...::KENT AKADEMİSİ | URBAN ACADEMY

Volume: 18 Issue: 3 - 2025 | Cilt: 18 Sayı 3 - 2025

ARTICLE INFO | MAKALE KÜNYESİ

Article Type: Research Article | Araştırma Makalesi
Submission Date | Gönderilme Tarihi: 19.07.2024
Admission Date | Kabul Tarihi: 06.01.2025

CITATION INFO | ATIF KÜNYESİ

Aras, H. (2025). Kamusal İtibarın Güvenliği İçin Dezenformasyona Karşı Mücadele, *Kent Akademisi Dergisi, 18*(3):1532-1550. https://doi.org/10.35674/kent.1519062

Kamusal İtibarın Güvenliği İçin Dezenformasyona Karşı Mücadele

Combating against Disinformation for the Security of Public Reputation

Hüseyin Aras[1]

Öz

Kamusal itibar kamu güvenliğinin bir referans nesnesidir. Kamusal itibarın zarar görmesi halinde devletin siyasî ve toplumsal meşruiyeti zedelenebilir. Bu nedenle kamusal itibara zarar verebilecek olan değişkenler/etkenler kontrol altına alınmalıdır. Bu değişkenlerden/etkenlerden biri dezenformasyondur. Bu çalışma Türkiye Cumhuriyeti Devleti'nin dezenformasyon nedeniyle yürüttüğü mücadeleye bir eleştiri yöneltmekte ve bu mücadelenin güvenlikçi yaklaşım temelinde yürütülmesini içeren bir işleyiş süreci önermektedir. Bu işleyiş sürecinde, dezenformasyon nedeniyle yürütülen mücadelenin "dezenformasyonla mücadele" değil, "dezenformasyona karşı mücadele" biçiminde kavramlaştırılmasını, kamu güvenliği ile ilgili istihbarat birimlerinin ise bu sürecin merkezine yerleştirilmesini tavsiye etmektedir. Aslında çalışmanın bu hususta bir tartışma başlatması ve dezenformasyon nedeniyle yürütülen mücadelenin gözden geçirilerek geliştirilmesine teşvik etmesi umulmaktadır. Zira dezenformasyonun önlenmesindeki imkânsızlıklar ile gerçekleştikten sonra verdiği zararın telafi edilmesindeki zorlukların bu türde bir gözden geçirme ve geliştirme ihtiyacını gerektirdiği değerlendirilmektedir. Postmodern dönem teknolojisinin dezenformasyonu, çeşitli aktörler tarafından kolayca gerçekleştirilebilir ve yaygınlaştırılabilir hale getirmiş olması bu değerlendirmeye haklılık kazandırmaktadır. Kuramsal düzeyde bir inceleme olan çalışmanın nihai hedefi Türkiye Cumhuriyeti Devleti'nin kamusal itibarın güvenliğini sağlamaya yönelik çabalarına katkı sunmaktır.

Anahtar Kelimeler: Kamusal İtibar, Kamusal İtibarın Güvenliği, Dezenformasyona Karşı Mücadele, İstihbarata Dayalı Kolluk

ABSTRACT

Public reputation is a reference object of public security. If public reputation is damaged, the political and social legitimacy of the state can be damaged. For this reason, variables/factors that may harm public reputation should be controlled. One of these variables/factors is disinformation. This study criticizes the struggle of the State of the Republic of Türkiye due to disinformation and proposes a functioning process that includes the execution of this struggle on the basis of a security-oriented approach. In this process, it recommends that the struggle because of disinformation should be conceptualized as a "combating against disinformation" rather than "fighting disinformation", and that intelligence units related to public security should be placed at the center of this process. In fact, it is hoped that the study will initiate a discussion on this issue and encourage the combating against disinformation to be reviewed and improved. Because it is considered that the impossibilities in preventing disinformation and the difficulties in compensating for the damage it causes after it has occurred require the need for such a review and development. The fact that the technology of the postmodern period has made disinformation easily realizable and disseminated by various actors justifies this assessment. The ultimate goal of the study, which is a theoretical review, is to contribute to the efforts of the State of the Republic of Türkiye to ensure the security of public reputation.

Keywords: Public Reputation, Security of Public Reputation, Combating against Disinformation, Intelligence Based Policing

[1] **Corresponding Author | Yetkili Yazar:** Doç. Dr., Nevşehir Hacı Bektaş Veli Üniversitesi, huseyinaras06@gmail.com, ORCID: 0000-0001-8117-6574

GİRİŞ:

Kamusal hizmetleri kamu sektörü (idare) tarafında sunan kişi, kurum ve kuruluşları hedef alan dezenformasyon[2] kamu yönetiminin önemli bir meselesidir. Çünkü kişi, kurum ve kuruluşların vatandaşlar ve diğerleri[3] nazarındaki itibarına olumsuz etkide bulunarak hem kamu yönetiminin hem de hükûmetlerin meşruiyetine zarar verme potansiyeline sahiptir. Çalışmada bu mesele "kamusal itibarın güvenliği" biçiminde kavramlaştırılmış, bu kavramlaştırmaya dayanarak kamu güvenliği ile ilgili istihbarat birimlerinin merkezde yer aldığı bir işleyiş süreci önerilmiştir. Özgürlükçü yaklaşımı yadsımayan ancak güvenlikçi yaklaşımı özellikle dezenformasyonun kontrol altına alınması gibi zorlu hâllerde elzem gören bir yönetim felsefesine sahip olan araştırmacının bu önerisinin temelinde, "Hükümdar" adlı eserinde Machiavelli'in hükümdara yaptığı bir tavsiyenin günümüzde hükûmetler tarafından kullanılabilirliğine dair kabul yatar. Nitekim Carpenter (2010, s. 70) Machiavelli'in bu tavsiyesinin hükûmetler tarafından başarılmasının hükümdarlara kıyasla daha mümkün olduğunu, hükûmetlerin bunu hükümdarlara kıyasla daha az sorunlu şekilde başarabileceklerini ve üstelik bunu gerilimli ortamlarda hassas dengeyi de koruyarak yapabileceklerini ifade etmektedir.

Eserinde Machiavelli (2019, s. 62-66) hükümdarın hem sevilecek hem de korkulacak biri olmasını, ama aynı anda ikisini bir arada bulunduramazsa sevilecek biri olmaktansa korkulacak biri olmayı tercih etmesini tavsiye eder. Genel olarak insanların çıkarcı, içten pazarlıklı, riyakâr, nankör doğalarının bunu zorunlu hale getirdiğini savunur. Sevginin bir zorunluluk bağı olmasını, çıkarlarının gerektirmesi halinde doğaları gereğince insanların o bağı rahatlıkla koparıp atabilecek olmalarını buna kanıt olarak sunar. Buna karşılık korku bağının insanın aklından hiç çıkaramadığı cezalandırılma kaygısını içerdiğini, hâl böyleyken hükümdarın korku salmayı başarmasının kendi yararına olacağını vurgular. Bunun için hükümdarın elinde bulunan korku salma imkânına (gücüne) güvenmesine, ancak bu imkânı kin ve nefret kazanmamaya da özen göstermek suretiyle kullanmasının gerekliliğine dikkat çeker.

Whyte'ın (2020, s. 2) "dezenformasyonun demokratikleşmesi" hâli olarak betimlerken vurguladığı üzere yıkıcı nitelikteki dezenformatif içerikler günümüzde bireyler tarafından kolayca elde edilebilmekte, üretilebilmekte ve kullanılabilmektedir. Bu hâlde Machiavelli'in yönetim faaliyetini sevgi, korku, kin ve nefret kavramlarıyla ilişkilendirerek hükümdara yaptığı bu tavsiyenin, hükûmetlere, demokratikleşen dezenformasyonun kontrol altına alınması için fırsatlar sunabileceği değerlendirilmektedir. Hükûmetler yönetim faaliyetlerini bu tavsiye ışığında gerçekleştirebilirler. Kamu yönetiminin meşruiyetine etki edebilecek olan kamusal itibarın kazanıldıktan sonra güvenliğini sağlayabilecek tedbirleri bu tavsiye ışığında gerçekleştirecekleri uygulamalarla alabilirler. Çünkü kamusal itibarın güvenliğinin sağlanmasının sorumluluğu sadece dezenformasyonların hedefindeki kişi, kurum ve kuruluşların öznel çabalarına bırakılamaz. Öznel çabalar gerekli olsa da güvenlik bürokrasisi bu konuda aslî derecede yetkili, görevli ve sorumludur. Türkiye Cumhuriyeti Devleti'nin hükûmetleri bu çalışmada önerilen işleyiş sürecini kullanarak, dezenformasyon nedeniyle yürütmek zorunda oldukları mücadeleyi etkin, etkili ve verimli şekilde yürütebilirler. Bu çalışma bu amaca matuftur.

1. Kamu Yönetiminde Bir Meşruiyet Göstergesi: Kamusal İtibar ve Kamusal İtibarın Güvenliği

[2] Dezenformasyon çeşitli ortamlarda çeşitli araçlarla gerçekleştirilebilir. Çalışmada sözü edilen dezenformasyon, sanal ortamda gerçekleştirilen çevrimiçi dezenformasyondur.

[3] Kamusal hizmetlerin hedef-kitlesi sadece bir devletin vatandaşı olanlar değildir. Kamu yönetimi nitelikli kamusal hizmetler yoluyla vatandaş olmayan kişilerin ve aktörlerin de ihtiyaçlarını karşılama, beğenilerini kazanma, onları etkileme, onları çeşitli biçimlerde davranmaya teşvik etme vb. gibi amaçları başarmak ister. Yabancı yatırımcılar, yabancı öğrenciler, yabancı turistler, uluslararası sivil toplum kuruluşları, uluslararası şirketler, devletler vb. kamusal hizmetlerin hedef-kitleleri arasındadır. Nitekim "kamu diplomasisi" kavramı bu kişilerin ve aktörlerin de kamu yönetiminin hedef-kitleleri arasında yer aldığına kanıttır. Bu nedenle kamu yönetiminin meşruluğu konusu sadece vatandaş olanlarla ilgili bir konu değildir. Bir devletin vatandaşı olmayanlar nazarında da meşruluk kazanmak kamu yönetimi için önemli hale gelmiştir. Bu bakımdan, kamusal itibara dair bu çalışmada bir devletin vatandaşı olmayanlardan söz edilmesi gerekli görüldüğünde bu kişiler için "diğerleri" zamiri kullanılmıştır.

İtibar bir varlıktır (Rao, 1994, s. 30). Eskiden "iyi" derecesinde sahip olunmasına değer atfedilen bu varlık günümüzde "yönetilmesi ve korunması gereken" bir varlık haline gelmiştir (Diermeier, 2012, s. 304). Bu durum vatandaşlar ve diğerleri nazarında iyi itibara sahip olması gereken kamu yönetiminin de bir meselesidir. Kamu yönetimi de kendisi için değer içeren bu varlığın zarar görmesinin yol açacağı olumsuz sonuçlar gerekçesiyle "zorunlu" olarak çareler üretmelidir. İtibar kayıplarını hükûmetlerin meşruiyetine yönelik tehditler olarak kabul edip çareler aramak kamu yönetiminin ertelenemez nitelikteki bir sorumluluğudur. Zavattaro ve Eshuis (2021, s. 420-421) kamu yönetiminin hâlihazırda içinde bulunduğu çağı "İtibar Çağı" olarak adlandırıp bu post-modern durumun kamu kurum ve kuruluşları için itibar yönetimini stratejik biçimde kullanmayı gerektirdiğini tespit ederken tam olarak buna dikkat çekerler.

