T.C.
BURSA ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
TEZLİ YÜKSEK LİSANS PROGRAMI

Filistin ve Ürdün Anayasaları Çerçevesinde Dijital Mahremiyet Hakkı: Niteliği, Kapsamı ve Mevcut Anayasal Güvenceler

YÜKSEK LİSANS TEZİ

MAHMOUD W M ABUNADA

BURSA 2022

T.C.
BURSA ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
TEZLİ YÜKSEK LİSANS PROGRAMI

Filistin ve Ürdün Anayasaları Çerçevesinde Dijital Mahremiyet Hakkı: Niteliği, Kapsamı ve Mevcut Anayasal Güvenceler

YÜKSEK LİSANS TEZİ

MAHMOUD W M ABUNADA

Danışman:
Asst. Prof. Dr. Zeynep Burcu AKBABA

BURSA 2022

ÖZET

Yazar Adı ve Soyadı: MAHMOUD W M ABUNADA
Üniversite: Bursa Uludağ Üniversitesi
Enstitüsü: Sosyal Bilimler Enstitüsü
Anabilim/Anasanat Dalı: Kamu Hukuku
Bilim/Sanat Dalı: Anayasa Hukuku Anabilim Dalı
Tezin Niteliği: Yüksek Lisans Tezi
Sayfa Sayısı: 151
Mezuniyet Tarihi: ……/……./20....
Tez Danışmanı: Asst. Prof. Dr. Zeynep Burcu AKBABA

Filistin ve Ürdün Anayasaları Çerçevesinde Dijital Mahremiyet Hakkı: Niteliği, Kapsamı ve Mevcut Anayasal Güvenceler

Bu tez, dijital mahremiyet hakkının Ürdün ve Filistin'deki anayasal düzenlemesini ele almakta ve özellikle dijital mahremiyet hakkının gelişimi, yasal kapsamı, Ürdün ve Filistin anayasalarındaki ele alınışı ve iki ülke mevzuatının bu hakka tanınan anayasal güvencelere uygunluğu gibi çeşitli konuları incelemektedir. Ayrıca tezin önemi, dijital mahremiyet hakkı anlayışının yeni olmasından ve anayasa ile diğer mevzuat kapsamında bu hakkın konusunu düzenleyen açık ve net yasal metinlerin bulunmamasından kaynaklanmaktadır.

Bu durum, doğalarındaki benzerlikten dolayı özel hayat gizliliği hakkının genel kurallarını dijital mahremiyet hakkı için uyarlama ve örnek alma gerekliliğini doğurmaktadır. Zira günümüz dünyasında dijital mahremiyet hakkı, giderek daha önemli bir hale gelmektedir. Bu tezin ilk bölümü, dijital mahremiyet hakkı anlayışının gelişim tarihini sunarken, ikinci bölüm, bu hakkın Ürdün ve Filistin anayasal ve yasal anlamda ele alınmasını ve bunların karşılaştırılmasını incelemiştir. Üçüncü bölüm ise, Ürdün ve Filistin'de dijital mahremiyet hakkına tanınan anayasal güvenceleri analiz etmiş ve bu hakla ilgili yasaların Ürdün ve Filistin anayasalarının ilkeleriyle ne kadar uyumlu olduğu ele almıştır.

Anahtar Sözcükler:

Dijital Mahremiyet, Yasal Kapsam, Anayasal Güvenceler, Özel Hayat Hakkı, Filistin Anayasası ve Ürdün Anayasası.

ABSTRACT

Name and Surname: MAHMOUD W M ABUNADA

University: Bursa Uludag University

Institution: Social Science Institution

Field: Public Law

Branch: The Constitutional law

Degree Awarded: Master

Page Number: 151

Degree Date: …../……/20….

Supervisor: Asst. Prof. Dr. Zeynep Burcu AKBABA

The Right to Digital Privacy: Essence, Scope, and Constitutional Guarantees: A comparative study between the Palestinian and Jordanian constitutions

This thesis addresses the constitutional regulation of digital privacy rights in Jordan and Palestine. In particular, the thesis discusses the evolution of digital privacy rights and their legal scope, while also examining their status in the Jordanian and Palestinian constitutions and whether the jurisdictions in these two countries offer constitutional guarantees in regard to privacy rights.

In addition to an increased interest in digital privacy rights in today's world, the study is also important because it sheds light on a fairly recent phenomenon. Additionally, no explicit and direct juridical or constitutional articles exist to regulate the issue. Therefore, this paper reviews and analyzes the general constitutional rules governing the right to private life, while tailoring them to digital privacy rights given the similarities they both share.

Chapter 1 provides a historical overview of the evolution of the concept of digital privacy rights, while chapter 2 reviews and compares the Palestinian and Jordanian constitutional rules governing digital privacy rights. Chapter 3 discusses the constitutional protections of digital privacy rights in Palestine and Jordan, while

examining the extent to which the laws relevant to digital privacy rights conform to Palestinian and Jordanian constitutional rules.

Key Words:

Digital Privacy, Legal Scope, Constitutional Guarantees, The Right To A Private Life, Palestinian Constitution, Jordanian Constitution.

İÇİNDEKİLER

Sayfa

ÜÇÜNCÜ BÖLÜM

Dijital Mahremiyet Hakkının Kapsamı ve Bu Alandaki Filistin ile Ürdün Yasal Mevzuatının Anayasal İlkelere Uyumu

Giriş

Dijital teknolojinin muazzam gelişimi ve bireylerin internete hızlı erişimi sayesinde gereken işlemleri tamamlama, hizmet alma ile sunma, bireylerle iletişim kurma ve fikirleri ifade etmek için yeni alanlar yaratma gibi konularda devasa ve hızlı bir gelişim sağlanmıştır. Ancak bu gelişim, bireylerin izlenmesi, takip edilmesi ve özel hayatlarının açığa çıkması gibi tehlikelere yol açarak mahremiyet hakkının ihlal edilme olasılığını artırmıştır. Zira yetkililer, devlet kurumları ve internet servis sağlayıcıları dahil olmak üzere çeşitli taraflar, yazışma ve internet bağlantı verileri gibi kullanıcı verilerine erişebilme ve bireylerin özel hayatlarını izleyebilme gücü bulunmaktadır.

Dolayısıyla bütün bu gelişmeler ve tehlikeler ışığında, bireylerin itibar, onur ve haysiyetini koruma hakkı gibi değerlerle ilgili bazı ahlaki boyutlarla ve genellikle konut dokunulmazlığı gibi maddi boyutlarla sınırlı olan klasik mahremiyet anlayışını yeniden ele alınması gerekmektedir. Bu nedenle bireylerin hakları, özgürlükleri ve kişisel verilerine yönelik saldırıların tüm yönlerini kapsayan yeni bir mahremiyet anlayışının ortaya çıkmasını gerekmiştir. Söz konusu yeni anlayış, unsurları ve özellikleri bakımından klasik versiyonuyla mahremiyet hakkından farklı olup teknolojilerin gelişmesi ve İnternet'in yaygınlaşması ile bağlantılı bir anlayış olarak dijital mahremiyet adıyla ortaya çıkmıştır.

Bu bağlamda hem Ürdün hem de Filistin anayasalarında yeni anlayışı ve doğası ile dijital mahremiyet hakkını düzenleyen açık bir anayasal metnin bulunmamasının yanı sıra dijital dünyayı düzenleyen yasal mevzuatta hızlı dijital gelişmelere benzer bir gelişme yaşanmamıştır. Bu nedenle söz konusu iki ülkenin yasal düzenlemelerinde bu hakkı ele alan eski ve farklı yasalarda dağınık bazı maddeler bulunmaktadır. Bu yasaların önde geleni ise, bazı maddelerinde dijital mahremiyet hakkına açık ihlaller içeren Filistin ve Ürdün'deki Siber Suçlar Yasasıdır. Kapsamlı ve düzenleyici bir anayasal ve yasal çerçevenin olmamasına rağmen mahremiyeti etkileyen dijital gelişmeler artmaya devam etmekte ve aslında tezin önemi burada yatmaktadır.

Zira dijital mahremiyet hakkına ilişkin açık yasal metinlerin yokluğu nedeniyle tez, özel hayat gizliliği hakkına ilişkin genel kuralları ve dijital mahremiyet hakkını zımnen ele alan yasal metinleri analiz ederek dijital mahremiyet hakkının anlayışını, bunun yasal kapsamını ve onun için zımnen tanınmış anayasal güvenceleri incelemeye çalışmaktadır. Bu anlamda tez, özellikle dijital dünyada bireylerin temel haklarını koruyabilecek herhangi bir açık anayasal güvence olmadığından dolayı verilere eksik bir koruma sağlayan dijital işlemleri düzenleyen yeni yasalar ışığında dijital mahremiyet hakkının incelenmesinin önemine dayanmaktadır. Filistin ve Ürdün özelinde anayasal ilkelere aykırı olan bu yasaların en belirgin tezahürü, 2018 tarihli Ürdün Siber Suçlar Yasası ve Filistin Devlet Başkanı tarafından çıkarılan 2017 tarihli 16 Sayılı Siber Suçlar Yasasıdır.

Ürdün ve Filistin'de dijital mahremiyet hakkını düzenleyen açık yasal metinlerin yokluğu nedeniyle, bu tez şu temel soruları yanıtlamaya çalışıyor: Ürdün ve Filistin anayasalarında dijital mahremiyet hakkı için ne kadar anayasal güvenceler sağlanmıştır? Özel hayat gizliliği hakkını düzenleyen anayasal ilkelere dayanarak bunları dijital mahremiyet hakkı için kullanmak mümkün müdür? Bu ilkeler dijital mahremiyet hakkının doğasına ne kadar uygundur? Aynı zamanda bu temel sorulardan birkaç alt soru ortaya çıkmıştır:

1. Mahremiyet hakkı kavramının tarihsel gelişim süreci nedir?
2. Dijital mahremiyet hakkı ne demektir? Bu hakkın anayasal değeri nedir? Bu hakkın özel hayat gizliliği hakkı ile ilişkisi nedir?
3. Filistin ve Ürdün anayasalarında dijital mahremiyet hakkı nasıl ele alınmıştır?
4. Filistin ve Ürdün anayasalarında dijital mahremiyet hakkının yasal kapsamı nedir?
5. Filistin ve Ürdün anayasalarında dijital mahremiyet hakkının ve ona bağlı diğer hakların anayasal güvenceleri nelerdir?
6. Dijital mahremiyet hakkına ilişkin Filistin ve Ürdün yasaları anayasal metinlerle uyumlu mu yoksa onlara aykırı mıdır?
7. 2018 tarihli Ürdün Siber Suçlar Yasası ve Filistin Devlet Başkanı tarafından çıkarılan 2017 tarihli 16 Sayılı Siber Suçlar Yasası örneklerinde dijital mahremiyet hakkına ilişkin güvenceler ve ihlaller nelerdir?

Yöntemi ve araştırma araçları ile bu tez, anlayış, yasal kapsam ve ilgili yasal mevzuatla uyumluluk açısından Ürdün ve Filistin anayasaları için dijital mahremiyet hakkına ilişkin teorik bir çerçeve geliştirmeyi hedeflemektedir. Bu anlamda tez, dijital mahremiyet hakkına ilişkin açık anayasal düzenlemelerin yokluğunu gidermeyi teşvik etmek adına söz konusu hakkın kökenlerini ve unsurlarını analiz etmeye dayalı öneriler sunarak gelecekte bu alanla ilgili çeşitli yasal düzenlemelerin hazırlanmasında Ürdünlü ve Filistinli yasa koyuculara katkıda bulunmayı amaçlamıştır. Aynı zamanda tez, araştırmacılar, avukatlar ve yargıçlar dahil olmak üzere hukuk alanındaki uzmanlara bilimsel bir yasal materyal hazırlayarak tez konusuyla ilgili uygun bir yasal anlayışa varmalarına yardımcı olmaktadır.

