sanal yatırım yapmaya devam etme davranışı gözlemlenmiştir. Bu durumu her sitenin güvenilir olmadığı, güvenilir olan sitelerde sanal yatırım yapılmasında bir sakınca olmadığı şeklinde olumlamaya çalıştıkları görülmektedir. Kısacası bireylerin rutin internet kullanım alışkanlıklarının mağduriyet yaşamalarına sebebiyet vermekte olduğu sonucu elde edilmiştir.

KAYNAKÇA

Akarslan, H. (2011). Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı, Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi- Güvenlik Bilimleri Enstitüsü.

Akcan, E. A. (2014). Ceza Hukukunda Mağdurun Korunmasına Yönelik Düzenlemeler, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, Özel Sayı, 16, 3949-3997.

Akdağ, P. (2009). Siber Suçlar ve Türkiye'nin Ulusal Politikası, Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi- Güvenlik Bilimleri Enstitüsü.

Akıncı, F. S., Dursun, S. (2016). *Viktimoloji,* 3. Baskı, İstanbul: Beta Yayınları.

Akyeşilmen, N. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik*, 1. Baskı, Orion Kitabevi, Ankara.

Aykara, A., Özkan, S. (2017). Mağdur Hakları ve Gereksinimleri Bağlamında Engelli Mağdur Bireyler, *Trakya Üniversitesi Sosyal Bilimler Dergisi,* 19(1), 143-165.

Bal, H. (2013). *Suç Sosyolojisi,* 1. Baskı, Isparta: Fakülte Kitabevi Yayınları.

Birceviz, F. (2019). Rutin Aktiviteler Teorisi Bağlamında Siber Suç Mağduriyeti, Yayınlanmamış Yüksek Lisans Tezi, Milli Savunma Üniversitesi- Savunma Bilimleri Enstitüsü.

Branic, N. (2016). Routine Activities Theory, W. G. Jennings (Ed.), *Encyclopedia of Crime and Punishment* içinde (1-3), United States: John Wiley & Sons Inc. Publishing.

Brennen, S., Kreiss, D. (2016). Digitalization, Eric W. Rothenbuhler (Ed.), *The International Encyclopedia of Communication Theory and Philosophy II içinde* (1-12), United States: John Wiley & Sons Inc. Publishing.

Brenner, S. (2010). *Cybercrime: Criminal Threats From Cyberspace,* 1. Baskı, California: Preager.

Budak, Ö. S. (2015). Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği, Yüksek Lisans Tezi, Atatürk Üniversitesi- Eğitim Bilimleri Enstitüsü.

Bullock, K. vd. (2010). Introduction, R. V. Clarke (Ed.), *Situational Prevention of Organised Crimes* içinde (1-17), United Kingdom: Willan Publishing, First Publish.

Castells, M. (2008). *Enformasyon Çağı: Ekonomi Toplum ve Kültür; Ağ Toplumunun Yükselişi,* E. Kılıç (Çev.), 2. Baskı, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Clarke, R., Felson, M. (2008). *Routine Activity and Rational Choice,* Second Edition, New Jersey: Transaction Publishers.

Clevenger, S. vd. (2018). *Understanding Victimology*, 1. Baskı, New York: Routledge Publishers.

Cohen, L., Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach, *American Sociological Review,* 44(4), 588-608.

Das, S., Nayak, T. (2013). Impact of Cyber Crime: Issues and Challenges, *International Journal of Engineering Sciences & Emerging Technologies,* 6(2), 142-153.

Dashora, K. (2011). Cyber Crime in The Society: Problems and Preventions, *Journal of Alternative Perspectives in The Social Sciences,* 3(1), 240-259.

Dolu, O. (2009). Bir Fırsat Olarak Suç: Suçun Durumsal Belirleyicileri, Suç Fırsatları ve Rutin Faaliyetler Teorisi, *Polis Bilimleri Dergisi,* 11(2), 1-30.

Dolu, O. (2012). *Suç Teorileri: Teori, Araştırma ve Uygulamada Kriminoloji,* 4. Baskı, Ankara, Seçkin Yayıncılık.