İtibar ve meşruiyet kavramları birbirlerinin tamamlayıcılarıdırlar (Fombrun & Riel, 1997, s. 9; King & Whetten, 2008, s. 192-202). Bu nedenle kamu yönetiminde kurum ve kuruluşların meşruiyetleri itibar yönetimini gerektirir (Carpenter & Krause, 2012, s. 30). Çünkü onların marka, güven, imaj, kimlik, prestij ve statü gibi varlıklarının oluşup gelişebilmesi de toplumla ilişkilerinin güçlendirilebilmesi de kendilerine zarar verebilecek iç ve dış tehditlere karşı etkili yönetim süreçleri geliştirebilmeleri de buna bağlıdır (Bustos, 2021, s. 731). Buna karşın kamu kurum ve kuruluşları iyi itibara sahip olmadıklarında kamu yönetimine toplumun desteği kaybedilebilir, seçimle gelen politikacıların ve hükûmetlerin yönetme yetkisini kullanabilmelerinin temelleri sarsılabilir, nitelikli kişilerin kamusal hizmetlerde istihdam edilebilmelerinin ve elde tutulabilmelerinin fırsatları kaçırılabilir ve nihayetinde kamu kurum ve kuruluşları siyasî içerikli saldırılara maruz kalabilirler (Carpenter, 2002, s. 491). İtibar yönetimi çerçevesinde hem itibar kazanmak hem de kazanılmış olan itibarın güvenliğini sağlamak günümüz koşullarında kamusal hizmetleri kamu sektörü tarafında sunan tüm aktörler için bu gibi saiklerle elzemdir. Tam bu noktada, sözü edilen aktörleri de içerecek şekilde "kamusal itibar" kavramına değinmek uygundur.

Alan yazında "kurumsal itibar" ve "bürokratik itibar" kavramları kurum ve kuruluşların itibarlarını ifade etmek gayesiyle kullanılır. Bu iki kavram bu çalışmada kullanılan "kamusal itibar" kavramı ile benzer görünse de benzer değildir. Bu nedenle bu iki kavramdan birini tercih etmektense çalışmada "kamusal itibar" kavramının kullanılması tercih edilmiştir. Bunun "kurumsal itibar" kavramı özelinde iki temel nedeni vardır. Birincisi, "kurumsal itibar" kavramı, özel sektörde kuruluşların özellikle ekonomik gerekçelerle ulaşmak istedikleri amaçlarla ilgilidir. Argüden (2003, s. 10-12) kuruluşlar, kurumsal itibar elde ettiklerinde pazardaki konumlarını güçlendirmiş, ürünlerinin ve hizmetlerinin insanlar tarafından tercih edilmesinin imkânlarını oluşturmuş, marka bilinirliklerini sağlamış vb. olabileceklerini ifade etmiştir. Bu kavram özel sektörde bu amaçlar gereğince kullanıldığında kamu sektöründe itibar kavramına önem atfedilmesinin gereğinden ayrışır. Özel sektör ile kamu sektörüne içkin "kâr" ve "yarar" kavramları bu ayrışmayı açıklar. Özel sektör kâr motivasyonuyla hareket ederken, kamu sektöründe sunulan hizmetlerde ağırlıkla kamu yararı esastır. Kamu sektörü ile özel sektörün itibar kavramına önem atfetme gerekçeleri bu nedenle farklıdır. Bu bakımdan özel sektörde kullanılan kurumsal itibar kavramı kamu sektörü tarafında sunulan kamusal hizmetlere dair itibarı tam anlamıyla karşılamayabilir. Çünkü son derece indirgeyici bir yaklaşım içerir. Şu hâlde bu çalışmada kullanılması tercih edilmiş olan "kamusal itibar" kavramının özel sektörde de kullanılan "kurumsal itibar" kavramı ile birebir aynı muhtevalı olmadığı açıktır.

"Kamusal itibar" kavramının "kurumsal itibar" kavramına tercih edilmesinin ikinci nedeni ise kamu sektöründe "kurumsal itibar" kavramının kamusal hizmetler sunan kurum ve kuruluşların itibarına işaret edip kamusal hizmetlerin sunumunda görevli olan kişilerin itibarını dışarıda bırakabilmesi ihtimalidir. Oysa hükûmetler tarafından kamu yönetiminde görevlendirilen kişiler (memurlar ve kamu görevlileri) özellikle heterojen siyasî, ekonomik ve kültürel yapılı toplumlarda dikkatlerin odağında olabilirler. Bu kişilerin kamusal hizmetlerin sunumundaki rolleri, başarıları vb. toplum tarafından

dikkatle izlenebilir. Başarısızlık halinde bu kişiler toplum tarafından "devletin değil, hükûmetin bürokratı/memuru/görevlisi" olmakla eleştirilebilirler. Bu kişilerin toplum nezdindeki olumsuz kişisel itibarları neticesinde yapılan sorgulamalar kamu yönetiminin ve hükûmetlerin meşruiyetinin eleştirisine dönüşebilir. Kamu sektörü tarafında kamusal hizmetler sunan kurum ve kuruluşlar, kamu görevlilerini hedef alan bu minvaldeki eleştiriler nedeniyle yıpranabilirler. Bu nedenle kamusal hizmetlerin sunumunda kamu sektörü (idare) adına görev yapan kişilerin itibarlarını kamu sektörü tarafında kamusal hizmetler sunan kurum ve kuruluşların itibarına entegre edip onunla bütünleştirmek bir ihtiyaçtır. Bu ihtiyaç ışığında kamu sektörü tarafında kamusal hizmetler sunan kişi, kurum ve kuruluşlar için kişisel ya da kurumsal itibar ayrımı yapmaksızın tamamı için "kamusal itibar" kavramının kullanılmasının uygun olduğu değerlendirilmektedir. Üstelik çalışmadaki "kamusal itibar" kavramının "kamu yönetiminde itibar" biçimindeki kavramın daha iyi anlaşılması bakımdan da kullanışlı olabileceği düşünülmektedir. Açıklanan nedenlerle, çalışmada kullanılan "kamusal itibar" kavramının "kurumsal itibar" kavramı karşısında daha geniş bir anlam taşıdığı ifade edilebilir.

Kamusal itibar kavramı, bürokratik itibar kavramından da farklıdır. Dursun (2012, s. 133-134) bürokrasi kavramının "kurumları ve personeliyle devletin gerçekleştirdiği yönetim"i ifade ettiğini, ancak bu kavramın "işlerin yavaş yürümesi", "kırtasiyecilik", "kamu yönetiminin verimsiz çalışması" vb. gibi olumsuzluk içeren küçültücü anlamlarla da yüklü olduğunu açıklar. Kavrama dair duygusal içerikli bu anlamların toplum nazarında yaygın olması nedeniyle, bu kavramın hakaret kastıyla ya da eleştiri aracı olarak da kullanılabildiğine işaret eder. Ayrıca bilim çevrelerinde yönetime dair bir olumsuzluğu ifade etmek için "bürokratizm" ve "büropatoloji" gibi kavramların kullanıldığını tespit eder. Kavramın yüklü olduğu bu pejoratif anlamlar nedeniyle bürokrasi ve itibar kavramlarının bir arada kullanılması da uygun görülmemiş; "kurumsal itibar" kavramı için olduğu gibi "bürokratik itibar" kavramının da bu çalışmada kullanılmaması tercih edilmiştir. Kamu yönetiminin bürokrasi kavramına içkin diğer anlamlarıyla uyumlu olabilirken bürokrasi kavramının çağrıştırdığı olumsuz anlamları çağrıştırmayacağı gerekçesiyle çalışmada "kamusal itibar" kavramının kullanılmasının isabetli bir tercih olduğu değerlendirilmektedir.

Bu açıklamalar ışığında "kamusal itibar" kavramı bu çalışmaya özgü olarak "kamusal hizmetleri kamu sektörü (idare) tarafında sunan kurum ve kuruluşlar ile bu hizmetlerin sunumunda görevli olan kişilerin vatandaşlar ve diğerleri nazarındaki değeri" olarak tanımlanabilir. Kamusal itibar; kamu sektörü tarafında sunulan kamusal hizmetlerin kamunun (toplumun) ihtiyaçlarını beklentiler dahilinde karşılayabilmesine, bu hizmetlerin sunuluş biçimlerine, bu hizmetleri sunan kamu görevlilerinin bilgi, beceri ve tutumlarına vb. dair kamunun algılarına dayanır. Kamusal hizmetler sunan gerçek ve tüzel kişiliği haiz aktörlerin tek tek kişisel ve kurumsal itibarlarını şekillendiren algılardan daha fazlasıdır.

İtibar "soyut" veya "görünmeyen", ama "somut" sonuçları olan bir varlıktır (Er, 2008, s. 11). Somut sonuçlar ortaya çıkarabilme potansiyeli nedeniyle, kamu güvenliğinin sağlanmasından sorumlu olan birimler can ve mal-mülk güvenliğini sağlamak için yaptıkları gibi itibar güvenliğini sağlamak için de görevler icra ederler. Ancak itibar güvenliğinin sağlanması, can ve mal-mülk güvenliğinin sağlanması için kullanılan güvenlik yönetimi stratejilerinden farklı stratejiler gerektirebilir. Elbette can ve mal-mülk güvenliğinin sağlanması sayesinde itibar güvenliğinin de sağlanmış olabileceği durumlar vardır. Ancak can ve mal-mülk güvenliğine zarar vermeden de itibara zararlar verilebilir. Sanal ya da fizikî ortamlarda paylaşılan ve kullanılan dezenformatif içerikler can ve mal-mülk güvenliğine zarar vermeden itibara zarar verebilecek nitelikteki faaliyetler arasındadır. Bu gibi saiklerle itibar güvenliği istihbarat birimlerinin kullanımıyla daha etkili şekilde sağlanabilir. Bu minvalde kamusal itibarın güvenliğinin en iyi şekilde kamu güvenliği ile ilgili istihbarat birimlerini etkin hale getiren, hatta bu birimleri bir mücadele sürecinin merkezine yerleştiren bir güvenlik yönetimi yaklaşımını gerektirdiği değerlendirilmektedir. Çalışmada önerilen işleyiş süreci bu değerlendirmenin ürünüdür.

Çünkü kamusal itibar iktidarların (hükûmetlerin) meşruiyetiyle son derece ilgilidir. Çalışmada kavramlaştırıldığı şekliyle ifade edilecek olursa kamu sektörü tarafında kişi, kurum ve kuruluşlar tarafından sunulan kamusal hizmetler gerekçesiyle vatandaşlar ve diğerleri nazarında oluşan kamusal itibar değerlendirmesi hem kamu yönetiminin hem de hükûmetlerin meşruiyetine etki etme potansiyeli barındırır. Bu durum realist bir tehdit değerlendirmesi olarak kabul edilirse, kamu yönetiminin ve hükûmetlerin kamusal itibar kaybından kaynaklanabilecek meşruiyet sorunlarının önüne geçilmesinin imkânları oluşturulabilir. Kısaca kamusal itibarın güvenliğinin sağlanması hükûmetlerin ve ilgili yönetimlerin ertelenemez nitelikteki yetki, görev ve sorumlulukları arasındadır.