Tez, betimsel ve karşılaştırmalı analitik yöntemlerini benimseyecektir. Aynı zamanda tez, mahremiyet hakkı kavramının ortaya çıkışını ve dijital mahremiyet hakkı anlayışına ulaşana kadar yıllar içindeki gelişimini anlamak ve analiz etmek amacıyla, bir yandan önceki yasal literatüre, diğer yandan konuyla ilgili çeşitli anayasal deneyimlere dayanacaktır. Ayrıca tez, nitelik ve yasal kapsam bakımından özel hayat gizliliği hakkı ile dijital mahremiyet hakkı arasındaki benzerlikleri ve farklılıkları göstermek adına betimsel ve analitik yöntemleri kullanacaktır. Ayrıca tez, ele alınan yasaların tanım, yasal kapsam ve anayasal ele alınış açısından dijital mahremiyet hakkıyla ilgili mevcut durumunu açıklamak ve karşılaştırmak amacıyla karşılaştırmalı analitik yöntemini tercih edecektir.

Bu yöntemi üç aşama şeklinde kullanan tez, ilk olarak Filistin ve Ürdün Siber Suçlar Yasaları gibi mahremiyet konusuyla ilgili söz konusu iki ülkenin mevzuatındaki yasal metinleri inceleyecek ve analiz edecektir. İkinci aşama, bu yasal metinlerin Ürdün Anayasası ve 2003 yılında değiştirilen Filistin Temel Yasası'nın maddelerinde yer alan anayasal ilkelerle ne kadar uyumlu veya aykırı olduğunu tespit edecektir. Üçüncü aşamada ise tez, dijital mahremiyet hakkının Ürdün ve Filistin'de anayasal ve yasal anlamda ele alınışını karşılaştıracaktır. Zira bu iki hukuk sistemi, mahremiyet hakkının anayasal güvencelerinin sağlanması, bu hakkın tanımlanması, yasal kapsamını

belirlenmesi ve yasal mevzuatların anayasal ilkelerle ne kadar uyumlu olması gibi konularda farklılık göstermiştir.

Ayrıca bu çalışmada araştırmacı, Ürdün ve Filistin örneklerini iki nedenden dolayı seçmiştir. Bunların birincisi, iki ülkenin yakın bir zamana kadar aynı siyasi otoriteye tabi olması ve dolayısıyla topraklarında aynı yasaların uygulanmasıdır. Ancak bu durum, İsrail'in 1967 yılında Batı Şeria'yı işgal etmesi ve ardından Filistin Yönetimi'nin 1994 yılında kurulması nedeniyle değişmiştir. Bunun sonucunda iki ülke arasında siyasi, yasal ve anayasal açılardan dikkate değer farklılıklar ortaya çıkmıştır. Yasal anlamdaki farklılıkların en önde gelenlerinden bir tanesi de dijital mahremiyet hakkının iki ülkedeki ele alınışı ile ilgilidir. Bu iki ülkeyi seçmenin ikinci nedeni ise, bunların vatandaşlarından dikkate değer bir sayının diğer ülkenin vatandaşlığına sahip olmasıdır. Bunun sonucunda bu çifte vatandaşlar, iki ülkenin kimileri benzer kimileri farklı yasalarına tabi olmuştur. Aynı zamanda araştırmacı, iki ülkenin dijital mahremiyet hakkını ele almakta ve bu konuda bireyler için gerçek koruma sağlayan güncel yasalar çıkarmakta ne kadar geç kaldıklarının farkındadır. Bu nedenle, ikinci ve üçüncü bölümlerin sonlarında, dijital mahremiyet konusunda genel olarak iki ülkenin yasaları ile bu konudaki Avrupa Birliği yasaları arasında kısa bir karşılaştırma sunmaya çalışacağız.

Birinci Bölüm: Dijital Mahremiyet Hakkı

Üçüncü binyılın başlamasıyla birlikte derinleşen teknolojik devrimin etkileri ve bilimsel gelişimin boyutları çerçevesinde yeni medya, geniş bir alana yayılmış aynı zamanda da insan hayatında önemli bir yer edinmiştir. Bahsi geçen zaman dilimi içerisinde gelişen internete bağlı kişi ve cihazların sayısındaki artışı hızlı ve büyük çaplı olmuştur. Bu büyük çaplı artış sayesinde internet; çevrimiçi alışveriş, bankacılık hizmetleri, çevrimiçi formları doldurmak, sosyal medyada paylaşım yapmak gibi durumların yanı sıra dijital ortamda hassas veri ve belgeleri depolamak gibi çeşitli günlük rutinlerine bağlı görevleri yerine getirmek için kullanılan hayatın vazgeçilmez bir aracı haline gelmiştir. Bu bağlamda dijital mahremiyet kavramı, özellikle dijital veri ve hesapları hackleme, çalma eylemlerinin yol açtığı sayısız özel bilgi ihlalleri gölgesinde büyük bir önem kazanmıştır. Zira dijital ortamdaki mahremiyete yönelik yapılan tehditler, birçok bireyin özellikle kimlik hırsızlığı tehlikesi sebebiyle endişelenmesine neden olmuştur.

Ancak dijital ortamı basit şekilde kullananların bilgilerinin korunması olarak tanımlanan dijital mahremiyet kavramı, daha karmaşık bir olgudur. Bu anlamda özel hayat ve dijital çağda mahremiyet haklarının önemi gittikçe artmıştır. Dijital ortamdaki hak ve özgürlüklerin korunması konusunu ciddi bir şekilde etkileyen mahremiyet ihlalleri olgusu, modern suç yöntemlerinin yayılmasına zemin hazırlamıştır. Bu nedenle son dönemlerde artan siber güvenlik ihlalleri, dijital mahremiyet tehditleri ışığında daha güvenli bir internet kullanımı ve dijital ortam yaratma hedefi; toplumları ve bireyleri korumak amacıyla dünyada hukuk sistemlerinin bir önceliği haline gelmiştir. Böylece yaşadığımız modern dünyada veri mahremiyeti ve veri güvenliği, her zaman için tüm kurum ve kuruluşların önemsediği en temel güvenlik standartları arasında hak edilen bir yere sahip olmuştur.

Bilgi ve iletişim teknolojileri hızlı bir şekilde gelişmeye devam ederken bu teknolojilerin artan kullanımıyla birlikte özellikle bireylerin bu gelişme aşamalarını izleme ve aşamaları belirli sıra ile takip etme durumları dolayısıyla elde edilmiş olan mahremiyet hakkının ihlal edilme olasılığını ve sıklığını arttırmıştır. Bu bağlamda dijital mahremiyet; kullanıcı

anonimliğinin ihlali, kişisel verilerin yetkisiz bir şekilde ifşası, kişisel verilerin yetkisi verilmeyen amaçlarla kötüye kullanımı ve kişiliği karalama gibi tehlikelerle karşı karşıya kalmaktadır. Bu bölüm, mahremiyet hakkının internet ve dijital ortamla ilişkisini ve bu ilişkinin kişisel mahremiyet anlayışını nasıl değiştirdiğini bunların yanı sıra günümüzde uygulanan yasal düzenlemelerin çevrimiçi iletişim ve sosyal medya ortamında ne kadar yetersiz olduğu durumunu açıklamayı hedeflemiştir. Aynı zamanda bu bölüm, bu şartlar çerçevesinde dijital çağda kişisel mahremiyete sağlanan korumanın niteliği ve kapsamı yeniden gözden geçirilmesi gerektiğini savunmaktadır.

Ayrıca bu bölüm, dijital ortamda depolanan kişisel verilerin kötüye kullanımını önlemek için yasal korumayı sağlayacak tutarlı ve kapsamlı dijital mahremiyet yasalarına acil ihtiyacın bulunduğunu ileri sürmektedir. Zira dijital çağda mahremiyet hakkının karşı karşıya kaldığı en büyük meydan okuma; bu alanda bağlayıcı mevzuat, yasa ve düzenlemelerin olmamasıdır. Bunların haricinde bu alan ile ilgili mevcut çoğu mevzuat ve düzenlemeler, mahremiyet kavramlarının net olarak tanımlanmamış bunun aksine kafa karıştırıcı ve muğlak kalmıştır. Bu durum gözetim ve hesap verebilirliğin olmaması, yetki veren merciler üzerinde bağımsız ve tarafsız bir organın olmaması ve yanıltıcı kullanım imkânı gibi belirgin sorunları taşmaktadır. Bütün bununlar ışığında dijital mahremiyet hakkının karşılaştığı tehditler ister hükümetlerden gelsin ister ise özel kişi veya kuruluşlardan, bu tehdit ve ihlallerin dijital mahremiyet hakkına keyfi saldırılar olmadan yaşama hakkı ve mahremiyetin yasal olarak nasıl savunulabileceği ve korunabileceği konusu ile ilgili önemli sorular gündeme getirmektedir.

A. Mahremiyetin Kökenleri ve Gelişimi

Mahremiyet, modern dönemin bir ürünü değildir. Zira Taş Devri'nden beri insan, güvenli alanını temsil eden evini ve kendi özel alanını korumanın önemini fark etmiştir. Böylece o zamandan beri özel hayat hakkı, Mezopotamya'nın Hammurabi Yasaları, Hindistan'ın Manu Yasaları ve eski Mısır yasaları gibi birçok Doğulu ve Batılı yasa aracılığıyla çeşitli şekillerde gelişerek korunmuştur. Ancak bu aşamalarda mahremiyet hakkı anlayışı, evi herhangi bir saldırı, suç veya casusluktan koruma konusunda sınırlı kalmıştır. Modern çağa gelince özel

hayat ve mahremiyet hakları yasalarla tanınmıştır. Bu bağlamda İngiliz yasaları, 1361 yılında dikiz etmeyi ve kulak misafiri olmayı cezalandırarak bu hakkı açık bir şekilde tanıyan ilk mevzuat olmuştur.

1890 yılında ise mahremiyet hakkı, "Mahremiyet Hakkı" adlı yasayı gözden geçirerek inceleyen bir makale yazan iki Amerikalı hukukçu Louis Brandeis ve Samuel Warren tarafından açık bir şekilde açıklanmıştır. Bu bağlamda Brandeis ve Warren, mahremiyet hakkını "insanların yalnız bırakılma hakkı ve mümkün olan en az müdahaleyle kendi hayatlarını istediği gibi yaşamaları" olarak tanımlamıştır.[1] Bu iki hukukçunun mahremiyet hakkı anlayışı, mahremiyetin bireyler için önemi ile sınırlı kalmamış, aynı zamanda o dönemde bilgi paylaşımında ve saklamasında kullanılan geleneksel yayın yöntemlerini ele geçirmenin mahremiyete olan tehlikesine işaret etmiştir. Böylece söz konusu makale, mahremiyet hakkı ile ilgili literatürün önemli bir parçası haline gelip mevzuatın değişmesine yol açmıştır.[2]

Bu anlamda söz konusu mahremiyet hakkı anlayışı, o dönemde anayasal bir değişikliğe yol açmasa da bazı anayasal haklara zemin hazırlayarak Amerika Birleşik Devletleri'nin (ABD) ulusal düzeyinde birçok yasanın ortaya çıkmasında etkili olmuştur. Bu bağlamda ABD'de birçok mahkeme, Warren ve Brandeis'in mahremiyet hakkı anlayışını benimsemiş ve onların mahremiyet hakkı ile ilgili düzenlemelerin genişletme çağrılarına desteklemiştir. Böylece Warren ve Brandeis'in mahremiyet hakkı anlayışı ve tanımı, şu ana kadar çoğu ülkelerin hukuku düzenlemelerinde yerini korumakla birlikte onların makalesi Amerikan toplumu ve hukukunda önemli bir yer tutmaktadır. Bunun göstergesi de ABD'nin mahkemeleri, söz konusu makalenin yayımlanmasına bir asırdan fazla bir süre geçmesine rağmen şu ana kadar onu güvenilir bir kaynak olarak kabul etmektedir.[3]

[1] Samuel Warren ve Louis Brandeis, "The Right To Privacy", *Harvard Law Review*, 4/5 (1890), ss.193-220.
[2] Olga Kuznetsova ve Natalia Bondarenko, "Private Life Safety Provision In Digital Age", *The Journal Of Digital Forensics, Security And Law*, 12/3 (2017), s.80.
[3] Irwin Kramer, "The Birth of Privacy Law: A Century Since Warren and Brandeis", *Catholic University Law Review*, 93/3 (1990), s.703.