Ermeydan, D. (2018). Türk Ceza Kanunu'nda Bilişim Suçları, Yayınlanmamış Yüksek Lisans Tezi, Çağ Üniversitesi- Sosyal Bilimler Enstitüsü.

Felson, M., Eckert, M. A. (2018). *Crime And Everyday Life: A Brief Introduction,* 6. Baskı, United States: SAGE Publications.

Güçlü, İ., Akbaş, H. (2016). *Suç Sosyolojisi: Kavram, Teori ve Uygulama,* 1. Baskı, Ankara: Seçkin Yayıncılık.

Güney, H. (2008). Sosyolojik Açıdan Çocuk Suçluluğu ve Nedenleri, Yayınlanmamış Yüksek Lisans Tezi, Kırıkkale Üniversitesi-Sosyal Bilimler Enstitüsü.

Güngör, M. (2019). Mağduriyetin Giderilmesi Açısından Uzlaştırma Kurumu ile Mağdur Hakları Tasarısının İncelenmesi, *Yıldırım Beyazıt Hukuk Dergisi,* (2), 189-230.

İçli, T. G. (2007). *Kriminoloji,* 8. Baskı, İstanbul: Seçkin Yayıncılık.

İşliyen, M. (2019). Dijital Çağın Yeni Hastalığı: Dijital İstifçilik, *Akdeniz Üniversitesi İletişim Fakültesi Dergisi,* (31), 404-420.

Karaca, M. vd. (2021). Siber Mağduriyet: Kavramsal Bir Çalışma, *Anadolu Akademi Sosyal Bilimler Dergisi,* 3(1), 177-191.

Katoğlu, T. (2012). Ceza Hukukunda Suçun Mağduru Kavramının Sınırları, *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 61(2), 657-693.

Kılıç, Y. S. (2007). Çocuk Suçluluğuna Sebep Olan Sosyo-Ekonomik Faktörler, Yayınlanmamış Yüksek Lisans Tezi, İnönü Üniversitesi-Sosyal Bilimler Enstitüsü.

Kundi, G. M., Nawaz, A. (2014). Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge To Governments In Developing Countries, *Journal of Information Engineering and Applications,* 4(4), 61-70.

McLuhan, M. (1994). *Understanding Media,* 1. Baskı, London: The MIT Press.

Ngo, F., Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational Level Factors, *International Journal of Cyber Criminology,* 5(1), 773-793.

Özüdoğru, U. (2010). *Siber Suçlar ve Mücadele Yöntemleri: Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri,* 1. Baskı, Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Peker, B. (2010). Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu, Yayınlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi- Sosyal Bilimler Enstitüsü.

Polat, A., Gül, S. K. (2010). Kriminoloji Araştırmalarında Mağdur Anketlerinin Yeri ve Önemi, *Uluslararası İnsan Bilimleri Dergisi*, 7(1), 1290-1310.

Russell vd. (2015). Introduction: Cybercrime Risks and Responses-Eastern and Western Perspectives, R. G. Smith (Ed.), *Cybercrime Risks and Responses,* New York: Palgrave Macmillan.

Sarıyar, H. (2019). Dijital Çağda Kimliğin Kavramsallaştırması ve Gerçeklik: Twitter Parodi Hesapları, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi- Sosyal Bilimler Enstitüsü.

Seçkin, M. B. (2020). Ceza Muhakemesinde Mağdur ve Şikâyetçinin Hakları, *Uyuşmazlık Mahkemesi Dergisi,* (15), 621-664.

Sokullu Akıncı, F., Dursun, S. (2016). *Viktimoloji*, 3. Baskı, İstanbul: Beta Yayıncılık.

Taşçı, U., Can, A. (2015). Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014, *Fırat Üniversitesi Sosyal Bilimler Dergisi,* 25(2), 229-248.

Wolhuter, L. vd. (2009). *Victimology: Victimisation and Victims' Rights,* 1. Baskı, New York: Routledge Cavendish.

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory, *European Journal of Criminology,* 2(4), 407-427.

Yüksel, M. (2017). Klasik Suç Kuramları, F. Güllüpınar (Ed.), *Suç Sosyolojisi,* Eskişehir: Anadolu Üniversitesi Yayını.