2. Bir Tehdit Bir Seçenek

2.1. Kamusal İtibara Bir Tehdit: Dezenformasyon İçin Hizmet Sabotajı ve Bürokratik Casusluk

Dezenformasyon bir gerçek hakkında başkalarını kasıtlı olarak aldatmak amacıyla içeriklerde eksik, yanlış veya yanıltıcı bilgiler kullanılmasıdır (Fetzer, 2004, s. 228). Avrupa Birliği (AB) kurumları, çeşitli türdeki manipülasyonların yolunu açabileceğine ve başta ifade özgürlüğü olmak üzere temel hak ve özgürlüklere önemli zararlar verebileceğine dair öngörüler nedeniyle dezenformasyonu, önemsenmesi ve yasal ve teknik araçlarla çözüme kavuşturulması gereken bir tehdit olarak kabul etmiştir (Bontridder & Poullet, 2021, s. e32-2). Gerçekten de dezenformasyon, toplumların siyasî, kültürel ve ekonomik yapılarını dönüştürebilecek ve nihayetinde demokratik toplumların temel ilkelerini aşındırabilecek etkiler yaratma potansiyeline sahip bir tehdittir (Montoro-Montarroso vd., 2023, s. 2). Dezenformasyon faaliyetleri devletler güçlendikçe yoğunlaştırılabilmekte, devletlerin demokratik yapıları bu saldırılarla hedef alınabilmektedir. “Psikolojik harp”, “siber ordu” vb. gibi kavramlarla birlikte kullanılarak yapılan semantik eşleştirmeler dezenformasyon amaçlı saldırıların ne kadar büyük bir tehdit olabileceğinin anlaşılmasını sağlayabilir. Böyle bir ortamda Hunt (2021, s. 83-84) siber saldırıların dezenformasyon amacıyla karmaşık biçimde ve ciddiyetle kullanılmasının siber-destekli dezenformasyonla mücadeleyi ulusal güvenliğin önemli meselelerinden biri haline getirdiğini Cavelty ve Wenger’in (2019, s. 1) bazı tespitlerinden yararlanarak ifade eder.

Bu nedenle dezenformasyon kamu yönetiminin önemli bir meselesidir. Eksik, yanlış veya yanıltıcı bilgiler kullanılarak kamu sektörü tarafındaki kişi, kurum ve kuruluşlarca sunulan kamusal hizmetlerin sürekli, kaliteli, yeterli ve ekonomik biçimde sunulmasının kesintiye uğratılabilecek olması, dezenformasyonu önemli bir mesele haline getirmektedir. Çünkü bu halde kamu yönetiminin vatandaşlar ve diğerleri nazarındaki itibarı (kamusal itibar) zarar görebilir. Bu nedenle gerek iç siyasetteki rekabet gerekse devletler arasındaki güç mücadeleleri sürecinde hükûmetlerin ve devletlerinin meşruiyet sorunları yaşamasından fayda sağlayabilecek olan aktörler bu tehdidi etkili biçimde kullanmanın yollarını arayabilirler. Örneğin Harris ve Ogbonna’nın (2002; 2009) “hizmet sabotajı”[4] olarak adlandırdıkları eylemler bu süreçte kasıtlıca gerçekleştirilebilir. Bu eylemler dezenformatif olduğu iddia edilen içeriklerin aslında yanlışlanamaz içerikler olduğu konusunda kabuller oluşmasını kolaylaştırabilir. Bu nedenle hizmet sabotajlarının dezenformasyonun bir aracı olabileceği çok açıktır. Başka bir ifadeyle hizmet sabotajlarının varlığı, bazı içeriklerin dezenformasyon barındırdığına dair iddiaları boşa çıkarabilir. Diğer taraftan dezenformasyonlar için ihtiyaç duyulan bilgiyi temin etmek amacıyla kamu görevlileri kurum ve kuruluşlardaki bürokratik faaliyetlere dair casusluk (bürokratik casusluk) yapmaları için yabancı ülke istihbarat birimleri tarafından teşvik

[4] Harris ve Ogbonna (2002; 2009, s. 326) kuruluşlarda, çalışanların, sundukları hizmetin kalitesini olumsuz yönde etkileyecek kötü niyetli davranışlarda bulunmalarının bir istisna olmadığını, çalışanlar tarafından çeşitli gerekçelerle kasıtlıca gerçekleştirilen bu davranışın ayrım yapmaksızın çok sayıda kuruluşta endişe verici derecede yaygın olduğunu tespit etmişlerdir. Çalışmalarıyla hizmet sabotajının, hizmeti alanlarda memnuniyetsizliklere sebep olduğunu, alınan hizmetin kalitesinde ve ona atfedilen değer düzeyinde düşüşlere yol açtığını ve nihayetinde çalışanlarla hizmeti alanlar arasındaki ilişkiyi yok edebildiğini ortaya koymuşlardır. Bu bağlamda bu sabotajın endüstriyel sabotajdan katbekat daha tehlikeli olduğunu ileri sürerler.

edilebilirler.[5] Bu nedenle bürokratik casusluğun da dezenformasyon için bir araç olarak kullanılabileceği reddedilemez.

Çalışmada önerilen işleyiş sürecinde dezenformasyonla mücadelenin merkezine yerleştirilmiş olan istihbarat birimleri dezenformasyonla mücadele ederken hem kişi, kurum ve kuruluşları oto-kontrole sevk ederek hem de mücadele sürecinde onlara "yakında" bulunarak dezenformasyonun bu iki aracı ile mücadele edebileceklerdir. Başka bir ifadeyle kamu güvenliği ile ilgili istihbarat birimlerinin dezenformasyonla mücadele sürecinde yer alması, dezenformasyonlara katkı sunan bu iki aracın kontrol altında tutulabilmesini, bu sayede dezenformasyonla mücadelenin daha etkin şekilde yönetilebilmesini sağlayabilecektir. Çünkü bu iki araç dezenformasyonlar yoluyla yaratılmak istenen krizleri besleyebilmektedir. Bu krizlere yol açabilecek risklerin yönetilebilmesi kamusal itibarın güvenliğinin sağlanabilmesinin gereğidir.

2.2. Dezenformasyona Karşı Mücadele İçin Bir Seçenek: İstihbarata Dayalı Kolluk

Dezenformasyon tartışmalı bir olgudur. Bu nedenle olsa gerek dezenformasyon nedeniyle yürütülecek mücadelenin nasıl yürütülebileceği konusunda bir uzlaşı oluşmamıştır. Ancak zorunlu gerekçeler bulunması ve meşru bir hak olması hasebiyle Türk Ceza Kanunu'nun "Kamu Barışına Karşı Suçlar" başlıklı beşinci bölümüne 13.10.2022 tarih ve 7418 sayılı Kanun'un 29. maddesiyle eklenmiş olan 217/A maddesinde "Halkı yanıltıcı bilgiyi alenen yayma" başlığı altında dezenformasyon suçu[6] düzenlenmiştir. Bu düzenleme konusunda Balcı ve Çakır (2023, s. 15) suç politikasında hâkim olan ilkeler bakımından tartışmalara sebebiyet verse de düzenlemenin kamu barışını koruma amacına matuf olduğunu; yanlış ve yanıltıcı bilgiyi yayma fiiline yaptırım öngörmesiyle ifade hürriyetini engellemeyi değil, ifade hürriyetinin kötüye kullanılmasını engellemeyi hedeflediğini; suçun manevi unsurunda failin halk arasında endişe, korku, panik vb. yaratmak amacıyla hareket etmesi şartının aranmasıyla suçun oluşmasının aslında zorlaştırıldığını, bu yönüyle kişilerin kanaatlerini açıklama, haber alma/verme haklarına sınırlama getirilmemesine özen gösterildiğini tespit etmişlerdir.

Düzenlemeyle, doğal olarak, dezenformasyon suçunu işleyebilecek olan özneler hedef alınmıştır. Kamusal itibara zarar verebilecek olan dezenformasyon nedeniyle gerçekleştirilen mücadele için bir işleyiş süreci öneren bu çalışma da özne odaklı bir yaklaşıma sahiptir. Bu bakımdan çalışmadaki önerinin dezenformasyon nedeniyle gerçekleştirilen mücadele konusunda ceza kanununda yapılmış olan bu düzenlemeye katkı sunabileceği ifade edilebilir. Önerilen işleyiş sürecinin merkezine yerleştirilen istihbarat birimlerinin çalışmalarıyla iki hususta başarı sağlanabilirse bu katkı somut biçimde gözlenebilir. Başarı sağlanması hedeflenen ilk husus, dezenformasyon yapanlara ve yapacak olanlara gerek kimliklerinin tespit edilmesi gerekse hukukî süreçlerin başlatılması için ihtiyaç duyulacak verilerin elde edilmesi konusunda güçlükler bulunmadığı mesajını vermek ve onlara bu yolla korku salmaktır.

[5] Hükûmetlere muhalif siyasî ve ideolojik kimliğe sahip olmak, hükûmetler aleyhinde yıkıcı, yıpratıcı vb. faaliyetler gerçekleştirmeye kişisel olarak istekli olmak, hükûmetleri yıkıcı, yıpratıcı vb. faaliyetler gerçekleştiren aktörlerle iş birliği içinde bulunmak vb. gibi haller bürokratik casusluğu var edebilmektedir. Bu nedenle kamusal itibara zarar vererek hükûmetlerin meşruiyetini zedeleme amacını başarmak isteyen bu türdeki aktörlere karşı verilecek mücadele, kamu güvenliği ile ilgili istihbarat birimlerini etkinleştirmeyi gerektirmektedir. Bu mücadele hukuk sınırları içerisinde kalarak gerçekleştirildiğinde meşruiyeti de tartışılmaz. Nitekim Millî İstihbarat Teşkilatı'nın (MİT) (2024) kendi web sitesinden yayımladığı bir video casusluk ile ilgilidir. MİT bu videoda "casusluğun sıklıkla başvurulan bir faaliyet olduğuna", "hasım veya hasım olması muhtemel (yabancı) istihbarat mensuplarının Türk vatandaşlarıyla çeşitli yöntemlerle irtibat kurup onları casus olarak devşirdiklerine" ve "devşirdikleri casuslardan çeşitli bilgiler istediklerine" dikkat çekmiştir. Video; casusluğun türleri, gerçekleştirildiği yerler, gerçekleştirilme yöntemleri vb. gibi hususlarda ayrıntılı bilgi içermese de bir casusluk türü olarak bürokratik casusluğun varlığını düşündürmektedir. Çünkü yabancı istihbarat mensupları tarafından casus olarak devşirilmek istenenler arasında, bürokrasi içerisinde kamu kurum ve kuruluşlarında kamu görevlisi ve memur olarak görev yapan kişiler de bulunabileceği düşüncesini uyandırmaktadır. Video, herkes gibi memurların ve kamu görevlilerinin de casusluk yaptırmak için kullanılabilecekleri fikrini üretmektedir. Gerek bu nedenle gerekse casusluğun amacı dikkate alındığında bürokratik casusluğu yadsımak ya da "kanıtlanamaz bir olgu" olarak görmek rasyonel değildir. Bürokratik casusluğun kamusal hizmetler sunan kurum ve kuruluşlardaki varlığı inkâr edilemez.

[6] Maddenin birinci fıkrası "Sırf halk arasında endişe, korku veya panik yaratmak saikiyle, ülkenin iç ve dış güvenliği, kamu düzeni ve genel sağlığı ile ilgili gerçeğe aykırı bir bilgiyi, kamu barışını bozmaya elverişli şekilde alenen yayan kimse, bir yıldan üç yıla kadar hapis cezasıyla cezalandırılır."; ikinci fıkrası ise "Fail, suçu gerçek kimliğini gizleyerek veya bir örgütün faaliyeti çerçevesinde işlemesi hâlinde, birinci fıkraya göre verilen ceza yarı oranında artırılır." hükümlerini amirdir.