Mahremiyet kavramını tanımlayacak olursak; birincisi, bireyin başkalarının müdahalesine maruz kalmaksızın yaşam biçimini seçme hakkı ve ikincisi ise bireyin bilgileri başkalarıyla paylaşmak istememesi gibi mahremiyetten doğan özgürlüğü koruma hakkı olmak üzere iki temel ilkeye dayanmaktadır.[4] Bununla birlikte mahremiyeti belirleyen tanımlar; yere, zamana, kültüre, geleneklere ve mahremiyet kavramına neyin dahil edilmesi ve korunması gerektiğini belirleyen değerlere göre değişmektedir. Zira siyasi, kültürel, sosyal ve teknik unsurlarıyla bağlam, diğer tüm kavramlar gibi sürekli gelişen ve bu nedenle göreceli bir hak olarak kabul edilen mahremiyetin anlamını şekillendirmektedir. Ayrıca Mahremiyet anlayışı ve kavramı, ortaya çıkışından beri üç tarihsel aşamada farklı niteliksel değişimler geçirmiştir.[5]

İlk aşamada mahremiyet, maddi bir perspektiften ele alınarak insanların yaşamları ve mülklerinin korunmasına odaklanmıştır. İkinci aşamaya gelince bu hak, yavaş yavaş değerler ve manevi mahremiyet gibi daha baskın bir manevi boyut kazanmaya başlamıştır. Üçüncü aşamada ise mahremiyet hakkı, görünüşüne veya hakkın niteliğine bakılmaksızın insanı, yaşamına yönelik her türlü saldırı ve müdahaleden korumayı amaçlayan bir anlam kazanarak bir kamu hakkı haline gelmiştir. Bununla birlikte mahremiyet hakkı, bilgilerin gizliliği hakkı veya bireylerin kişisel verileri koruma ve olası ihlallerin karşısında kontrol etme hakkı gibi anlayışlarla teknik anlamda özel hayat hakkının bir parçası olarak ortaya çıkmıştır.[6]

1. Özel Hayat Hakkı, Ondan Ortaya Çıkan Mahremiyet Hakkı ve Aralarındaki Farklar

Mahremiyet hakkının tanımlarının çoğu özel hayat hakkına dayanmıştır. Aynı zamanda araştırmacıların çoğunluğu, iki kavramın de benzer olduğunu düşünmektedir. Ancak "özel hayat hakkı" kavramı, özellikle Latin Amerika ülkelerinde yaygınlık kazanan ve yasal olarak ilk kez tanınan kavramdır. Aynı zamanda özel hayat hakkı eski çağlardan beri kullanılan

[4] Naim Mugabgib, *Makhatir Almaelumatia Walantarnit (TR: Bilişim ve Internet Tehlikeleri)*, Beyrut: Al-Halabi Hukuk Yayınları, 2.b., 2008, s.98.
[5] Mahmoud İbrahim, *Alhimaya Aljinayiya Lilkhususia Waltijara Al'iiliktirunia (TR: Mahremiyetin ve E-Ticaret Alanlarında Cezai Koruma)*, 1.b., İskenderiye: Al-Wafa Hukuk Yayınevi, 2014, s.272.
[6] Annie Anton ve John Mylopoulos, "Digital Privacy: Theory, Policies And Technologies", *Requirements Engineering*, 16/1 (2011), ss.1-2.

geleneksel kavram iken mahremiyet hakkı daha çok modern döneme ilişkin bir anlayışı taşmaktadır. İlk başta mekân, bireyin özel hayat alanını belirlemekte asıl kriter ve başlangıç noktası temsil etmiştir. Başka bir deyişle mekân, yani bireyin mekânsal alanı ve bu alanın tanık olduğu olaylar, onun özel hayatı ile eş anlamlı bir kavram olarak algılanmıştır. Özellikle 1991 yılından beri internet ağlarının yarattığı teknolojik sıçrama çerçevesinde artan kişisel verilerin dolaşımı ve bu dolaşım durumunu saklanması nedeniyle özel hayat kavramından mahremiyet kavramına yönelik bir geçiş yaşanmıştır.[7]

Bu bağlamda mahremiyet kavramının kriteri yer ve mekânsal alandan çok bireylerle ilişkilendirilmiştir. Bu nedenle insanları korumak ve edinilen bilgilerinin güvenliğini sağlamak için yasalar çıkarılmıştır.[8] Böylece "mahremiyet hakkı, yerin kamusal veya özel niteliğine bakılmaksızın, bir yere koruma sağlayan hak statüsünü kazanmıştır çünkü bireyin hukuki korumadan yararlanabilmesi için önemli olan yer değil, içinde bulunduğu durumdur".[9] Özel hayat, insanın iç dünyası, düşünceleri, duyguları, dünya görüşü ve psikolojik güvenliğidir.[10] Ancak özel hayat hakkı ile mahremiyet hakkı arasındaki temel fark, özel hayat hakkı çoğu zaman ev gibi fiziksel bir unsura işaret ederken; mahremiyet hakkı, kişisel konuşmalar ve telefon görüşmeleri gibi manevi bir unsuru ele almasıdır.[11]

Özel hayat kavramı, kavramın bireyin yalnız bırakılma hakkının ötesine geçip genişlemesiyle birlikte mahremiyet kavramına dönüşmüştür.[12] Mahremiyet kavramı, gizliliğin esasını temel alan manevi boyutu içermiş ve müdahalenin her türünü kapsayarak kişisel bilgilerin kontrol

---

[7] Nasir Muhammad, *Haqa Al'iinsan Fi Himayat Hayaatih Alkhasat Fi Alqanun Alduwali Waltashrieat Aldaakhilia (TR: Uluslararası hukukta ve iç mevzuatta insanın özel hayatını koruma hakkı)*, 2.b., Riyad: Hukuk ve Ekonomi Yayınevi Yayım ve Dağıtım, 2013, s.33.
[8] Muhammad, a. g. e., s.35.
[9] Hussam Alahwani, *Alhaqu Fi İhtiram Alhayaa Alkhassa Walhaqi Fi Alsumea (TR: Mahremiyete Saygı ve İtibar Hakları)*, 3.b., Kahire: Dar Al-Nahda Al-Arabiya, 2021, s.118.
[10] Malkova Zhuravlev, *Philosophy Of Information Security*, 2.b., Tula: Proceedings Of The Tula State University, 2014, s.42.
[11] Ahmed Samida, *Altanzim Alqanuniu Lilhaqi Fi Alkhususia: Almaskan - Alaitisalat Alkhasa - Albayanat Alshakhsia (TR Mahremiyet Hakkının Yasal Düzenlemesi: Konut - Özel Iletişim - Kişisel Veriler)*, 1.b., Kahire: Dar Al-Nahda Al-Arabiya, 2021, s.79.
[12] Muhammad, a. g. e., s.41.

edilmesini düzenleyen bir kamu hakkı haline gelmiştir.[13] Bu anlamda mahremiyet kavramı, farklı türleri ve nitelikleri olan birçok mahremiyet biçimini birleştirdiği için daha doğru bir kavram olarak kabul edilmiştir. Buna dayanarak Fransız yasa koyucusu, 17 Temmuz 1970 tarihinde yapılan bir yasa oylamasında özel konut hürmeti kavramını ve anlayışını mahremiyet kavramıyla değiştirilmesini kabul etmiştir.[14]

Özel hayat hakkının çeşitli tanımları bulunmaktadır. Örneğin; Fransız hukukçu Roger Nerson'a göre bu hak, bireyin sırlarını başkalarından saklama hakkı ve bireyin onayı olmadan hiçbir şahıs veya merciinin bunları bilememesi olarak tanımlamıştır. Aynı zamanda Nerson, bu hakkın kişisel haklar grubu içinde bulunduğuna ve bu grubun hepsini içermese de önemli bir parçasını temsil ettiğine inanmıştır.[15] Ayrıca Hukukçu Roger Collar, özel hayat fikrinin dünyada özel mülkiyet anlayışının gelişmesiyle birlikte giderek netleşmeye başladığına ve yerin kapsamını aşarak kişiyle ilgili herhangi bir haber veya resim izni olmadan yayınlamamakla ilgili bir anlam kazandığına değinmiştir.[16]

Özel hayat hakkı, yazılı veya sözlü yazışmaların korunması, fotoğrafların korunması, tıbbi kaydının korunması gibi bu hakkın kapsamına giren ve bireyin hiç kimsenin ihlal etmesini istemediği sır olarak kabul edilen birçok unsuru içermektedir. Başka bir deyişle özel hayat hakkı, bireyin kendisine ait olan üzerindeki egemenliğinin ifadesi ve bunun güvenliğinin teminatıdır.[17] Özel hayat hakkının mahiyeti ve doğası hakkında hukuk alanında uzun tartışmalar olmuştur. Zira bazı hukukçular, bu hakkın insanı ve insanlığı merkeze aldığı için kişisel haklar kapsamına girdiğini savunurken başka bir grup hukukçular, maddi anlamda

---

[13] Usama Qayed, *Alhimaya Aljinayiya Lilhayaa Wabanuk Almaelumat (TR: Özel Hayat ve Bilgi Bankaları İçin Cezai Koruma)*, 2.b., Kahire: Dar Al-Nahda Al-Arabiya, 1994, s.11.
[14] Samida, a.g.e., s.110.
[15] Oda Salman, "Aljraym Almasa Bihimayat Alhya Alkhasa Alty Tqe Ebr Wasayl Tqnyt Almaelumat Alhdytha" (TR: Modern Bilgi Teknolojisi Vasıtasıyla İşlenen Özel Hayatın Korunmasına İlişkin Suçlar), *Al-Rafidain College*, 16/29 (2018), s.99.
[16] Suleyman Fadl, *Almawajiha Altashrieia Wal'amniat Liljarayim Alnaashiat An İstikhdam Shabakat Almaelumat Alduwalia (TR: Uluslararası Bilgi Ağının Kullanımından Kaynaklanan Suçlarla Yasama Ve Güvenlik Alanında Mücadele Edilmesi)*, 1.b., Kahire: Dar Al-Nahda Al-Arabiya, 2013, s.215.
[17] Essam Al-bahji, *Himayat Alhaqi Fi Alhayaat Alkhasa Fi Daw' Huquq Al'iinsan Walmasyuwliat Almadania (TR: İnsan Hakları ve Medeni Sorumluluk Işığında Özel Hayat Hakkının Korunması)*, İskenderiye: Al-Jamia Al-Jadida Yayınları Yayınevi, 2005, s.29.

tasarruf edilebilir ayni haklardan oluştuğundan ve fikri mülkiyet haklarına benzeterek manevi anlamda da tasarruf edilebilir olduğundan dolayı bu hakkın mülkiyet hakları içinde değerlendirmiştir. Buna ilaveten diğer bir grup, bu hakkın birbiriyle kesişen bir haklar grubu olarak görmüştür.[18]

2. Dijital Mahremiyet Kavramının Ortaya Çıkışı ile Oluşumu ve Dijital Mahremiyet Hakkının Gelişimi

Teknolojinin ilerlediği dijital dünyada mahremiyet, önemli ve tartışmalı bir konu olarak yerini korumuştur. Bu anlamda özellikle internetin ve sosyal medya kullanımının yaygınlaşması ile kişisel mahremiyet alanında bir devrim yaşanmıştır. Ayrıca kamu ile özel kişiliklerin ayırt edilmesinin zorlaştığı bu dönemde, sayısı siber güvenlik tehditlerine maruz kalan kullanıcı sayısının arttığı görülmüştür. Dijital mahremiyet kavramının fiili ortaya çıkışı, geçen yüzyılın altmışlı ve yetmişli yılların sonunda, mahremiyet kavramını geleneksel anlayışın ötesine teknolojik ilerleme ve dijital alanda verilerin yayılması ile bağlayan bazı hukuk çalışmalarının yayınlanmasıyla ortaya çıkmıştır. Bu süreçte hukuk literatürü, birincisi Privacy and Freedom (Mahremiyet ve Özgürlük) eserini yazan Wisten Allen ve ikincisi The Assault on Privacy eserini yazan Arthur R. Miller olmak üzere iki Amerikalı yazara minnettardır.[19] Bu bağlamda iki yazar, bilgi mahremiyeti adlandırdıkları kavrama tanım ve açıklama sunmuştur. Bu anlamda Westin'e göre bilgi mahremiyeti, "bireylerin bilgilerinin başkalarına ne zaman, nasıl ve ne ölçüde ulaştığını belirleme hakkı"[20] anlamına gelirken Miller, bilgi mahremiyeti daha derin bir şekilde ele alarak "bireylerin kendileriyle ilgili bilgileri kontrol etme yeteneği" olarak tanımlamıştır.[21]

İnternetin ortaya çıkması ve dünyanın sürekli olarak tanık olduğu değişim çerçevesinde dijital mahremiyet ile ilgili çeşitli tanımlar ortaya koyulmuştur. Bütün bu tanımlar, teknolojiyi kullanırken verilerin korunması ve bilgi bankalarının garanti altına alma ile

---

[18] Al-bahji, a.g.e., s.31.
[19] Hadi Salem, *Aliaetida' Ela Alhayat Alkhasa Ean Tariq Al'iintirnti: Dirasa Muqarana (TR: İnternet Üzerinden Özel Hayata Yönelik Saldırılar: Karşılaştırmalı Bir Çalışma)*, Kahire: Dar Al-Nahda Al-Arabiya, 2018, s.130.
[20] Alan Westin, *Privacy And Freedom*, New York: Atheneum, 1967, s.34.
[21] Arthur Miller, *The Assault On Privacy: Computers, Data Banks, And Dossiers*, 1.b., Ann Arbor: University Of Michigan Press, 1971, s.1394.

kişisel verilerin otomatik işleme süreçlerinin karşılaştığı tehlikelerle mücadele edilmesi gibi noktalar etrafında toplanmıştır. Böylece dijital mahremiyet, genel ağlar üzerinden kişisel veya ticari işlemler yapıldığında internet üzerinden sağlanan kişisel bilgilerle ilgili mahremiyet olarak tanımlanabilmektedir.[22] Ayrıca dijital mahremiyet, bireyin dijital iletişim araçları üzerinden yayınlanan ve paylaşılan kişisel verilerinin koruma sürecinin bir tanımı olarak da görülebilmektedir. Bu bağlamda kişisel veriler, e-posta, banka hesapları, kişisel fotoğraflar, iş ile adres bilgileri ve bilgisayar, cep telefonu veya başka herhangi bir dijital iletişim aracını kullanırken internet etkileşiminde kullanılan tüm verilerden oluşmaktadır. Ürdün Açık Kaynak Derneği'ne göre dijital mahremiyet, kullanıcının bilgilerini dünyanın geri kalanından istediği zaman saklama yeteneğidir.[23]

Bugün dünya nüfusunun %58,7'sini temsil eden beş milyardan fazla internet kullanıcısı bulunmaktadır.[24] Bu bağlamda internetin veri işlemek ve depolamak için kullanılmasıyla bireylerin dijital dünya ile etkileşimi arttığı gibi siber suçların oranları yükselmiştir. Böylece dijital mahremiyet tehdit altına girmesiyle birlikte kişisel veriler, ticari olarak pazarlama tanıtımlarında kullanılabilen, devlet kurumları tarafından izlenen veya çalınarak sahipleri istismara maruz bırakan bir materyal haline gelmiştir. Sosyal medya, kullanıcıların arkadaşları ve aileleriyle etkileşim kurarken kendilerini güvende hissettikleri bir alan sağlamışsa da bireylerin, sadece sosyal ağlarda değil, bankacılık işlemleri sırasında da gerekli tüm güvenlik önlemlerini alması gerekmektedir.[25] Mahremiyet hakkının karşı karşıya kaldığı tehlikeler, işlemler sırasında kullanıcı anonimliğinin ihlalleri, kişisel verilerin yetkisizce ifşası, kişisel verilerin yetkisi verilmeyen amaçlarla kötüye kullanımı, kişiliği karalama ve benzeri çok çeşitli risk ve tehlikeler içermektedir.[26]

---

[22] Miller, a.g.e., s.1394.
[23] "Privacy", The Jordan Open Source Association, erişim 15 Ekim, 2021, https://2u.pw/auLuo.
[24] "World Internet Users Statistics And 2021 World Population Stats 2021", Internet Society, erişim 09 Ocak, 2021, https://2u.pw/nVuwE.
[25] Apu Kapadia vd., "Virtual Walls: Protecting Digital Privacy In Pervasive Environments", *Dartmouth Scholarship*, 5/3380 (2007) s.165.
[26] Kapadia vd., a.g.m., s.165.

Bu dönem, bireyler üzerinde gözetim ve casusluğun artması nedeniyle, bazı araştırmacılarca nitelendirildiği gibi, gözetleme ve mahremiyet ihlallerinin "altın çağıdır". Toplumlar, dijital teknolojiye ve internet bağlı cihazlara daha bağımlı hale geldikçe, mahremiyet hakkını korumaya yönelik uluslararası anlaşmalar ve konferanslar ışığında uluslararası hukuk ve kuralların çizdiği koruma parametreleri bilinmesi bir elzem haline gelmiştir. Ayrıca dijital alanda mahremiyet hakkını korumak adına ülkeler, mevcut cezai yaptırımları etkinleştirme veya ihtiyaç duyulan korumayı sağlayacak özel mevzuat oluşturma yollarına başvurarak bu alanda adımlar atıp odaklanması gerekmektedir. Bu bağlamda uluslararası, bölgesel ve ulusal anlaşmalar dijital haklara odaklanmaya çalışmıştır.[27] Örneğin İnsan Hakları Evrensel Beyannamesi (Madde 12), mahremiyeti temel bir hak olarak tanıyan ve dolayısıyla dijital mahremiyet hakkına aynı şekilde ele alınmasına zemin hazırlayan anlaşmalardan biri olarak görülmektedir.[28]

Bununla birlikte uluslararası sivil toplum ve STK'lar, devletlere ve özel şirketlere, mahremiyetin yasal olarak daha iyi korunması ve özel verilere erişim, depolama ve işleme konularında şeffaflık sağlanması için çağrılarda bulunmuştur. Ayrıca Avrupa ülkeleri, 1950 yılında imzalanan ve özel hayatın ihlalini yasaklayan 8. maddeyi içeren Avrupa İnsan Hakları Sözleşmesi ile insan haklarını korumak için ilk bölgesel örgütü kurmuştur.[29] Bununla birlikte dijital mahremiyet meselesinin yaşanan gelişmelerle daha önemli hale gelmesiyle Birleşmiş Milletler Genel Kurulu, 2012 ve 2013 yıllarında dijital insan haklarını korumaya yönelik kararlar almaya başlamıştır. Buna ilaveten Birleşmiş Milletler Batı Asya Ekonomik ve Sosyal Komisyonu (ESCWA), 2012 yılında kişisel verilerin korunmasına ilişkin tavsiyeler dahil olmak üzere internet ile ilgili mevzuat hakkında bir dizi tavsiye yayınlayarak Arap ülkelerinde bu tür mevzuatı uyumlu hale getirmeyi amaçlamıştır.[30]

Söz konusu verilerin korunmasına ilişkin tavsiyeler, büyük ölçüde 1995 yılında yayınlanan AB Veri Koruma Direktifi'ni ve Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından

[27] Al-bahji, a.g.e., s.84.
[28] İnsan Hakları Evrensel Beyannamesi, erişim 21 Ocak, 2022, https://2u.pw/v3aNw.
[29] Avrupa İnsan Hakları Sözleşmesi, erişim 17 Mayıs, 2022, https://2u.pw/GUOkn.
[30] Salem, a.g.e., s.106.

Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ile Konseyi Direktifi'ni temel almanın yanı sıra 1980 yılında yayınlanan Mahremiyetin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkelerine yönelik Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) Konsey Direktifi'ne dayanmıştır.[31] Mahremiyet hakkı, güçlü şifreleme gibi bilgisayar korsanlarının özel mesajları ele geçirme çabalarını neredeyse imkânsız hale getirecek ve şifrelemeyi kırmaya yönelik tüm girişimleri önleyecek şekilde kullanılan teknolojiler icat etmek gibi teknik bir yönü bulunmaktadır.[32]

Aynı zamanda Mahremiyet, hak ihlalleri durumunda hakkı koruyan, verileri depolamaktan ve işlemekten sorumlu tarafları hukuk önünde sorumlu tutan ve hükümet gözetimini yalnızca makul ve gerekli olduğu kadarıyla sınırlayan bir yasa çıkarmak gibi bir yasal boyutu içermektedir. Bu bağlamda üretilen veri hacminin büyüklüğü ve teknolojinin hızlı gelişimi nedeniyle dünyada mevcut veri koruma yasaları eski ve yetersiz olmuştur. Bunun için Avrupa Birliği, dört yıllık bir hazırlık sürecinden sonra Mayıs 2018 tarihinde şimdiye kadar türünün en büyük ve kapsamlı mevzuatı olan Genel Veri Koruma Tüzüğü'nü (GDPR) uygulamaya koymuştur.

B. Dijital Mahremiyet Hakkının Anayasal Ele Alınışı

1. Dijital Mahremiyet Hakkının Anayasal Ele Alınışı ve Yasal Kapsamının Genişletilişi

Mahremiyet Hakkının Anayasal Olarak Ele Alınışı, Dijital Mahremiyetin Yasal Kapsamının Genişletilişi ve Anayasaların Bireylerin Çevrimiçi Varlığını, Verilerini ve Mahremiyetlerini Koruma Çabası:

Dijital ve iletişim teknolojilerinin artan kullanımı ile dünyada yetkisiz müdahale girişimlerinin ve özel hayatın mahremiyetine yönelik tehditlerin ciddi bir şekilde artmasına

[31] "Regional Harmonization of Cyber Legislation to Promote the Knowledge Society in the Arab World", United Nations Economic and Social Commission for Western Asia, erişim 21 Ocak, 2022, https://2u.pw/r7Myr.
[32] Samida, a.g.e., s.44.

tanık olunmuştur.[33] Bu şartlar ışığında mahremiyet hakkı, devlet yetkilileri veya özel şirketler, gazeteciler, işverenler ve akrabalar gibi başka çeşitli gruplar tarafından ihlal edilme tehlikesine maruz kalmaktadır. Teknoloji kullanıcıları, çoğu zaman dijital teknolojileri akıllı ve bilinçli olmayan bir şekilde kullanarak kendi kişisel fotoğraflarını, verilerini, telefon numaralarını, adreslerini, hikayelerini ve hayatıyla ilgili videolar çeşitli internet sitelerinde yayınlayarak mahremiyet haklarını ihlal etme fırsatları yaratmakta ve kendi elleriyle kendi mahremiyet haklarını "kabahat kurbanı" haline getirerek tehlikeye atmaktadır.[34] Aynı şekilde bireyler, özel bilgilerin kullanımına ilişkin davranışlarının oluşturduğu tehdidi ciddiye almadıkları zaman dijital küreselleşme süreçleri yüzünden özel bilgilerinin "küresel alana" yayılma potansiyeli yükselmektedir.[35]

Bireylerin faaliyetlerinden yola çıkarak bireyin kişisel tanıtım bilgileri ve hassas kişisel bilgiler olmak üzere iki tür bilgi toplanabilmektedir. Bu anlamda teknoloji, bireylerin mahremiyetinin ihlal edilmesine, sırlarının genel erişme açılmasına ve hukuka aykırı bir şekilde istismar edilmesine olanak sağladığı için mahremiyet hakkını koruyup saldırıları önlemek adına uluslararası ve ulusal düzeylerde yasal müdahaleler gerekmiştir.[36] Mahremiyet yasalarının amacı, internet, telefon ve hatta posta gibi tüm bilgi aktarım ortamlarını korumaktır. Aynı zamanda bu hak, bireylerin finansal veya sağlık bilgileri gibi kayıtlarda yer alan özel bilgilerinin gizliliği korunmasını ve internette gezinme, iletişim yoluyla dolaşan özel verilerin de güvence altına alınmasını içermektedir. Mahremiyet hakkı, bilgi teknolojilerinin gelişmesiyle artan bilgisayar sistemlerinin potansiyel gözetim imkanları sonucunda altmışlı ve yetmişli yıllarda gelişmiştir. Bununla birlikte mahremiyetin korunmasını gerektiren çeşitli zorlukların ortaya çıkması sonucunda özel verilerin toplanması ve işlenmesi konusunu düzenleyen belirli kuralların oluşturulmasını elzem kılmıştır.[37]

---

[33] Stephanie Bird, "Security and Privacy: Why Privacy Matters", *Science and Engineering Ethics*, 19/3 (2013), s.670.
[34] Bird, a.g.m., s.669.
[35] Bird, a.g.m., s.670.
[36] Renta Mekovec, "Online Privacy: Overview and Preliminary Research", *Journal Of Information And Organizational Sciences*, 34/2 (2010), s.203.
[37] Mekovec, a.g.m., s.203.