İkinci husus ise kamu kurum ve kuruluşlarında görev yaparken hizmet sabotajları ve bürokratik casusluklar gerçekleştirebilecek olan kamu görevlilerine ve memurlara varlıklarını hissettirerek korku salmak suretiyle onları kontrol altında tutmaktır. Bu sürecin hukuk sınırları içinde yürütülmesi demokratik bir hukuk devleti olarak kalabilmenin şartıdır. Ancak ifade edildiği üzere bunun meşru bir hak olduğu da göz ardı edilmemelidir.

Bu başarı güvenlik birimleri tarafından yerine getirilecek görevlerin, dezenformasyonun öznelerinin istihbarat çalışmalarıyla tespit edilmesine "dayalı" olmasıyla başarılabilir. Başka bir ifadeyle kamusal itibara zarar verecek nitelikteki dezenformasyonun öznelerini tespit etmek amacıyla güvenlik birimleri tarafından gerçekleştirilecek istihbarat faaliyetleri sürecin başarılı biçimde işlerliğinin gereğidir. Bu bakımdan sürecin istihbarat anlayışı çalışmaya özgüdür ve Türk Ceza Kanunu'nun 217/A maddesinin umduğu caydırıcılığın sağlanmasına katkıda bulunabilir.

Sürecin istihbarat anlayışı, proaktif güvenlik yönetimi yaklaşımı gereğince geliştirilmiş olan "istihbarat odaklı polislik" stratejisini çağrıştırsa da ondan farklıdır. Kelling ve Bratton (2006, s. 5) istihbarat odaklı polisliği, veri elde etme ve analiz etme yoluyla gerçekleştirilen bir suçla mücadele stratejisi olarak tanımlarlar. Proaktif bir yaklaşım dahilinde suçun önlenmesi, azaltılması, kesintiye uğratılması ve ortadan kaldırılması bu stratejinin amaçları arasındadır (OSCE, 2022, s. 10). Bu stratejinin suçla mücadelede özgün bir yönetim felsefesine sahip olduğunu ifade eden Ratcliffe (2008, s. 89) istihbarat odaklı polislik stratejisinde suçlara dair veri analizleri gerçekleştirilmesinin nedenini "belirli suçlara karşı tedbirler geliştirmek suretiyle o suçları önlemek" olarak açıklar. Ancak istihbarat odaklı polislik stratejisinin bu amaçları başaracak şekilde işleyemediği konusunda görüşler gelişmiştir. Örneğin James (2013, s. 1-2) bu stratejinin gerçek anlamının tam olarak belirlenemediğini iddia eder ve kafa karıştırıcı bir şekilde kullanılabildiğini ileri sürer. İncelemeleri neticesinde "Belki de reaktif polislik baskın yaklaşım olmaya devam ediyor." (James, 2013, s. 206) diyerek istihbarat odaklı polislik stratejisinin suçla proaktif yaklaşım çerçevesinde mücadelede yeterince etkili olmayı başaramadığını ifade etmiştir.

Bu başarısızlığın nedenlerini incelemek bu çalışmaya katkı sağlamayacaktır. Ancak James'in istihbarat odaklı polisliğe dair sözü edilen değerlendirmesinden hareketle bazı suçlarla mücadelenin proaktif yaklaşımlarla başarılmasının zor olabileceği, örneğin istihbarat odaklı polisliğin "olmadan önleme"nin amaç olduğu her durumda kullanılamayacağı sonucuna ulaşılabilir. Dezenformasyon suçu bu türde bir suçtur. Dezenformasyonun gerçekleşmeden önce tespit edilemeyeceği, başka bir ifadeyle dezenformatif içeriğin çevrimiçi ortamlarda dolaşıma girmeden önce tespit edilebilmesinin olanaklı olmadığı değerlendirilmektedir. Gül Ünlü ve Küçükşabanoğlu'nun (2023) dezenformasyonla mücadelede hâlihazırdaki yapay zekâ sistemlerinin potansiyelini yapay zekâ uzmanlarıyla mülakatlar gerçekleştirerek anlamaya çalıştıkları araştırma bunun cevabını vermektedir: "Dolaşıma giren dezenformasyonla yapay zekâ sistemleri kullanılarak mücadele edilebilir, ancak yapay zekâ sistemleri çevrimiçi ortamlarda dezenformasyonun dolaşıma girmesini engelleyemez." Şu hâlde suça odaklanmayı ve suça dair analizler gerçekleştirmek suretiyle suçla mücadele etmeyi önemli gören istihbarat odaklı polisliğin ya da yapay zekânın kamusal itibara zarar verecek nitelikteki dezenformasyonla mücadelede kullanılmasının makul görülmediği ifade edilebilir. Çünkü istihbarat odaklı polisliğin dezenformasyona karşı proaktif yaklaşım çerçevesindeki mücadelesine umut bağlanamaz. Bu mücadelenin başarısının ölçülebilir olmaması ya da elde edildiğinde başarının somut verilerle açıklanamaması da bunun gerekçeleri arasındadır. Ancak kamusal itibara zarar verebilecek nitelikteki dezenformasyonlara karşı proaktif yaklaşımlar çerçevesinde sürdürülebilecek mücadele mutlak surette dışlanamaz. Zira bu türdeki mücadele süreçlerinde elde edilen başarı "hedeflenmemiş" olsa da açıkça "olumlu bir sonuç"tur. Böyle bir sonuca ulaşılmasına istihbarat odaklı polislik stratejisinin etki edip etmediği ya da stratejinin hangi teknik ve taktiklerinin katkı sağladığı net olarak bilinemese de bu sonuç memnuniyet vericidir. Bu nedenle dışlanamaz. Hâl böyle iken "istihbarata dayalı kolluk"

tarafından gerçekleştirilecek çalışmaların "olmadan önleme" amacına matuf sonuçlar da üretmesi mümkündür. Asıl amaç bu olmasa da istihbarata dayalı kolluk faaliyetleri bunu da sağlayabilir.

Ancak bu çalışmada önerilen işleyiş sürecinde, proaktif yaklaşımlar çerçevesinde suçun değil, reaktif yaklaşımlar çerçevesinde suçu işleyen öznelerin istihbaratının yapılması önemli görülmüştür. Başka bir ifadeyle bu çalışma suç sayılan "eylemin istihbaratının yapılmasını" değil, suç sayılan "eylemi gerçekleştiren öznelerin istihbaratının yapılmasını" dezenformasyon nedeniyle gerçekleştirilen mücadelenin gereği olarak kabul etmektedir. Güvenlik birimlerinin dezenformasyon nedeniyle gerçekleştirmesi gereken faaliyetlerin suça dair önceden istihbarat elde ederek değil, suç işleyen özneler hakkında sonradan istihbarat elde edilmesi amacıyla yürütülmesi çalışmada önerilen işleyişin temelidir. Başka bir ifadeyle önerilen işleyişte dezenformasyon nedeniyle gerçekleştirilen mücadelenin reaktif yaklaşımlar çerçevesinde yürütülmesi esastır. Dezenformasyonu gerçekleştirenlerin veya hizmet sabotajları ve bürokratik casusluk yoluyla dezenformasyonu besleyenlerin Türk Ceza Kanunu'nun 217/A maddesi gereğince cezalandırılacakları konusunda işleyiş sürecinde verilecek mesajlar ve gerçekleştirilecek uygulamalar dezenformasyon nedeniyle gerçekleştirilen mücadelede etkili sonuçlar alınmasını sağlayabilir. Bu nedenle bu çalışma alan yazında "istihbarat odaklı polislik" biçiminde kavramlaştırılmış olan stratejinin değil, dezenformasyona münhasır özellikler nedeniyle güvenlik birimlerinin istihbarat çalışmalarının dezenformasyon gerçekleştikten sonra özneler üzerinde kullanımını bu mücadelenin gereği olarak görmektedir.

Mücadelenin bu minvalde sürdürülmesi sayesinde, bir yandan gerçekleşen dezenformasyonlarla somut alanda mücadele edilirken, diğer yandan soyut alanda yeni dezenformasyonların gerçekleşmesinin önüne geçilebilecektir. Somut alanda gerçekleştirilen mücadelede özneler üzerinde yaratılan korku ikliminin cezasızlık algısını bertaraf edebilmesi, soyut alanda da başarı sağlanabilmesini mümkün kılabilecektir. Bu minvalde, dezenformasyon nedeniyle gerçekleştirilen mücadelenin *"dezenformasyonla mücadele" değil, "dezenformasyona karşı mücadele"* biçiminde kavramlaştırılmasının isabetli olacağı değerlendirilmektedir. Bu bir "*kamusal itibara zarar verecek nitelikteki dezenformasyon nedeniyle yürütülen mücadele sürecinde reaktif temeldeki yaklaşımların kullanılması sayesinde dezenformasyona karşı aynı anda proaktif temelde mücadele etme*" durumu olarak betimlenebilir. Çünkü suçlar işlendikten sonra gerçekleştirilecek etkili müdahalelerin gelecekte aynı türde suçların işlenmesini önleyebileceğine dair varsayım oldukça gerçekçidir.

3. Türkiye'de Kamusal İtibarın Güvenliği İçin Dezenformasyona Karşı Mücadele

Türkiye, enformasyonun bir silah olarak kullanılmasına, sosyal medya botlarına, trollere ve büyük ölçekli algoritmalar yoluyla üretilen bilişsel tehditlere karşı zafiyetleri en fazla olan ülkelerden biridir (Kırdemir, 2024, s. 1). Oxford Üniversitesi tarafından 2018 yılında 37 ülkede gerçekleştirilen bir araştırma, dezenformasyona ve yalan habere en çok maruz kalan ülkelerden birinin yüzde 49 oranıyla Türkiye olduğunu göstermiştir (Yanatma, 2018, s. 26). Bu durum Türkiye Cumhuriyeti Devleti tarafından dezenformasyona karşı mücadele konusunda hâlihazırda gerçekleştirilen uygulamaların etkililiğinin artırılmasına yönelik arayışları meşrulaştırır. Çünkü içinde bulunulan post-modern dönemin özellikleri nedeniyle dezenformasyonların etki gücünün gelecekte artış gösterebileceği öngörülebilir.

Türkiye Cumhuriyeti Cumhurbaşkanlığı İletişim Başkanlığı bünyesindeki Dezenformasyonla Mücadele Merkezi'nin (DMM) kamusal itibarın güvenliğinin sağlanması için dezenformasyona karşı mücadele konusunda etkili çalışmalar yapıp yapamadığını sosyal medya platformu "X" adlı sosyal medya platformundaki paylaşımları üzerinden inceleyerek değerlendirebilmek mümkündür. X platformunda DMM tarafından yapılan gönderilerde "*Bazı sosyal medya hesaplarından paylaşılan …*", "*Bazı basın yayın organlarında yer alan …*" ya da "*…'nin resmî yetkilileri tarafından ortaya atılan …*" biçiminde öznesi belirsiz ifadeler kullanıldığı görülebilir. Bu ifadelerin yer aldığı paylaşımlarda "*bilginin doğru*

olmadığı", "*bilginin toplumu yanıltma amacı taşıdığı*" vb. açıklanmakta ve doğru bilgi verilmektedir. Ancak DMM'nin bu paylaşımlarına X kullanıcıları tarafından verilen yazılı tepkiler incelendiğinde DMM'nin eleştirilere maruz kaldığı görülmektedir. Bu eleştirilere yakından bakıldığında bilginin yanlış olduğuna dair DMM tarafından yapılan açıklamaların kullanıcılar tarafından tatmin edici bulunmadığı, DMM tarafından yapılan açıklamanın dezenformatif olduğu iddia edilen içeriği yanlışlayamayıp neredeyse doğruladığının düşünüldüğü, DMM'nin bu türdeki açıklamalarının sürekliliğine rağmen dezenformasyon üretilmesinin önüne geçilemediği kanaatinin oluştuğu ve bu nedenle bunun bir başarısızlık olarak kabul edilmesi gerektiğinin değerlendirildiği, DMM'nin bu çalışmalarına X kullanıcıları tarafından saygı gösterilmediği vb. görülmektedir. Dezenformatif içeriği üretenlerin tespit edilmesinin ve onlara karşı korku salacak yöntemler kullanılmasının dezenformasyonla mücadele edilebilmesi için gerekli olduğu kanaati X kullanıcıları arasında yaygındır.