Bu bağlamda veri koruma alanındaki ilk bilimsel gelişme, 1970 yılında Almanya'nın Hessen kentinde başlamıştır. Bundan kısa bir süre sonra mahremiyet ile ilgili ulusal yasalar ortaya çıkmaya başlayarak 1973 yılında İsveç'te dünyanın ilk bütünleşmiş ulusal veri koruma yasasının yürürlüğe girmiştir.[38] Ardından 1974 yılında Amerika Birleşik Devletleri, 1977 yılında federal düzeyde Almanya ve 1978 yılında Fransa mahremiyet ile ilgili ulusal yasalar çıkarmıştır.[39] Ocak 2018 tarihi itibariyle, dünyada 100 ülkeler veri koruma yasalarını benimsemiştir. Dijital mahremiyetin korunması güncel bir konu olduğu için, hükümetler veya diğer aktörler tarafından yapılan ve bu hakkı etkileyen ihlallerle baş etmek adına ilgili yasal çerçeveleri güncelleyerek hakkın nasıl korunacağına dair birçok adımın atılması gerektirmektedir.[40]

Bununla birlikte ülkeler, genel olarak mahremiyet ve özel olarak dijital mahremiyet haklarını anayasal olarak nasıl ele aldıkları konusunda farklılık göstermektedir. Mahremiyet konusunun halen yeni bir konu olarak değerlendirilmesi, bu alanda ülkeler arasında mevzuat ve anayasa farklılıklarının ortaya çıkmasının nedenlerinden biridir. Zira ülkeler, dijital dünyada mahremiyet hakkı ile ilgili konularda farklı deneyimlere sahip olmakla birlikte her ülke, kendi yasama çerçevesi dışında olan yeni sorunlarla karşılaştığında yasaları değiştirmek için dayandığı kendine ait farklı bir yasama felsefesi bulunmaktadır.[41]

Ayrıca dijital alanda mahremiyet konusuna gelince, e-posta korunması, sosyal medya verilerinin yayılmasına ilişkin kısıtlamalar, web tarayıcı etkinliğinin izlenmesi ve kayıtlı

[38] Samida, a.g.e., s.137.
[39] Yasen Qoutal, *Haqu Alkhususia Al'iilikturunia Bayn Altaqyid Wal'iitlaq (TR: Kısıtlama ile Özgürlük Arasında Dijital Mahremiyet Hakkı)*, 1.b., İskenderiye: Al-Wafa Hukuk Yayınevi, 2017, s.561.
[40] Qoutal, a.g.e., s.561.
[41] Salem, a.g.e., s.67.

verilerin ihlalleri gibi farklı konular düzenleyen çeşitli yasa türleri ortaya çıkmıştır.[42] Dijital mahremiyet ihlalleri, yanlış kişisel verilerin kullanılması, yasa dışı bir şekilde doğru kişisel verilerin toplanması, saklanması ve verilerin kötüye kullanılması ile kişisel verilerin hukuka aykırı bir şekilde ifşa edilmesi gibi birçok ihlal biçimi içermektedir. İhlallerin çeşitliği karşısında dünyada farklı dijital mahremiyet yasaları ortaya çıkmıştır.[43] Örneğin; internet hizmetleri sunan ve müşterilerin dijital bilgilerini depolayan şirketlere uygulanan Veri Koruma Yasası gibi şirketlerin müşterilerden onay almadan onların bilgilerini yayınlama veya başka taraflarla paylaşma imkânlarını sınırlayan yasalar bulunmaktadır.[44] Ayrıca iş ortamında, halka açık yerlerde veya evde bulunan internet iletişim araçlarının izlenmesini kısıtlayan İletişim Gözetimi Yasası gibi yasalar çıkarılmıştır. Buna ilaveten kimlik, e-posta ve her tülü kişisel veriler hırsızlığını engellemeyi ve bireyin interneti kullanırken paylaştığı kişisel verilerin korumayı amaçlayan Siber Suçlardan Koruma Yasası gibi yasalar örnekleri hazırlanmıştır.[45]

Bilgi mahremiyeti kavramı, geleneksel olarak bireylerin kişisel bilgilerin ifşası üzerindeki egemenliği olarak tanımlanmıştır. Ancak bugünlerde bilgi mahremiyeti, kişisel bilgilerin kullanımı ve yayılmasıyla daha fazla ilişkili bir kavram olarak tartışılmaktadır. Sonuç olarak bu çalışma, İnternet ve bilgi mahremiyetinin kesiştiği noktanın anayasal düzeyde ele alınması gerektiğini ileri sürmektedir. Yasa veya başka bir çözüm mekanizması, interneti kendi başına bir teknoloji olarak ele alabilmektedir. Zira, benzeri görülmemiş bilgi toplama haznesi ve diğer yeteneklerinin yanı sıra internet, bugünkü hayatın her alanına nüfuz etmektedir. Böylece bilgi mahremiyeti konusu, örneğin; finansal veya tıbbi kayıtlarla ilgili nadir bir endişe konusu olmaktan çıkarak günlük hayatın bir gerçeği haline gelmiştir.[46]

[42] Khadosh AlDahbi, "The Right to Privacy in The Face of Cyber Attack", *The journal of Teacher Researcher of Legal and Political Studies*, 8/1 (2017), s.144.
[43] AlDahbi, a.g.m., s.144.
[44] AlDahbi, a.g.m., s.144.
[45] AlDahbi, a.g.m., s.153.
[46] Woodrow Hartzog ve Neil Richards, "Privacy's Constitutional Moment and the Limits of Data Protection", *Boston College Law Review 1687*, 61/5 (2020), s.1702.

Mahremiyet hakkının ihlallerine karşı koruma mekanizmalarının oluşturulması hem ulusal mevzuatta hem de uluslararası mevzuat düzeylerinde çok çaba gerektirmiştir. Ayrıca bu alanın yasal çerçevesinde özellikle Arap ülkelerinde açık bir eksikliği bulunmaktadır. Bu bağlamda Arap ülkelerinin yarısında olduğu gibi ulusal düzeyde veri koruma yasaları yokken Tunus, Lübnan ve Fas gibi veri koruma yasalarını çıkaran ülkeler, bu alandaki politikaları hala kırılgan ve yasayı yürürlüğe sokmak ve uygulamak için yetersiz olarak kabul edilmektedir[47]. Bu zayıflık ve eksiklik nedeniyle bazı ülkelerin tüm vatandaşlarının kişisel verileri, ya maddi çıkar amacını güden özel şirketler tarafından ya da terör ve suçla mücadele etme veya güvenlik sağlama adına vatandaşlarını gözetmeye bunların dışında ifade özgürlüğü gibi haklarını ihlal etmeye çalışan hükümetler tarafından ifşa edilme durumu ve istismar riskine sürekli olarak maruz kalmaktadır.[48]

1.1 Batı Ülkelerinin Mevzuatlarında Dijital Mahremiyet Hakkının Korunması.

Tezin bu kısmı, özellikle dünyadaki farklı mevzuatı karşılaştırmalı bir şekilde etkilemekte önemli bir rol oynayan bazı Batılı ülkelerdeki dijital mahremiyetle ilgili mevzuatı incelemektedir.

İlk olarak Amerikan mevzuatında özel hayatın korunmasına gelince, bu hakkın anayasada açıkça ve doğrudan düzenlenmemiş ancak bazı değişikliklerle ele alınmıştır. Özel hayatın ve mahremiyetin korunmasına ilişkin olarak ABD Anayasası, inançların mahremiyetini koruyan birinci değişiklikten başlayarak evin mahremiyetini koruyan üçüncü değişikliğe kadar aşamalı olarak ilerlemiştir. Bundan sonra beşinci değişikliğe giden ABD Anayasası, bu değişiklikle suçlanan bireyin kendi aleyhinde tanıklık etmeye zorlanamayacağını hükme bağlayarak kişisel bilgilerin mahremiyetini savunan bir koruma getirmiştir.[49] Mahremiyet hakkı ile ilgili mevzuatın gelişim tarihi izlendiğinde ABD yargısı, bu hakkın her zaman maddi olmayabilecek ve niteliğini ve bu üç alanla ilgili yargı içtihatlarının yokluğu nedeniyle ilk başta bu hakkı tanımayı kabul etmemiştir. Bu bağlamda Amerikan hukukçular, özellikle

[47] Marwa Fatafta ve Dima Samaro, "Exposed and Exploited: Data Protection In The Middle East and North Africa", *Access now.org*, (2021), ss.9-14.
[48] Fatafta ve Samaro, a. g. e., s13.
[49] Tim Sharp, "Right To Privacy: Constitutional Rights and Privacy Laws", erişim 10 Ekim, 2021, https://2u.pw/37ndE.

o dönemin ekonomik ve sosyal koşullarının iyileşmesiyle insanı ve mülkiyetini koruyan mevzuatın geliştirme ihtiyacı gündeme getirmiştir. Bu gündem çerçevesinde mahremiyet hakkının korunmasının önemine vurgu yapmışlardır.[50]

Emsal bir durumun bulunmaması ve dolayısıyla hakkı açıklayan yasal bir metnin olmaması nedeniyle Amerikan yargısı, daha önce ona sunulmamış yeni bir durumun ortaya çıkması ilkesini uygulayarak mahremiyet hakkını korumuştur. Böylece bireyin yaşama hakkını temel alarak zamanın şartlarına göre barışçıl ve güvenli bir yaşam elde etme ve başkalarının kendi özel yaşamına karşımalarını ve mahremiyetini ihlal etmelerini engelleyebilme haklarını tanıyan bu ilke, ABD'nin Anayasa metinlerine girerek onaylanmıştır.[51]

Bunun sonucunda Amerikan yasa koyucusu, yargının işleyişinden etkilenerek 1935 yılında Amerika'da mahremiyet hakkını savunan ve bu hakka saldırı yapıldığında dava açılmasına izin veren bir yasa çıkarmıştır. Daha sonra Amerikan yasa koyucu, 1970 yılında dolaylı metinlerle bireyin mahremiyetini koruyan ve bilgiye erişimi garanti altına alan yeni düzenlemeler yürürlüğe koymuştur. Ardından 1974 yılında çıkarıldıktan sonra 1976 yılında düzeltilen ve federal hükümet tarafından tutulan kişisel bilgilerin izinsiz bir şekilde ifşa edilmesini yasaklayan, herkesin kendi kişisel bilgilerini gözden geçirme, düzeltme talep etme ve bunların herhangi bir kullanımını kendisine bildirme haklarını sunan ve böylece kişisel bilgilerle ilgili yargı denetimini sağlayan Mahremiyet Yasası çıkarılmıştır.[52]