Bu sorun, kamu sektörü tarafında kamusal hizmetler sunan kişi, kurum ve kuruluşları hedef alarak kamusal itibara zarar verebilecek olan dezenformasyona karşı mücadele etmek için Şekil-1'de sunulan altı aşamalı bir işleyiş sürecinin kullanılabilirliğini bir seçenek haline getirmektedir. Bu işleyiş süreci Türkiye Cumhuriyeti Cumhurbaşkanlığı İletişim Başkanlığı bünyesindeki Dezenformasyonla Mücadele Merkezi (DMM) tarafından dezenformasyon nedeniyle hâlihazırda gerçekleştirilmekte olan çalışmaların etkililiğini artırabilir. Süreç, bunu, Machiavelli'in tavsiyesinde yer alan "korku salma" ve "sevgi oluşturma" amaçlarının aynı anda başarılmasını sağlayarak yapabilecektir. Önerilen süreç; çalışmalarda hangi kurumdan kaç temsilci bulunması, çalışmaların hangi ortamlarda (fizikî ya da sanal) yürütülmesi, kimlerle iş birlikleri yapılması, kararların nasıl alınması, hangi aşamalardan geçirilerek yayımlanması gerektiği vb. gibi ayrıntılı hususları, prosedürleri, işlem basamaklarını vb. içermez. Süreç, organizasyonda yer alabilecek aktörler konusunda da kesin bir söyleme sahip değildir. Ancak koordinasyon görevini Dezenformasyonla Mücadele Merkezi'ne verir. İçişleri Bakanlığı'na bağlı Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı bünyesindeki istihbarat birimlerini ise sürecin merkezî unsurları olarak görür. Bu merkezî unsurlar Machiavelli'in tavsiyesinde yer alan "korku salma" amacını DMM'nin koordinesi altında yürütülecek çalışmalar sayesinde başarabilecek aktörlerdir. Süreç, kamusal hizmetleri sunan kişi, kurum ve kuruluşların Bakanlık düzeyindeki temsilcilerine de alan açar. Çünkü onlar Machiavelli'in tavsiyesinde yer alan "sevgi oluşturma" amacını başarmak için çalışmalar yürütecek aktörlerdir. Bilgi Teknolojileri ve İletişim Kurumu (BTK) da süreç önerisinde gerekli görülmüş olan aktörlerden biridir.

Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı bünyesindeki istihbarat birimlerinin bu süreçteki en önemli misyonları kamusal itibara zarar verecek nitelikte dezenformasyon yapanlara kontrollü biçimde korku salmaktır. Ancak bu korku salma işi açık ya da kapalı biçimde tehdit etme gibi yöntemler içermemelidir. Çünkü bu tür yöntemler kişilerin hükûmetlere, güvenlik birimlerine, ilgili kişi, kurum ve kuruluşlara karşı olumsuz tutumlar geliştirmelerine sebep olabilir. Korku salma amacına matuf faaliyet "yapıcı bir uyarı" niteliğinde olmalıdır. Bu sayede itidallı bir süreç işletilebilecektir. Her şeye rağmen bu süreçte oluşabilecek gerilimli zamanlarda hassas dengeyi kurabilmek önemli olacaktır. Önerilen işleyiş sürecinde dezenformasyonun hedefinde olan kişi, kurum ya da kuruluşların bazı rollerle öne çıkarılarak aktif görevler icra etmelerinin bu dengenin kurulabilmesini sağlayabileceği değerlendirilmektedir. Kısaca bu süreç kamusal itibara zarar verebilecek olan dezenformasyon faaliyetlerinin sürekli ve sistematik biçimde takip edildiğini, bu türdeki faaliyetlerin suç olarak tanımlanmış bulunduğunu, bu nedenle müsaade edilmeyeceğini, gerektiğinde tüm hukukî tedbirlere başvurulacağını, yapılan dezenformasyonun hata olduğunun özneleri tarafından kabul edilmesi halinde ise ceza tedbirlerinin işletilmeyeceğini kurumsal bir yaklaşımla deklare edecek olan bir süreçtir. Devleti yapıcı, bağışlayıcı, inşa edici bir aktör olarak öne çıkarmak bu sürecin felsefî temelidir. Bu felsefî temel vatandaşlar ve diğerleri ile hükûmetler arasındaki gerilimleri büyütmemeyi ve yeni gerilimler yaratmamayı esas tutar. Dezenformasyon yoluyla suç işlenmiş de olsa hemen hukukî yola

başvurmamak, suç olduğunun özneler tarafından fark edilmesi için fırsatlar yaratmak ve bir hata yapıldığının hatayı yapan özneler tarafından ilânı halinde sorunu kapatmak esas olmalıdır. Hukukî yollara başvurmak son çare olarak görülmelidir. Çünkü Ciarlone ve Wiechmann'ın (2003, s. 62) dikkat çektiği üzere, hakkında hukukî yollara başvurulanlar hırslanabilirler, bunun sonucunda dezenformasyon faaliyetlerine farklı konularda devam edebilirler ve bunları yapabilmek için yeni yollar arayabilirler. Bu durum kişi, kurum ve kuruluşlar hakkında toplumda daha fazla yanlış bilgi yayılmasına da yol açabilir.

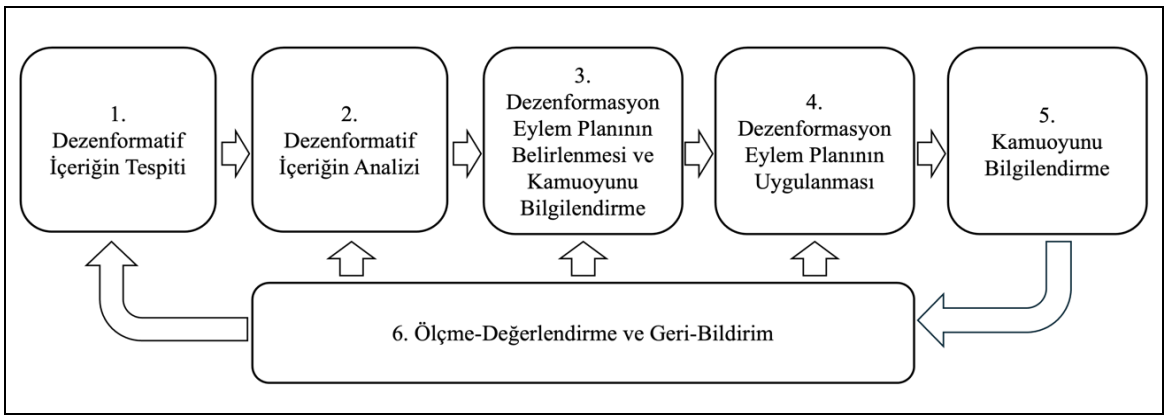
Önerilen bu işleyiş süreci reaktif güvenlik yönetimi yaklaşımına dayanır. Bu güvenlik yönetimi yaklaşımında dezenformasyon gerçekleştiren özneleri tespit etmek esastır. Süreç başarılı biçimde işletilebildiğinde, bir yandan gerçekleşmekte olan dezenformasyon faaliyetlerine karşı öznelerin tespiti suretiyle mücadele edilirken diğer yandan bu mücadelede elde edilen başarı sayesinde yeni dezenformasyonlar gerçekleşmesinin önüne geçilebilecektir. Başka bir ifadeyle bu süreç reaktif güvenlik yönetimi yaklaşımlarını etkili biçimde kullanmak suretiyle dezenformasyonla mücadele ederken, dezenformasyona karşı mücadeleyi proaktif güvenlik yönetimi yaklaşımları temelinde de sürdürmektedir. Bu yönüyle süreç, "olabilecek/gerçekleşebilecek" olanı, olanlara/gerçekleşenlere karşı yürüttüğü mücadelenin etkililiği sayesinde "önlemeyi" hedeflemektedir. Süreçte proaktif güvenlik yönetimi yaklaşımındaki "olmadan önleme" anlayışı bu minvalde anlam kazanmaktadır.

Çalışmada önerilen süreç "gerçeklik" üzerine kuruludur. Dezenformasyon faaliyetleri gerekçesiyle gerçekleştirilen mücadele sürecinde ya da sonunda özneler tarafından hangi dezenformasyonun hata olduğunun kabul edildiği, hangi dezenformasyon karşısında ne tür iş ve işlemler yapıldığı ve nihayetinde ne kadar başarı sağlanabildiği vb. somut şekilde ölçülebildiğinde dezenformasyonla mücadelenin başarılı olup olmadığı tespit edilebilecektir. Bu da özelde dezenformasyonla mücadele sürecini, genelde ise kamusal itibarın güvenliğinin sağlanabilmesi sürecini yönetmeyi kolaylaştırabilecektir. Bu bakımdan bu işleyiş süreci hem dezenformasyona karşı mücadeleyi başarabilecek hem de bu mücadelenin etkililiğini ölçebilecek bir yönetim faaliyeti olarak tasarlanmıştır. Bu iki başarının bu süreç sayesinde aynı anda elde edilmesinin hem kamu yönetiminin vatandaşlar ve diğerleri nazarındaki meşruiyeti hem de hükûmetlerin gücü açısından önemli kazanımlar sağlayacağı ifade edilebilir.

3.1. İşleyiş Süreci Önerisi

"Kamu sektörü tarafındaki kişi, kurum ve kuruluşlarca sunulan kamusal hizmetlerin sürekli, kaliteli, yeterli ve ekonomik biçimde sunulmasını kesintiye uğratabilecek ya da vatandaşlar ve diğerleri nazarında kamusal hizmetlere dair olumsuz algılar oluşmasına sebep olabilecek nitelikteki yanıltıcı ve yanlış bilgiler" bu çalışmanın odağındaki dezenformasyon türüdür. Dezenformasyonun bu türüne karşı mücadele etmek için bu çalışmada önerilen işleyiş süreci Şekil-1'de görülmektedir.

Şekil 1: *Dezenformasyona Karşı Mücadele Süreci*



Altı aşamalı bu sürecin her bir aşaması için öngörülen ve aşağıda ayrıntılı biçimde açıklanan iş ve işlemlerin yerine getirilmesi suretiyle dezenformasyonun bu türüne karşı başarılı şekilde mücadele edilebileceği değerlendirilmektedir.

Birinci Aşama: Dezenformatif İçeriğin Tespiti

Sürecin bu ilk aşamasında dezenformatif olduğu değerlendirilen içerikler tespit edilmelidir. Bu tespit için bu süreçte yer alan birimler ve/veya o birimlerdeki alt birimler tarafından gerekli yöntem, teknik ve araçlar kullanılabilir. Sanal devriye, kişisel ve kurumsal çalışmalar vb. bu amaçla kullanılacak yöntem, teknik ve araçlar arasındadır. Yapay zekâ da bu aşamada kullanılabilir. Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) çalışmalarından ve kabiliyetlerinden bu aşamada yararlanmak mümkündür.

Bu aşamada gerçekleştirilmesi önerilen işlem, dezenformasyon nedeniyle istihbarat birimleri tarafından suç soruşturması yapmak veya o suçu işlediği değerlendirilen özneler hakkında hukuka aykırı biçimde kişisel veriler elde etmeye çalışmak ya da delil toplamak değildir. Bu aşamada önerilen işlem, özneleri ve onların faaliyetlerini usulsüz biçimde takibe alma işlemi de değildir. Başka bir ifadeyle bu aşamada Cumhuriyet Savcısı'nın görev ve yetkilerine mugayir bir iş/işlem yapılması önerilmez. Burada önerilen işlem hakkında Anayasa Mahkemesi'nin "sanal devriye" konusunda verdiği bir karar üzerinden açıklama yapmak isabetli olur.

2559 sayılı Polis Vazife ve Salâhiyet Kanunu'na 2017 yılında eklenen bir madde polise ve jandarmaya sanal ortamda işlenen suçlarda suç araştırması yapma (sanal devriye) yetkisi vermişti. Ancak bu yetkiyi düzenleyen madde Anayasa Mahkemesi tarafından Anayasa'nın 13. ve 20. maddelerine aykırı görülmüş, bireyin özel hayatının gizliliğinin ihlâline sebep olacağı ve kişisel verilerin korunmasının ihlâline yol açacağı gerekçeleriyle Mahkeme'nin 19.02.2020 tarih ve 2018/91 E., 2020/10 K. sayılı kararıyla iptal edilmişti. Bu çalışmada önerilen işleyiş sürecinin ilk aşamasında dezenformatif içeriğin tespiti amacıyla sanal ortamlarda yapılması önerilen faaliyet Anayasa Mahkemesi'nin iptal kararına konu olan bu türde bir faaliyet değildir. Bu faaliyet gerek kolluk gerekse işleyiş sürecindeki diğer aktörler tarafından sanal ortamda dezenformatif içerikli paylaşımlara ulaşmak amacıyla gerçekleştirilecek basit bir araştırmadan ibarettir. Nitekim bu türdeki araştırmalar hâlihazırda güvenlik birimleri tarafından yapılmaktadır. Daha açık bir ifadeyle bu faaliyet herhangi bir kişinin sanal ortamda yapabileceğinden daha fazlası değildir. Suça ilişkin kanıtlar bulmak ya da suç işlediği değerlendirilenler hakkında kişisel veriler elde etmek bu faaliyetin amacı değildir. Önerilen işleyiş sürecinin ikinci aşaması olan "dezenformatif içeriğin analizi"ne veri sağlamak bu faaliyetin yegâne saikidir.

Dolayısıyla önerilen işleyiş sürecinin bu ilk aşamasında sözü edilen "sanal devriye" yasaldır; çünkü dezenformasyon olabileceği değerlendirilen bir içeriğin varlığının tespit edilmesinden ibarettir. Nitekim

bir içeriğin kamusal itibara zarar verebilecek nitelikte bir dezenformasyon olup olmadığı, önerilen işleyiş sürecinin ikinci aşamasında yapılacak analizle tespit edilecektir. Bu nedenle dezenformasyon olabileceği değerlendirilen bir içeriğin sanal ortamdaki varlığının tespit edilmesi amacına matuf olan sanal devriye konusunda gerekliyse yasal düzenlemeler de gerçekleştirilmelidir. Anayasa Mahkemesi'nin sözü edilen kararının bu çalışmada ifade edilen sanal devriye ile uyumlu olmadığı değerlendirildiğinden, kamusal itibara zarar verecek nitelikteki dezenformasyona karşı bu yöntemin ve ilgili araçların kullanılmasında sakınca görülmemektedir. Başka bir ifadeyle bu çalışmada önerilen işleyiş sürecinin kamusal itibarın güvenliğini sağlamak amacıyla kullanılabilirliği, sanal devriyenin hukuka aykırı bir yetki/uygulama olmadığının, AYM'nin sözü edilen kararına konu olan sorunları da içermediğinin kabulünü gerektirmektedir. Bu değerlendirme, çalışmaya temel teşkil eden Machiavelli'in "korku salma" amacı ile de uyumludur.

Dezenformasyon içeren durumlarda sanal ortamda vatandaşlar ve diğerleri tarafından gerçekleştirilebilecek ihbarlar/şikâyetler için kolay ve etkili biçimde kullanılabilecek başka mekanizmalar da bu aşamada dezenformatif içeriğin tespiti için düşünülmelidir. Bahar'ın (2020, s. 2785-2786) suç olabildiği düşünüldüğü için sosyal medya kullanıcıları tarafından etiketleme yapılarak gerçekleştirilen ihbar niteliğindeki paylaşımların gönderilebileceği bir "Güvenlik Portalı" oluşturulmasına dair önerisi bu aşamada dikkate değerdir. Güvenlik Portalı önerisinin altında yatan gerekçe çok sayıda sosyal medya kullanıcısını bir nevi sanal devriye operatörü haline getirmenin dezenformasyona karşı mücadeleye sağlayabileceği katkılardan yararlanma isteği olsa da portalın, işleyiş sürecinin bu ilk aşamasında dezenformatif içeriğin tespiti için kullanılabilecek önemli bir kanal/araç olabileceği değerlendirilmektedir. Ayrıca bu şekilde alınan ihbarların/şikâyetlerin, önerilen işleyiş sürecinin diğer aşamalarında gerçekleştirilebilecek çalışmalara da hukukî temel sağlayacağı değerlendirilmektedir.

İkinci Aşama: Dezenformatif İçeriğin Analizi

Bu aşamada, daha önce tespit edilmiş olan dezenformatif içeriğin kamusal itibara zarar verme amacı taşıyan bir içerik olup olmadığı analiz edilmelidir. Bu analiz işleminin, içinde hukukçuların yer alacağı bir çalışma grubu tarafından gerçekleştirilmesi elzemdir. Bu analiz için yapay zekâ da kullanılabilir. Gül Ünlü ve Küçükşabanoğlu'nun (2023, s. 87) konuyu yapay zekâ uzmanlarının görüşleri üzerinden inceleyen çalışmalarının da ortaya koyduğu üzere dezenformasyonun üretilip yaygınlaştırılmasında kullanılabilen yapay zekâ, sorunlu içeriğin analizinde de kullanılabilir. Kamusal itibara zarar verme amacı taşıdığı anlaşılan içerik bu işleyiş süreci için değerlendirmeye alınacak, diğer amaçlarla ilişkilendirilen içerikler ise bu çalışmanın kapsamı dışında tutulacak şekilde ayrıştırılacaktır. Ayrıştırılan içerikler, gerekli görülmesi halinde başka süreçlerde kullanılabilir.

Bu aşamada bir dezenformatif içeriğin kamusal itibara zarar verme amacı taşıyıp taşımadığını belirlemek için kullanılabilecek ölçütlere ihtiyaç duyulacaktır. Bu ölçütlerden biri kamu sektörü tarafında kamusal hizmetler sunan kişi, kurum ve kuruluşların Türkiye Cumhuriyeti Devleti'nin kanunlarında suç olarak tanımlanmış olan eylemleri gerçekleştirmekle veya varlık gerekçeleriyle uyumlu olmayan faaliyetler içerisinde bulunarak kamu yararına aykırı hareket etmekle suçlanmaları olabilir. Bu türdeki suçlamalar somut ve tanımlanmış olmalıdır. Bundan başka 657 sayılı Devlet Memurları Kanunu'nun "Sadakat" başlıklı 6.maddesi ve "Tarafsızlık ve Devlete Bağlılık" başlıklı 7.maddesindeki esaslar ile Türkiye Cumhuriyeti Anayasası'nın memurların ve diğer kamu görevlilerinin devlete sadakat yükümlülüğünü düzenleyen "Memurlar ve diğer kamu görevlileri" başlıklı 129.maddesindeki hususlar bu aşamada kullanılacak ölçütler olarak kabul edilebilir.

Üçüncü Aşama: Dezenformasyon Eylem Planının Belirlenmesi ve Kamuoyunu Bilgilendirme

Bu aşama dezenformasyon olduğuna karar verilen içerikler nedeniyle gerçekleştirilecek çalışmaların belirlenmesini ve o çalışmalar hakkında kamuoyunun önceden bilgilendirilmesini içerir. İstihbarat birimleri bu süreçte Dezenformasyonla Mücadele Merkezi'yle birlikte eylem planının belirlenmesinin, dezenformasyonun hedefindeki kişi, kurum ve kuruluşlar ise eylem planı hakkında önceden kamuoyunun bilgilendirilmesinin sorumluları olmalıdırlar. Dezenformasyonla Mücadele Merkezi hem istihbarat birimlerinin hem de kişi, kurum ve kuruluşların bu aşamadaki çalışmalarını koordine etmekle görevli olmalıdır. Dezenformasyonla Mücadele Merkezi "koordinasyonu sağlama" görevine ek olarak bu aşamada kullanılacak içerikler için metin oluşturma ve dilbilgisi desteği de sunmalıdır. Metinlerin nihaî halleri Dezenformasyonla Mücadele Merkezi'nin onayından geçmelidir.

İstihbarat birimleri tarafından dördüncü aşamada kullanılacak metinler bu aşamada hazırlanırken "yapıcı uyarılar" içerecek olmasına özen gösterilmelidir. Çünkü işleyiş sürecinin amaçlarından biri "korku salmak" olsa da zorunlu olmadıkça ceza gerektiren tedbirlere başvurmamaya çalışmanın esas olduğu gösterilmelidir. "Kamu yararının gerektirdiği her türlü iş ve işlem hukukî temelde gerçekleştirilecektir." biçimindeki bir mesaj işleyiş sürecinin bu aşamasında tehditkâr olmayan yapıcı bir yaklaşımla verilecek şekilde hazırlanmalıdır. Dezenformasyonun hedefindeki kişi, kurum ve kuruluşlar tarafından bu aşamada yapılacak kamuoyu bilgilendirmelerinde ise o ana kadar gerçekleştirilen çalışmalardan kısaca söz edilmeli, dezenformasyonu yapanların düzeltici faaliyetlerinin beklendiği açıklanmalı ve aksi halde Cumhuriyet Savcılığı'na suç duyurusunda bulunularak yasal sürecin başlatılabileceği ilân edilmelidir. Bu bilgilendirmelerde "yapıcı açıklamalar" yer almalıdır. Dezenformatif içeriğin makul bir süre içerisinde dezenformasyonu yapanlar tarafından düzeltilmesi, kaldırılması vb. gibi durumlarda kamuoyu bir kez daha kişi, kurum ve kuruluşlar tarafından bilgilendirilmeli ve sanal ortamda yapılacak bu bilgilendirme metninde "doğrunun anlaşılması için gösterdikleri erdemli davranıştan dolayı" teşekküre yer verilmelidir.