Daha sonra finansal kurumların müşterilere toplanan bilgilerin türünü ve nasıl kullanıldığını açıklayan bir gizlilik politikası sunmasını; müşterilerden topladıkları bilgileri koruyacak güvenlik önlemleri almalarını gerektiren 1999 yılındaki Havale Yasası başta olmak üzere ABD'de mahremiyet hakkıyla ilgili birkaç yasa çıkarılmıştır. Buna rağmen Amerikan yasa koyucusunun planı, dijital veriler konusunu doğrudan ele alarak bireyin mahremiyetini ve özgürlüklerini koruyan bir yasa çıkaran Fransız yasa koyucusunun aksine, dijital veriler gibi

[50] Sharp, a.g.e.
[51] Sharp, a.g.e.
[52] Sharp, a.g.e.

belirli bir konu ile ilgili olmayan genel yasalar oluşturmak olduğunu söylemek mümkündür.[53]

Bununla birlikte Amerikan yasa koyucusu, 1986 yılında Elektronik İletişim Mahremiyeti Yasası'nı çıkararak iletişim ve bilgi alışverişi sırasında bireylerin mahremiyetine de koruma sağlamıştır. Zira bu yasa, özel elektronik haberleşmenin ele geçirilmesi veya yayınlanmasını yasaklayarak yasadışı sesli posta veya e-posta girişini suç ve yasa ihlali olarak değerlendirmiştir. Bununla birlikte Amerikan yasa koyucusu, aynı yılda Dolandırıcılık ve Bilgisayarın Kötü Kullanımı Yasasını çıkarmıştır.[54] Böylece Amerikan yasa koyucusu, bireylerin mahremiyetiyle ilgili özel verileri doğrudan açık metinlerle korumaktan ziyade kişisel mahremiyeti ve bilgileri korumak için genel metinler ve bir dizi federal ile eyalet yasalarını kullanarak dolaylı olarak korumuştur.[55]

Mevzuat bakımından dünyanın en köklü ülkelerinden bir tanesi olan Fransa'ya gelince onun yargısı, esnek olmanın yanı sıra yasal metinleri gerçekliğin gereklerine uyacak şekilde uyarlamaya çalışmakla bilinmektedir. Mahremiyetle ilgili olarak Fransız yasama organları, mahremiyet hakkını tanıyarak ve garanti altına alarak korunmasında kilit bir rol oynamıştır. Ayrıca Fransız hukukçular, bu hakkı savunup bunun yargı tarafından daha fazla tanınmasını ve korunmasını talep etmişlerdir. Bu bağlamda Fransız yargısı, Fransız medeni yasasında yer alan genel hukuki sorumluluk ilkesine başvurarak mahremiyeti korumuştur. Zira Fransız yargısı, başkalarına zarar veren her hatanın tazmin edilmesi gerektiğini savuna genel hukuki sorumluluk ilkesini özel hayata saldırı vakalarını içerecek şekilde genişletmiştir. Ancak Fransız hukuku açısından genel hukuki sorumluluk ilkesi, mahremiyet hakkının etkin bir şekilde korunmasını sağlamak için yeterli ve güvenilir bir dayanak teşkil etmemektedir.[56]

Zira, mağdura yeterli tatmin ve saldırgana yeterli caydırıcılık sağlamayı amaçlayan bu sorumluluk; hata, zarar ve nedensellik unsurlarının kanıtlanmasını gerektirdiği için bazı özel

[53] Sharp, a.g.e.
[54] Sharp, a.g.e.
[55] Sharp, a.g.e.
[56] Alahwani, a.g.e., s.118.

hayata saldırı vakalarında bahsi geçen unsurlar gibi şartları karşılamak zor olabilmektedir. Buna göre Fransız yasa koyucusu, özel hayata saygı hakkını açıkça desteklemek ve ona daha genel ve kapsamlı bir koruma sağlamak için müdahalede bulunmuştur. 27 Temmuz 1970 tarihinde özel hayatın korunmasına ilişkin bir yasa çıkarmıştır. Söz konusu yasanın 11. maddesine göre, herkesin özel hayatına saygı gösterilmesi hakkı olduğunu belirtmiştir. Bahsi geçen bu hakkı korumak için hakimlerin koruma, hapsetme ve özel hayata saldırıyı önleyecek veya durduracak başka her türlü tedbirin alınmasını emredebilme yetkesini vermiştir. Bu yasa ile ortaya koyulan prosedürlerin acil durumlarda geçici davaların hâkimi tarafından emredilebildiğini belirten Fransız yasa koyucusu, özel hayat hakkını bağımsız bir hak olarak kabul etmiş ve aslında yargının içtihatlarını, bu içtihatların daha önce vardığı görüşleri yasallaştırmaktan başka bir şey yapmamıştır.[57]

Bu anlamda Fransız hukuku, özel hayatın önemine dikkat çekmekle yetinmeyerek bireylerin mahremiyetini ve özgürlüklerini koruyan yasal garantiler sağlamak adına bilgisayar ve internet alanlarını ele alan yasal düzenlemeler oluşturmaya başlamıştır. Bu alanı bilgi bankaları haline getirmeye yönelik öncü bir rol oynamıştır. Özellikle, ceza hukukunun geleneksel metinlerinin özel hayatın korunmasına ve bireylerin özgürlüklerine ilişkin eksiklikleri çerçevesinde Fransız yasa koyucusu, 1978 yılında 17 sayılı Otomatik Veri İşleme ve Özgürlükler Hakkında Yasası'nı çıkarmıştır. Bu bağlamda bilişsel-dijital hak ve özgürlükler gibi konulara değinen söz konusu yasa, bilgi işleme mekanizmalarının tüm vatandaşların hizmetinde olması gerektiğini ve kişinin özel hayatına saldırmaması gerektiğini hükümlerini içermiştir. Ayrıca Fransız Ceza Yasası, ilgili kişinin düşüncesine zarar verecek veya özel hayatının kutsallığını ihlal edecekse verilerin ilgili kişinin izni olmadan üçüncü kişilere bildirilmesi bir suç olarak düzenlemiştir.[58]

Ayrıca Fransız yasa koyucusu, verilerin işlenmesi ve kullanımı sonucunda ortaya çıkan tehlikelerden kaynaklanan hukuki sorunları çözmek için çeşitli yasal düzenlemeler çıkarmıştır. Bu düzenlemelerin en önemlileri, 1980 yılında çıkartılan ceza durumunu dijital

[57] Alahwani, a. g. e., s.177.
[58] Salem, a. g. e., s.161.

ortamda işlenmesine ilişkin yasa, yasal işlemlerde delillere ilişkin yasa ile ticaret ve şirketler için muhasebe yükümlülüklerine ilişkin yasa gibi farklı yasalar bulunmaktadır. Dijitalleşme ve özgürlükler ile ilgili yasalara gelince, bu yasalar genel anlamda dijital verilerin işlenmesinin vatandaşın hizmetinde olması ve bireyin kişiliğine, haklarına, özel hayatına, bireysel veya kamusal özgürlüklerine yönelik herhangi bir zarar vermemesi gibi bir dizi temel ilke ve şartlar içermiştir.[59]

Ancak Avustralya gibi bir ülkede, kişisel bilgilerin işlenmesi konusunda 13 yasal ilkeden oluşan Avustralya Gizlilik İlkelerine (APP) dayanılmaktadır. Bu ilkelere göre kişisel bilgiler, açık ve şeffaf bir şekilde yönetilmesi gerekmektedir. Başka bir deyişle Avustralya Gizlilik İlkeleri (APP), kişisel bilgilerin nasıl yönetildiğine dair açık ve güncel bir gizlilik politikasının bulunmasını gerekli kılmaktadır. Ayrıca Avustralya yasalarına göre gizlilik politikaları, kişisel bilgilerin neden ve nasıl toplandığını, kişisel bilgilerin verilmemesinin sonuçlarını, bireylerin özel bilgilerine nasıl erişip bunları düzeltebileceklerini ve bireylerin bu bilgilerin ihlali hakkında nasıl şikâyette bulunabileceklerini açıklayan maddeler içermelidir. Zira Avustralya yasaları, dijital dünyada herkesin istediği zaman ücretsiz olarak şikâyette bulunabilme hakkını garanti altına almıştır. Ancak Avustralya yasaları, kişisel verilerin kullanımı veya ifşası gerekli olduğu durumlar için istisnaları koymuştur. Örneğin; yasayla izin verilen veya mahkeme emri istenilen kullanım ve ifşa istisnalarının yanında ceza gerektiren suçların önlenmesi, tespit edilmesi, soruşturulması, kovuşturulması veya cezalandırılması için kişisel verilerin polis tarafından kullanılması veya ifşa edilmesi da istisnalar arasındadır.[60]

Finlandiya'da ise Kişisel Veriler Yasası, mahremiyetin temel bir hak olduğunu kabul ederek toplanan kişisel verilerin işlenmesi düzenlemektedir. Aynı zamanda Finlandiya'da kişisel veri toplayan herkes, verileri toplamak için açıkça tanımlanmış bir amacı olması gerektiğinin yanı sıra bu verileri başka bir amaç için kullanılması yasaklanmıştır. Bununla birlikte Finlandiya yasaları, kişisel veriler ancak kullanıcının açık rızası alındıktan sonra

[59] Salem, a. g. e., s.161.
[60] Law No.119 of 1988: Privacy Act 1988, Australia, erişim 27 Şubat, 2022, https://2u.pw/J1enx.

toplanabildiği ve verileri toplayan kişi, şirket veya kuruluşun adı, adresi ve veri toplama amacı dahil olmak üzere herkesin kullanımına sunulacak veri dosyası açıklamasını oluşturması gerektiği şartlarını koşmuştur. Ayrıca doğrudan pazarlama veya pazarlamayla ilgili diğer kişiselleştirilmiş iletişimler amacıyla kişisel veriler toplanıyorsa özel kısıtlamalar uygulanmaktadır. Bu kısıtlamalara örnek verilecekse veri tabanında müşterilerin hiçbir hassas verisi toplanamayacak ve sadece temel iletişim bilgileriyle sınırlı yetinilecektir.[61]

Ayrıca Portekiz'de Kişisel Verilerin Korunması Yasası uyarınca, kişisel verilerin işlemesi kullanıcıların gizliliğine saygı duyularak şeffaf bir şekilde gerçekleştirilmesi gerekmektedir. Aynı zamanda kişisel veriler, yalnızca belirli ve meşru amaçlar için ve yalnızca kullanıcının açık rızası alındıktan sonra toplanabilmektedir. Ayrıca kullanıcıya verilerin işleme amacı, işleyenin kimliği, verilerin diğer alıcıları ve benzeri belirli bilgilerle verilmesi gerekmektedir. Bu bağlamda Portekiz Anayasası, "bilgisayarları, nüfus sayımıyla ilgili ve kişisel olmayan veriler dışında, siyasi eğilimler, dini inançlar veya özel hayatla ilgili verileri işlemek için kullanılamaz" maddesini içermektedir. İsveç'te ise kullanıcıların kişisel bilgilerinin mahremiyetini koruyan Kişisel Veriler Yasası, kişisel verileri geniş bir şekilde tanımlayarak doğrudan veya dolaylı olarak yaşayan bir kişiye atfedilebilen herhangi bir veri olarak tanımlamaktadır. Ayrıca söz konusu yasa, kullanıcıların kişisel verilerinin işlenmesiyle ilgili bilgi alma hakkına sahip olduklarını ve verilerinin toplanabilmesi için önce kişilerin gönüllü, spesifik ve açık onay vermeleri gerektiğini belirtmiştir.[62]

Orta Doğu ve Kuzey Afrika bölgelerindeki kullanıcılar, verilerinin nasıl toplandığı ve dijital ortamda mahremiyetinin nasıl korunduğu konusunda dünyanın en çok endişelenen kullanıcılar arasında yer almıştır. Zira kişisel verilerin korunmasıyla ilgili endişelenme konusunda Avrupalıların %67'sine endişeli iken Orta Doğu ve Kuzey Afrika bölgelerindeki kullanıcılar %85'i, bu konu ile ilgili endişelerini bildirmiştir. Bunun sonucunda olarak, Orta Doğu ve Kuzey Afrika bölgelerindeki çoğu kullanıcılar giderek dijital davranışlarını