Dördüncü Aşama: Dezenformasyon Eylem Planının Uygulanması

İstihbarat birimleri bu aşamada öne çıkmalıdır. Dezenformatif içerikler bu aşamada istihbarat birimlerine ait sanal ortam hesaplarından herkese açık şekilde paylaşılmalıdır. Bu paylaşımlarda dezenformasyon olduğu değerlendirilen içerikler Dezenformasyonla Mücadele Merkezi tarafından uygulanagelen "Bazı sosyal medya hesaplarından paylaşılan …", "Bazı basın yayın organlarında yer alan …" ya da "…'nin resmî yetkilileri tarafından ortaya atılan …" biçimindeki söylemlerle ifade edilmemeli, paylaşımı yapmış olan öznelerin paylaşımı yaparken kullandıkları ve/veya açıkça bilinen isimlere bu paylaşımlarda açıkça yer verilmelidir. Nitekim Dezenformasyonla Mücadele Merkezi'nin X isimli sosyal medya hesabından yaptığı birçok paylaşım, paylaşımı yapan özneleri içermediği gerekçesiyle X platformunda kullanıcılar tarafından eleştirilmektedir. İstihbarat birimleri tarafından yapılacak bu tür paylaşımlar, öznelerin tespit edildiği/edilebileceği algısı oluşturarak bir yandan gerçekleşen dezenformasyonlarla mücadele edilmesini, bir yandan da yeni dezenformasyonların gerçekleşmeden önlenmesini sağlayabilecektir. Türk Ceza Kanunu'ndaki düzenleme gereğince dezenformasyona müsamaha gösterilmeyeceği, gerektiğinde hukukî süreçlerin başlatılacağı vb. konularında istihbarat birimleri tarafından yapılacak bu türdeki bilgilendirmeler dezenformasyona karşı mücadelenin başarı şansını artırabilir. Dezenformasyonla Mücadele Merkezi bu aşamada da metin oluşturma, dilbilgisi desteği sunma vb. gibi görevleri yerine getirebilir.

Bir önceki aşamada istihbarat birimleri tarafından sanal ortamlarda herkese açık şekilde yapılan uyarı ve bilgilendirme paylaşımları dezenformasyonu yapanları bu aşamada özel olarak da hedef almalıdır. Başka bir ifadeyle dezenformasyonu yaptığı tespit edilen ve herkese açık şekilde yapılan paylaşımlarla yapıcı biçimde daha önce uyarılmış olanlar, bu aşamada, hukuka uygun biçimde, tespit edilen özel iletişim kanallarından uygun olanların kullanılması suretiyle bir kez daha uyarılmalıdır. Bu uyarı

sürecinde kullanılacak metinler de Dezenformasyonla Mücadele Merkezi'nin onayından geçmiş olmalıdır.

İşleyiş sürecinin esası salt cezalandırmak olmadığı için, uyarılar ve bilgilendirmeler sonrasında dezenformatif içerik üzerinde beklenenleri yapanlara yine özel iletişim kanallarından "doğrunun anlaşılması için gösterdikleri erdemli davranıştan dolayı" teşekkür edilmelidir. Bunun yanında dezenformasyona dair beklenen düzeltmeleri yasal sürece başvurmadan gerçekleştirenleri küçük düşürmeden istihbarat birimlerine ait sanal ortam hesaplarından herkese açık şekilde bilgilendirme metni yayımlanmalıdır. Bu metin de Dezenformasyonla Mücadele Merkezi'nin onayını almış olmalıdır.

Yapıcı nitelikteki tüm çalışmalara rağmen dezenformatif içerik nedeniyle kendisinden beklenenleri yapmayanlar Cumhuriyet Savcılıklarına bildirilmeli ve savcılıkların talimatları doğrultusunda ilgili birimler tarafından suç soruşturmasına başlanmalıdır.

Beşinci Aşama: Kamuoyunu Bilgilendirme

Dezenformasyon nedeniyle geçirilen süreç bu aşamada şeffaf biçimde kamuoyuna duyurulmalıdır. Ancak bu aşamadaki duyurular bizzat Dezenformasyonla Mücadele Merkezi tarafından yapılmalıdır. Kamuoyunu bilgilendirmek amacıyla kullanılacak paylaşımlarda dezenformasyonların hedefindeki kişi, kurum ve kuruluşların yapıcı açıklamalarına, istihbarat birimlerinin yapıcı uyarılarına vurgu yapılmalı, süreç içerisinde gerçekleşen düzeltme faaliyetleri nedeniyle ilgili öznelere teşekkür edildiği açıklanmalıdır. Hukukî süreçler devam ederken ortaya çıkan olumlu gelişmelere de bu minvaldeki açıklamalarda teşekkür etmek suretiyle yer verilmelidir. Hukukî süreçlerin sonunda ceza alanlar ise sadece paylaştıkları içerikleri ilân etmek suretiyle bu aşamada kamuoyuna duyurulmalıdır.

Altıncı Aşama: Ölçme-Değerlendirme ve Geri-Bildirim

Bu aşamada hem dezenformasyona karşı mücadelede elde edilen başarı hem de kamuoyunun bu mücadele nedeniyle kamu yönetimine ve hükûmete dair algısı ölçülmelidir. Bunların ölçülmemesi hem mücadelenin başarılı biçimde gerçekleştirilip gerçekleştirilemediğini anlamayı zorlaştırır hem de kamusal itibarın korunması konusunda vatandaşların ve diğerlerinin algılarının nasıl şekillendiğini tespit etmeyi güçleştirir.

Dezenformasyona karşı mücadelede sağlanan başarı için somut verilere bakılabilir. Dezenformatif içeriğini düzelten, hatasını kabul eden, çeşitli gerekçelerle özrünü ileten vaka sayısı bu konuda somut veriler olarak kabul edilebilir. Kamuoyunun bu mücadele nedeniyle kamu yönetimine ve hükûmete dair algısını ölçebilmek için ise bu işleyiş sürecinin ilk beş aşamasında gerçekleştirilen iş ve işlemlere sanal ortamlarda gösterdikleri tepkilere bakılabilir. Hatta bu hususta saha araştırmaları da yapılabilir. Elde edilen veriler bu işleyiş süreci ile kamu yönetimine ve hükûmete dair algıların iyileştirilmesi amacıyla kullanılmalıdır. Çünkü gerek kamu yönetiminin gerekse hükûmetlerin vatandaşlar ve diğerleri nazarındaki meşruiyeti bunu da gerektirir.

SONUÇ:

Dezenformasyonun gerçekleşmesini önlemek de gerçekleştikten sonra verdiği zararı telafi etmek de zorluklarla doludur. Dezenformasyona karşı gerçekleştirilen mücadelenin mutlak doğrular içerdiğini iddia edebilmek de zordur. Bu halde bu mücadelenin geliştirilmesine katkı sağlayabilecek çalışmalara ihtiyaç vardır. Bu çalışma bu değerlendirmenin ürünüdür. Bu çalışmada kamusal itibara zarar verme olasılığı nedeniyle dezenformasyona karşı gerçekleştirilecek mücadelede kullanılabilecek bir işleyiş süreci önerilmiştir. Önerilen işleyiş süreci Machiavelli'in tavsiyesinde yer alan sevgi ve korkunun bir hükümdarın bünyesinde aynı anda bulunması ile bir hükûmetin bünyesinde aynı anda bulunması arasında fark olmadığı düşüncesi üzerine kuruludur. Hatta bir hükümdarın yapmakta zorlanabileceği böyle bir şeyin bir hükûmet tarafından kolaylıkla yapılabilecek olması dezenformasyona karşı mücadelenin başarısı açısından iyi bir fırsat olarak görülmektedir. Çalışmanın önerdiği işleyiş süreci bir yandan dezenformasyon suçu için Türk Ceza Kanunu'nun 217/A maddesiyle yapılmış olan düzenlemeye dikkatleri çekerek dezenformasyon yapan öznelerin cezalandırılacakları düşüncesinin oluşturulmasına, diğer yandan aynı anda devletin yapıcı, bağışlayıcı, inşa edici yanını öne çıkarmaya gayret ederek kamu barışının sağlanmasına katkı sunabilecektir.

Önerilen işleyiş sürecinin merkezine istihbarat birimlerinin yerleştirilmesinin gerekçesi, Machiavelli'in tavsiye ettiği "korku salma" amacının bu birimlerin varlığıyla ve "cezasızlık algısını" yıkmaya yönelik çalışmalarıyla başarılabilecek olmasıdır. Machiavelli'in diğer tavsiyesi olan "sevgi oluşturma" amacının başarılmasının da gerekli olduğu düşüncesiyle, dezenformasyonların hedefinde olan kişi, kurum ve kuruluşlara modelde yapıcı nitelikte çeşitli roller verilmiştir. Bu sayede bir yandan cezasızlık algısını yıkmak suretiyle korku salma amacı başarılırken, diğer yandan kamu yönetimine ve hükûmetlere karşı kin ve nefretin gelişmesini engellemenin mümkün olabileceği değerlendirilmiştir. Dezenformasyona karşı mücadele sürecinde ihtiyaç duyulabilecek hassas bir denge bu sayede oluşturulabilecektir. Nitekim kamusal itibar, sadece kazanılması gereken değil, kazanıldıktan sonra güvenliği de hassas bir dengede sağlanması gereken bir varlıktır.

Çalışmayla önerilen işleyiş süreci dezenformasyona karşı mücadele edilmesini ve kamusal itibarın güvenliğinin sağlanmasını başarırken bazı ek kazanımlar da getirebilir. Bunlardan biri oto-kontroldür. Bu süreç, kamusal hizmetlerin sunumunda kamu sektörü tarafında görevli olan tüm kişi, kurum ve kuruluşları dezenformasyona karşı ve dezenformasyonla mücadele konusunda oto-kontrole sevk edebilir. Çünkü süreç; kişi, kurum ve kuruluşların kamusal itibarın güvenliğinin sağlanması konusundaki farkındalıklarını ve hükûmetin bu konudaki hassasiyetine dair bilinçlerini daha fazla geliştirebilir. Bununla birlikte kurum ve kuruluşlarda hizmet sabotajlarının ve bürokratik casusluklarının önüne geçilmesini kolaylaştırabilir. Diğer taraftan bu işleyiş süreci, kamu güvenliğinden sorumlu birimlerin görevlerinin kamunun sadece can ve mal-mülk güvenliğini sağlamaktan ibaret olmadığı konusunda bilinç geliştirmelerine ve yeni fırsatlar aramalarına katkı sunabilir. Bu bakımdan süreçte yer alan tüm aktörlere gerek dinamizm kazandırabilmesinin gerekse korku salabilmesinin mümkün olduğu ifade edilebilir.

Bu işleyiş sürecinin ek kazanımlarından biri de bilişim suçları konusunda bilimsel bilgi üretilmesine katkı sağlayabilecek olmasıdır. Başka bir ifadeyle bu süreç, bilişim hukuku temelinde bilimsel bilginin gelişmesine ve bilişim suçlarıyla mücadele etmeyi kolaylaştıracak tecrübeler kazanılmasına katkı sağlayabilir. Bu sayede mevzuat da geliştirilebilir.

İşleyiş süreci, sağlayabileceği ek kazanımlar yanında, bir takım riskler de getirebilir. Sürecin yönetiminde liyakatsiz kişilerin bulunması, sürecin yönetiminde bulunan kişilerin kamu yönetiminin ve hükûmetlerin bu konudaki hedeflerini benimsememesi, sürece içeriden ve dışarıdan sabotajlar planlanması ve gerçekleştirilmesi, sürecin insan haklarına ve hukuka aykırılıklar taşıdığı gerekçesiyle

haksız ve mesnetsiz eleştirilere maruz kalması/bırakılması vb. gibi riskler ortaya çıkabilir. Diğer yandan iktidar değişimleri de dezenformasyona karşı mücadelenin bu süreçte öngörülen biçimde sürdürülememesine etki edebilir.

Kamusal itibarın güvenliğini sağlamak için dezenformasyona karşı gerçekleştirilecek mücadele kapsamında kullanılabilecek olan bu işleyiş süreci demokrasi kültürünün gelişmesine, ifade özgürlüğünün sınırları bulunduğu konusundaki anlayışın yerleşmesine, hükûmetlerin toplumsal barışın sağlanabilmesi için gayret içerisinde olduğunun gösterilmesine/görülmesine ve hükûmetler tarafından devletin bekası için gerçekleştirilen çalışmaların takdir edilmesine katkılar sağlayabilir. Çünkü dezenformasyona karşı etkili mücadele, devletlerin ve toplumlarının gelişmesi ve ilerlemesi konusunda potansiyel fırsatlar barındırmaktadır.

Etik Standart ile Uyumluluk

Çıkar Çatışması: *[TR] Yazar / yazarlar, kendileri ve / veya diğer üçüncü kişi ve kurumlarla çıkar çatışmasının olmadığını veya varsa bu çıkar çatışmasının nasıl oluştuğuna ve çözüleceğine ilişkin beyanlar ile yazar katkısı beyan formları makale süreç dosyalarına ıslak imzalı olarak eklenmiştir.*

[EN] The author(s) declare that they do not have a conflict of interest with themselves and/or other third parties and institutions, or if so, how this conflict of interest arose and will be resolved, and author contribution declaration forms are added to the article process files with wet signatures.

Etik Kurul İzni: Bu çalışma için etik kurul iznine gerek yoktur. Buna ilişkin ıslak imzalı onam formu, makale süreç dosyasına eklenmiştir.

KAYNAKÇA:

Argüden, Y. (2003). *İtibar Yönetimi*. ARGE Danışmanlık Yayınları.

Bahar, A. (2020). Polislik Perspektifinden Dijital Misenformasyon ve Dezenformasyon: Covid-19 Örnek Olayı Bağlamında Bir Analiz. *OPUS–Uluslararası Toplum Araştırmaları Dergisi*, 16(30), 2760-2794. https://doi.org/10.26466/opus.783266.

Balcı, M. & Çakır, K. (2023). Halkı Yanıltıcı Bilgiyi Alenen Yayma Suçu (TCK m. 217/A). *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*, 9(1), 1-17.

Bontridder, N. & Poullet, Y. (2021). The Role of Artificial Intelligence in Disinformation. *Data & Policy*, 3, e32. https://doi.org/10.1017/dap.2021.20.

Bustos, E. O. (2021). Organizational Reputation in the Public Administration: A Systematic Literature Review. *Public Administration Review*, 81(4), 731–751.

Carpenter, D. P. & Krause, G. A. (2012). Reputation and Public Administration. *Public Administration Review*, 72(1), 26–32.

Carpenter, D. P. (2010). *Reputation and Power: Organizational Image and Pharmaceutical Regulation at the FDA.* Princeton University Press.

Carpenter, D. P. (2002). Groups, the Media, Agency Waiting Costs, and FDA Drug Approval. *American Journal of Political Science*, 46(2), 490-505.

Cavelty M. D. & Wenger, A. (2019). Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science. *Contemporary Security Policy*, 41(1), 5-32. https://doi.org/10.1080/13523260.2019.1678855.

Ciarlone, T. G. & Wiechmann, E. W. (2003). Cybersmear may be Coming to A Website Near You: A Primer for Corporate Victims. *Defense Counsel Journal*, 70(1), 51-64.

Diermeier, D. (2012). Managing Public Reputation. B. J. Calder (Edt.) *Kellogg on Advertising and Media* (p. 304-330). John Wiley & Sons, Inc.

Dursun, D. (2012). Bürokrasi Teorisi ve Yönetim. *Journal of Social Policy Conferences*, 37-38, 133-149.

Er, G. (2008). *Sanal Ortamda İtibar Yönetimi: Kurumsal İtibar Yönetimi ve İnternette İtibarı İzlemenin, Korumanın ve Güçlendirmenin Yolları*. Cinius Yayınları.

Fetzer, J. H. (2004). Information: Does it have to be True? *Minds and Machines*, 14, 223–229.

Fombrun, C. J. & Riel, C. V. (1997). The Reputational Landscape. *Corporate Reputation Review*, 1, 5–13.

Gül Ünlü, D. & Küçükşabanoğlu, Z. (2023). Dezenformasyon ve Yapay Zekâ: Dezenformasyonla Mücadele Yollarına Yapay Zekâ Uzmanlarının Gözünden Bakmak. *İletişim ve Diplomasi*, 11, 83-106.

Harris, L. C. & Ogbonna, E. (2002). Exploring Service Sabotage: The Antecedents, Types and Consequences of Frontline, Deviant, Antiservice Behaviors. *Journal of Service Research*, 4(3), 163-183.

Harris, L. C. & Ogbonna, E. (2009). Service Sabotage: The Dark Side of Service Dynamics. *Business Horizans*, 52(4), 325-335.

Hunt, J. S. (2021). Countering Cyber-enabled Disinformation: Implications for National Security. *Australian Journal of Defence and Strategic Studies*, 3(1), 83–88. https://doi.org/10.51174/AJDSS.0301/MLTD3707.

James, A. (2013). *Examining Intelligence-led Policing: Developments in Research, Policy and Practice*. Palgrave Macmillan.

Kelling, G. L. & Bratton, W. J. (2006). Policing Terrorism. *Civic Bulletin*, 43, 1-8.

Kırdemir, B. (2024, Mayıs 9). *Türkiye'nin Dezenformasyon Ekosistemi: Genel Bakış.* Edam Ekonomi ve Dış Politika Araştırmalar Merkezi. https://edam.org.tr/wp-content/uploads/2020/07/Türkiyenin-Dezenformasyon-Ekosistemi-Genel-Bakış-Barış-Kırdemir.pdf.

King, B. G. & Whetten, D. A. (2008). Rethinking the Relationship Between Reputation and Legitimacy: A Social Actor Conceptualization. *Corporate Reputation Review*, 11(3), 192–207.

Machiavelli, N. (2019). *Hükümdar*. N. Adabağ (Çev.). Türkiye İş Bankası Kültür Yayınları.

MİT. (2024, Mayıs 4). *Casusluk Nedir?* Millî İstihbarat Teşkilatı. https://www.mit.gov.tr/medya.html.

Montoro-Montarroso, A., Cantón-Correa, J., Rosso, P., Chulvi, B., Panizo-Lledot, Á., Huertas-Tato, J., Calvo-Figueras, B., Rementeria, M. J. & Gómez-Romero, J. (2023). Fighting Disinformation

with Artifical Intelligence: Fundamentals, Advances and Challenges. *Profesional de la Informacion*, 32(3), e320322. https://doi.org/10.3145/epi.2023.may.22.

OSCE. (2022, September 10). *OSCE Guidebook Intelligence-led Policing*. TNTD/SPMU Publication Series, Vol. 13. Vienna. Organization for Security and Co-operation in Europe. https://www.osce.org/files/f/documents/d/3/327476.pdf.

Rao, H. (1994). The Social Construction of Reputation. *Strategic Management Journal*, 15, 29-44.

Ratchliffe, J. H. (2008). *Intelligence-led Policing*. Willan Publishing.

Whyte, C. (2020). Deepfake News: AI-enabled Disinformation as A Multi-level Public Policy Challenge. *Journal of Cyber Policy.* https://doi.org/10.1080/23738871.2020.1797135.

Yanatma, S. (2018). *Reuters Institute Digital News Report 2018 – Turkey Supplementary Report*. Reuters Institute and University of Oxford. https://doi.org/10.60625/risj-d65n-1n75.

Zavattaro, S. & Eshuis, J. (2021). Public Administration in the Reputation Era: A Conceptual Exploration. *Public Administration Quarterly*, 45(4), 418-438. https://doi.org/10.37808/paq.45.4.4.

EXTENDED SUMMARY:

Reputation is an asset, just like life and property. Moreover, reputation is a very clear indicator of legitimacy. Therefore, reputation needs to be managed and protected. Within the framework of reputation management, both gaining reputation and ensuring the security of the reputation gained are essential for individuals, institutions and organizations that provide public services in the public sector. In the study, the reputation of these actors providing public services is conceptualized as “public reputation”.

One of the goals of disinformation is to damage public reputation. Therefore, online disinformation targeting public reputation is an important issue of public administration. Because many fundamental rights and freedoms, especially freedom of expression, may be damaged by this type of disinformation. The basic principles of democracy can also be eroded due to this type. Such negative consequences arising from disinformation may affect the legitimacy of both public administration and governments in the eyes of citizens. Service sabotages and bureaucratic espionages can be used for these purposes in institutions and organizations that provide public services. Therefore, developing measures to combat disinformation is among the important responsibilities of public administrations and governments. In the study, this issue is conceptualized as “security of public reputation”. It has been suggested that an operating process in which law enforcement units that will carry out intelligence work against the subjects of disinformation are at the center is used to ensure the security of public reputation. The operating process does not deny the libertarian approach but adopts the security approach. Because disinformation can lead to crises. An advice given by Machiavelli to the ruler in his work “The Prince” inspired the operating process. In his work, Machiavelli advises the ruler to “prefer to spread fear if he cannot manage to create both fear and love at the same time.” It has been evaluated that this advice can also be used by governments. It is thought that the operating process can contribute to the fight against the crime of disinformation regulated in Article 217/A of the Turkish Criminal Law. Because the proposed operating process also has a subject-oriented approach.

This process can be achieved by ensuring that the duties to be performed by law enforcement are “based” on identifying the subjects of disinformation through intelligence work. In other words, intelligence activities to be carried out by law enforcement in order to identify the subjects of disinformation that will harm public reputation are a requirement for the functionality of the operating process. In this respect, the operating process’s understanding of intelligence is specific to the study and differs from the “intelligence-led policing” strategy developed in accordance with the proactive security management approach. It is considered that combating

some crimes may be difficult to achieve with proactive approaches, for example, intelligence-led policing cannot be used in all cases where “prevention without happening” is the goal. Disinformation crime is a crime of this type. It is considered that disinformation cannot be detected before it occurs, in other words, it is not possible to detect misinformative content before it circulates in online environments. For this reason, the operating process proposed in the study requires an “intelligence-based policing” strategy, not “intelligence-led policing”. It is envisaged that with the use of intelligence-based policing strategy, disinformation can be combated on a reactive basis, while proactive combat can also be achieved through fear.

When the posts on the social media platform “X” are examined, it is seen that the Center for Combating Disinformation (CCD) within the Directorate of Communications of the Presidency of the State of the Republic of Türkiye cannot carry out effective work on combating disinformation to ensure the security of public reputation. The reactions given by X users to this unit’s posts reveal the need for more effective practices in combating disinformation. The operating process suggested in the study can achieve this by highlighting the intelligence units within the law enforcement and instilling fear in the subjects of disinformation. However, it is also necessary that the love for governments should not be destroyed. For this reason, other institutions and organizations are also included in the operating process.

The ultimate goal of the study, which is a theoretical review, is to contribute to the efforts of the State of the Republic of Türkiye to ensure the security of public reputation. The study proposes a six-stage operating process to combat disinformation that can harm public reputation. Although the operating process has some risks, the advantages it can provide are greater. It is considered that it can be used to combat disinformation in an environment where there is no consensus on how to combat disinformation. Because effective combat against disinformation contains potential opportunities for development and progress. Failure to combat disinformation is a significant obstacle to development and progress.