[61] Law No.90 of 2016: Personal Data Act, Finland: Official Journal, erişim 27 Şubat, 2022, https://2u.pw/OShX0.
[62] Finland: Official Journal, a.g.e.

değiştirmekte ve kendilerini korumak için önlemler almaktadır. Örneğin; bu bölgelerde kullanıcıların %38'i belirli web sitelerinden kaçınırken %37'si daha fazla gizlilik ayarları kullanmaktadır. Ayrıca bu bölgelerdeki kullanıcıların dörtte biri internette söylediklerine öz denetim uygularken neredeyse her beş kişiden biri (%16) daha az çevrimiçi alışveriş yapmaya başlamıştır.[63]

1.2 Arap Ülkelerinde Dijital Mahremiyet Hakkı ile İlgili Mevzuat:

Orta Doğu ve Kuzey Afrika bölgelerindeki yasalara gelince, örneğin; Mısır mevzuatında dijital mahremiyet ve korunması ile ilgili özel bir yasa bulunmamaktadır. Bunun aksine dijital mahremiyetin korunması, konu ile ilgili özel destekleyici bir yasa olmadan mahremiyeti bir bütün olarak ele alan ve zımnen dijital mahremiyeti içeren bir sürü genel anayasal madde ile değerlendirilmiştir. Örneğin; Mısır Anayasası'nın 57. maddesi, "Vatandaşların özel hayatı dokunulmazdır ve gizliliği teminat altındadır. Posta, telgraf ve elektronik yazışmalar, telefon görüşmeleri ve diğer iletişim araçları, yasalarda belirlenen ve yargı emirlerine uyan belirli bir süre dışında haczedilemez, izlenemez, görüntülenemez" hükmünü içermektedir. Ayrıca bilgiye erişim konusunda Mısır'ın 2012 Anayasası, bilgiye erişimin "Özel hayatın mahremiyetini, diğer kişilerin haklarını ve milli güvenliği zedelemeyecek bir şekilde devletin her vatandaşa güvence altına aldığı bir hak" olarak tanımlamıştır.[64]

Banka müşteri verileri ve hasta verileri gibi belirli konumlardaki kişisel verileri koruyan yasaların yanında Mısır ceza mevzuatı, özel yerlerde fotoğraf çeken veya bir vatandaşın özel hayatının mahremiyetini ihlal eden kayıtlar yapan kişilere cezai yaptırım uygulamaktadır.[65] Cezayir üzerine verilen örneğe gelince ise, Cezayirli yasa koyucu, medeni yasada bireyin mahremiyet hakkının korunduğunu doğrudan ve açık bir şekilde belirtmiştir. Bu bağlamda

---

[63] "Regional Briefing: Consumer Privacy And Data Protection In The Middle East And North Africa", Consumers International Insight Briefing 2019, ss.2-4, erişim 23 Ocak, 2022, https://2u.pw/izrtD.
[64] Abdullah Shath, *Hurmat Alhayaat Alkhasa Fi 'Atar Alkhususia Walhimaya Walhaqi Fi Almuraqaba (TR: Mahremiyet, Koruma Ve Kontrol Hakkı Çerçevesinde Özel Hayatın Gizliliği)*, İskenderiye: Al-wafa Hukuk Yayınevi, 2017, s.24.
[65] Law No.175 of 2018, Anti-Cyber and Information Technology Crimes Law, Egypt: Official Journal, erişim 11 Aralık, 2021, https://2u.pw/fXiQW.

Cezayir mevzuatı, kişiliğe özgü hakların güvence altına alınmasına medeni yasanın 47. Maddesinde atıfta bulunmuş ve bu madenin metnine göre: "Kişiliğe özgü haklardan birine hukuka aykırı bir saldırıya uğrayan herkes, bu saldırının durdurulmasını ve uğrayabileceği zararın tazmin edilmesini talep etme hakkına sahiptir".[66]

Ürdün'ün yasal çerçevesine gelince, özel hayat hakkı anayasal bir hak olarak kabul edilmektedir. 2012 yılında, iletişimin dinlenmesini düzenlemek amacıyla anayasada bir değişiklik yapılmasının yanında yasal çerçevede dijital temasların ve kişisel bilgilerin çeşitli idari birimler tarafından depolanması ve bunlara erişimini yasallaştıran çeşitli değişiklikler devreye sokulmuştur. Ancak bu süreçte yapılan anayasa değişikliği, gözetimi düzenleyen diğer yasalara dokunmamıştır. Örneğin; Ürdün yasal sistemleri, 2015 yılına kadar İletişim Yasası kapsamında yargısal veya idari bir talep yoluyla verilerin izlenmesine izin verilmektedir. Öte yandan Terörle Mücadele Yasası, savcının bir kişiyi "terörist faaliyetlere" bağlayan "güvenilir" bilgilere dayanarak gözetim altına almasına izin vermektedir. Ancak bu yasa, neyin "güvenilir" olduğu veya neyin "terör faaliyeti" kapsamına girdiği konusunda açık tanımlar yapmamıştır.[67]

2015 yılında Ürdünlü yasa koyucu, nesnel ve usule ilişkin olan 17 maddeyi içeren Siber Suçlar Yasası adlı bir yasa çıkarmıştır. Söz konusu yasanın maddeleri incelendiğinde özel hayatı korumak için maddeler tahsis ettiği görülmektedir. Üçüncü tarafların bireylerin verilerine veya bilgilerine erişmesini sağlayan herkesi cezalandıran 4. madde ve bilgi ağı veya herhangi bir bilgi sistemi aracılığıyla gönderilen içeriği kasıtlı olarak ele geçiren, iletilmesini engelleyen, gizlice dinleyen veya silenlerin cezalandırılacağını belirten 5. Madde gibi bu yasanın özel hayatla ilgili içerdiği maddelere örnek verilebilmektedir. Bu yasanın çıkarılmasına rağmen, Ürdün'de özel hayatın korunmasında ciddi bir boşluk ve eksiklik bulunmaktadır. Zira, söz konusu yasa, açık bir şekilde ihlali durumunda cezaya tabi olan ve

[66] Shath, a.g.e., s.26.
[67] Article 4 Of Anti-Terrorism Law: "If The Prosecutor General Received Reliable Information Indicating That A Person Or Group Of Persons Is Connected To Any Terrorist Activity, The Prosecutor General Can Impose Surveillance Over The Residence Of The Suspect, His Movements, And His Means Of Communication", erişim 14 Aralık, 2021, https://2u.pw/fXiQW.

korunması gereken bilgileri belirtmemiş ve bu konuyu kamuoyuna bırakarak cezasızlık olasılığını artırılmasına zemin hazırlamıştır.[68] Bu bağlamda Ürdün'ün mahremiyet ve veri koruma mevzuatı, veri toplama ve paylaşma uygulamalarına ilişkin belgelenmiş kanıtların eksikliği nedeniyle bu alandaki düzenlemeler ve tartışmalar henüz başlangıç aşamasındadır.[69]

2012 yılında kabul edilen Basın Yayın Yasası'nda yapılan değişiklikler, dijital medya araçlarının sahiplerini ve çalışanlarını "aracının sorumluluğu" ilkesi çerçevesinde "yayınlanan tüm kullanıcı yorumlarının kaydını en az altı ay süreyle tutmakla yükümlü" hale getirmiştir.[70] Ayrıca Ürdün yasaları, özel mesajların yasa dışı yayılmasını cezalandırmasına rağmen cezalar farklı yasalar arasında tutarsızlık olduğunu fark edilmektedir. Bu bağlamada ceza yasası özel mesajların içeriğini yayınlamayı üç ayı geçmeyen hapis cezası ile cezalandırırken telli ve telsiz iletişim yasasının cezası, bir aydan bir yıla kadar hapis ve 100 Ürdün dinarından 300 Ürdün dinarına kadar tazminat arasında değişmektedir. Ayrıca bu cezalar, güvenlik kurumlarında bulunan kamu görevlileri hariç olmak üzere, yalnızca aramaları yönlendirmek için görevlendirilen kişilere uygulanmaktadır.[71]

1.3 Batı ve Arap Ülkeleri Arasında Dijital Mahremiyet ile İlgili Mevzuatın Karşılaştırılması

Yukarıdaki noktalara kapsamlı bir şekilde baktığımızda dijital mahremiyet konusunda farklı ülkelerin mevzuatları arasındaki farkları şu şekilde özetleyebiliriz:

---

[68] Bariq Lami, "*Jarimat İntihak Alkhususia Eabr Alwasayil Al'iilikturunia Fi Altashrie Al'urduniyi: Dirasa Muqarana" (TR: Ürdün Mevzuatında Dijital Araçlar Yoluyla Mahremiyetin İhlali Suçu: Karşılaştırmalı Bir Çalışma)*, Yüksek Lisans Tezi, Orta Doğu Üniversitesi, 2017, s.87.

[69] "Digital Privacy In Jordan: Perceptions And Implications Among Human Rights Actors", Irckhf Haqqi, erişim 10 Eylül, 2021, https://2u.pw/gVHFf.

[70] Rana Sweis ve Dina Baslan, *Mapping Digital Media: Jordan*, 1.b., Amman: Open Society Foundations, 2013, ss.8-13.

[71] Article 71 Of Telecommunication Law: "Anybody Who Spreads Or Releases The Content Of Any Communication Through Public Or Private Networks Or Views A Telephone Message By The Nature Of His Job, Or Records It Without Legal Base, Will Be Penalized A Prison Sentence For No Less Than A Month And No More Than A Year, Or By A Fine No Less Than 100 Jods Or More Than 300 Jod, Or With Both Penalties."
Article 384 Of Penal Code: "Responding To The Complaint Of The Victim, One Is Penalized For Not More Than Three Months In Jail For Breaching The Private Lives Of Others By Eavesdropping, Peaking, Or Any Other Medium Including Recording Audio. The Penalty Is Multiplied In Case Of Repetition."
Article 356 Of Penal Code: "Anybody Who Spreads The Content Of A Private Call Within The Capacities Of His Position In The Telephony Service Will Be Penalized For 6 Six Months Or Charged With 20 Jods. (Article 35,6 Months Or Charged With 20 Jods.", erişim 04 Ekim, 2021, https://2u.pw/ru11b.

İlk olarak ülkelerdeki farklı hukuk sistemlerinin, hız ve yavaşlık açısından henüz yasal bir çerçeve bulamayan yeni gelişmelere ayak uydurmaktaki etkisini görüyoruz. Örneğin Fransız hukuk sistemi (Medeni hukuk-Civil Code)[72], medeni hukukun genel kurallarının hakimlere verdiği geniş içtihat alanına ve yargının ile içtihat biliminin hükümleri geliştirme kabiliyetine dayanarak mahremiyet hakkının ortaya çıkışından beri ayak uydurmaktadır. Ancak Amerikan hukuk sisteminin (Anglosakson sistemi-Common law)[73], önceki yargı kararlarına

[72] Medeni hukuk terimi (Civil Code), Latince ius Civile teriminden türetilmiştir. Orta Çağ'da Avrupalılar, Roma hukukunu ve özellikle milattan sonraki altıncı yüzyılda İmparator Justinian tarafından çıkarılan Roma yasalarını yeniden keşfetmiştir. Bu hukuk sistemi, Orta Çağ Avrupa'sında yasaların temel aldığı zemin olarak görülmüştür. Bu anlamda Avrupalı hukukçuların farklı nesilleri, Roma hukukunun o dönem Avrupa'sındaki güncel koşullara göre uyarlanması için ciddi çabaları harcamıştır. O dönemde kilise, yasal sistem dahil olmak üzere Avrupa'daki hayatın tüm alanlarında hegemonyasını dayatmış ve bu nedenle o dönemin hukukçuları kilise yasalarından etkilenmiştir. Böylece Orta Çağ'ın sona ermesiyle birlikte Roma hukuku ve kilise hukuku, Avrupa hukuk anlayışının ana temelini oluşturmuştur. Bu iki hukuka ek olarak gelenekler, Avrupa'da medeni hukukun önemli bir kaynağı olmuştur. Zira devletlerin kendi hukuk sistemlerini birleştirme ve düzenleme çabaları, medeni hukukun bir kaynağı olarak geleneklerin öneminin artmasına zemin hazırlamıştır. Bunun sonucunda farklı ve dağınık yasal hükümleri düzenlemek için bilimsel deneyimler görülmeye başlanmıştır. Ayrıca gelenekler ile yerel yasalar arasında uyum sağlanmaya çalışılırken, Aynı zamanda medeni hukukun mantıksal ilkeleri ile doğal hukuk arasında uyumu gerçekleştirilmeye amaçlanmıştır. Dönemin Aydınlanmış hükümdarlarının desteğiyle, bu çabalar tarihsel anlamda en önemli medeni yasaların doğmasıyla sonuçlanmıştır. Bunların örneklerinden: II. Joseph'in 1786 tarihli Avusturya Kanunu, 1811 tarihli Tam Avusturya Medeni Kanun, 1794 Tarihli Prusya Umumî Memleket Kanunu ve Fransa Hukukundan Napolyon Kanunu olarak bilinen 1804 tarihli Medeni Kanun. Latin sistemi, ayrıntılı bir düzenleme sistemiyle bilinir. Başka bir deyişle Latin sistemi, yasal kural ve hükümleri konu veya prosedür açısından ayrılmış mevzuatta düzenlenerek mahkemeye getirilebilecek davalar için hükümler belirleyen maddeler şeklinde yazılan bir hukuk sistemidir. Aynı zamanda bu hukuk sisteminde mahkeme huzurundaki davaların görülmesinde uyulması gereken hususlar, suç oluşturan fiiller ve bu suçlara verilecek cezalar belirtilir. Bu sistemdeki yasalar çeşitlidir, örneğin olayların yasal hükümlerini belirleyen, suç veya cezayı belirleyen nesnel yasalar vardır. Aynı zamanda davanın gidişatını ve bununla ilgili tüm prosedürleri özetleyen usul yasaları bulunmaktadır. Hukuk veya ceza davaları olsun). Bu anlamda Hâkim, yazılı mevzuatta yer alan hükümlere uymakla yükümlü olduğundan, Latin sistemindeki rolü sınırlı kalmaktadır. Aynı zamanda Hâkim, yasa koyma sürecinde daha büyük bir role sahip olan yasa koyucular, yorumcular ve hukukçuların karşısında daha kısıtlı bir rolü bulunmaktadır. Hazem Zahroudi, *Tarihul Kanunul Madani (TR: Medeni Kanun Tarihi)*, 2.b., Beyrut: Arap Araştırmaları ve Yayınları Merkezi, 2017, ss.23-29

[73] Anglosakson sistemi, Orta Çağ Avrupa'sında ortaya çıkmıştır. Bu sistem, Britanya'da gelişmiş ve oradan daha sonra Britanyalı kolonilere yayılmıştır. Bu sistem, mutlak monarşinin Britanya üzerindeki kontrolü sağladığı dönemden başlayarak meşruti monarşi dönemine kadar süren süreçte gelişmiştir. Bu sistemin gelişmesi, bunun farklı iç siyasi olaylara adapte olmasıyla eş zamanlı olarak meydana gelmiştir. Bunun sonucunda bu sistem, Avrupa'nın geri kalanında yaygın olan sistemden farklı bir şekilde gelişmiştir. Anglosakson sisteminin temel özelliği, ayrıntılı bir düzenleme sisteminin olmamasıdır. Başka bir deyişle bu sistemde, yasal kural ve hükümleri içeren ayrıntılı ve yazılı bir mevzuat bulunmamaktadır. Bir yargı uyuşmazlığı meydana geldiğinde Hâkim, söz konusu uyuşmazlığı hükme bağlamak için genellikle benzer bir uyuşmazlığa uygulanmış olan önceki yargı kararlarına dayanmaktadır. Bu anlamda önceki yargı kararları veya bazen yasama kararları adıyla bilinen bu kararlar, hâkimin uyguladığı yasa olarak kabul edilir. Bu hukuk sisteminin uygulanmasının sonucunda hâkimler, hukuku ve onun hükümlerini oluşturmak konusunda daha büyük bir yetki sahip olmuştur. Ayrıca bu sistem, hâkimlere kendi anlayışlarını ve içtihatlarını uygulamak için daha fazla alan sağlamaktadır. Bu sistemi uygulayan ülkeler, jüri komitesi adıyla bilinen bir sistem benimsemektedir. Jüri komitesi, toplumun içinden hukukçu olmayan normal insanlardan oluşan ve davanın gerçeklerine göre karar vermekle yükümlü olan bir

bağlı olması nedeniyle mahremiyet konusuna ilişkin doğası açısından yeni uyuşmazlıkların ortaya çıktığında ayak uydurmakta zorluk çektiğini görüyoruz.

Aynı zamanda yukarıdaki noktalara bakarak ABD ve Avrupa ülkelerindeki veri mahremiyeti ile ilgili mevzuatın genel özelliklerini şu şekilde özetleyebiliriz: Bu ülkeler, bir yandan veriler üzerinde güçlü bir koruma sağlayacak yasaları artırırken, diğer yandan bu verileri işleyen tarafların çalışmalarını düzenlemeye yönelmişlerdir. Bu çaba, verilerin korunması ve düzenlenmesinin farklı yönlerini ele alan çeşitli yasalar çıkarmak ve yasal metinlerdeki muğlaklığı, genel hükümleri ve istisnaları mümkün olduğunca azaltmak gibi adımlarla ortaya çıkmaktadır. Bu ülkelerin bazılarında, söz konusu hakların önemini vurgulamak ve alt yasalarla ya da idari ile adli kararlarla ihlal edilmelerini engellemek için en üstün mevzuat olan anayasada bunlara yer verilmektedir. Aynı zamanda yasalar, vatandaşların verilerinin korunması konusuna ilişkin görevlerini netleştirmek adına devlet kurum ve kuruluşlarının yanı sıra büyük özel kurum ve şirketleri hitap edecek şekilde hazırlanmaktadır.

Arap ülkelerine gelince ise mahremiyet konusuna ilişkin yasal politikalar, genellikle mahremiyet ve veri korunma ile ilgili tüm yönleri kapsamayan yasalar koyduklarını görüyoruz. Ayrıca bazı Arap ülkeleri verilerle ilgili çeşitli yasalar çıkarsa da bunlar mükerrer olma eğilimindeydi ve birçok istisna ve (ulusal güvenlik, terör faaliyetleri, güvenilir bilgi vb.) geniş ve muğlak terimler içermektedir. Bu geniş ve muğlak terimler, yasanın özellikle devlet ve kurumları tarafından ihlal edilmesini kolaylaştıran bir boşluk olarak kabul edilmektedir. Arap ülkelerinin anayasalarına gelince, kişisel verilerin korunmasına ilişkin hakları çağdaş biçimiyle ele alan maddeler içermemekte ve bazıları geniş istisnalar dizmeyi ihmal etmeden mahremiyet hakkına yer vermiştir. Ayrıca Arap ülkelerindeki veri ve verinin korunmasıyla ilgili yasalar, genel ve herkese yönelik olmanın yanı sıra, çoğunlukla vatandaşlar ile özel kurum ve şirketler arasındaki ilişkilere müdahale etmemeyi tercih etmektedir. Aynı zamanda bu yasalar, vatandaşların verilerinin özel sektör tarafından işlenmesi konusunda güçlü kısıtlamalar getirmediği gibi bu verilere devlet kurum ve kuruluşları karşısında gerçek bir koruma sağlamamaktadır.

---

komitedir. Ayrıca bu sistemde hâkimin, jüri komitesinin verdiği karara göre davayı karara bağlamaktadır. Zahroudi, a.g.e,. ss.23-29.

2. *Anayasaların ve Yasaların Çözemediği Sorun ve İhlaller*

Dijital dünyada mahremiyet hakkı, geleneksel mahremiyet hakkına göre yasal, teknik ve düzenleyici koruma biçimleri arasında yoğun koordinasyon gerektiren bir avantaja sahiptir. Ayrıca internetin küresel doğası ile büyük şirketlerin belirli şehirlerde yerleşmesi sonucunda farklı mevzuat oluşmuş ve yasal konuları daha karmaşık hale gelmiştir. Tüm çabalara rağmen dijital mahremiyet ile veri koruma yasalarının çözemediği pek çok sorun bulunmaktadır. Bu sorunlardan en öne çıkanı, dijital mahremiyet yasalarının ihlal edilmesinin ve kişilerin onayı almadan verilerine erişmenin veya bunları başka kişilerle paylaşmanın gerekçesinin tanımsız ve genel temellere dayandırılmasıdır. Bu durum, özellikle hükümetlerin ve ülkelerin keyfiliği seçmeleri ve vatandaşlarının haklarını baskı altına almak istemeleri veya kendi önceliklerini ilk sıraya koymaları durumunda daha sıkça yaşanmaktadır.[74]

Örneğin; Mısır hukukuna bakıldığında, Siber Suçlar Yasası'nda web sitelerinin engellenmesi için milli güvenlik gibi belirsiz ve geniş kapsamlı nedenler öngörülmüştür. Bu bağlamda yasa, milli güvenlik kavramını, hem "vatanın bağımsızlığı, istikrarı, güvenliği, birliği ve toprak bütünlüğü ile ilgili her şey" hem de "cumhurbaşkanlığı ve Bakanlar Kurulu ile ilgili tüm iş ve işlemler" olarak tanımlamaktadır. Bu geniş tanım, baskıyı teşvik eden ve dijital mahremiyeti ihlal eden birçok gerekçe içermektedir. Bu bağlamda Milli Güvenlik Kurulu, silahlı kuvvetlerin soruşturma organları, İçişleri Bakanlığı, Genel İstihbarat, İdari Kontrol Kurulu ve bağlı kuruluşları, bu genel ve muğlak tanımdan çeşitli gerekçeler çıkararak gösteri çağrısı yapmak ve şiddeti teşvik etmek ile suçladığı protestoculara ve eylemcilere karşı davalar açmıştır. Böylece yasa ihlali kavramlarının açıkça tanımlanmaması, yetkililerin kendi tutum ve politikalarına aykırı olduğunu düşündükleri şeyleri gözetmek ve baskı altına almak için yasayı kötüye kullanabilecekleri veya ihlal edebilecekleri ve gözetimi milli güvenliği korumanın bir yolu olarak haklı gösterebilecekleri anlamına gelmektedir.[75]

---

[74] Bariq, a.g.e., s.23.

[75] Wafa Ben-Hassine, "Egyptian Parliament Approves Cybercrime Law Legalizing Blocking Of Websites And Full Surveillance Of Egyptians", accessnow.org, erişim 07 Şubat, 2022, https://2u.pw/I4SDM.

Hükümetlerin kişisel verileri hacklemesi ve dolayısıyla kendi vatandaşlarının dijital mahremiyet hakkını ihlal etmesi durumlarında şeffaflık ve hesap verebilirliğin olmaması yasal mevzuatta sorunlu bir konu temsil etmektedir. Bu durumlarda, özellikle Orta Doğu ve Kuzey Afrika bölgelerinde hükümetlerin bu hakkı ihlal etmek için kullandığı yöntemi belirlemek için ihtiyaç duyulan bilgilere ulaşmak oldukça zordur. Son dönemlerde dünya, hükümetlerin ve özel şirketlerin kişisel verileri ele geçirerek vatandaşların mahremiyetini ihlal ettiği vakalara tanık olmuştur. Bu vakaların genelinde vatandaşların kişisel verilerinin nasıl toplanıp işlendiğini ortaya koymak için gereken bilgileri elde etmek imkansızdır. Mahremiyet hakkına karşı devlet kaynaklı siber saldırıların çeşitli örneklerinden birinde Pegasus programı, Meksika hükümetinin insan hakları savunucularına ve yolsuzlukla mücadele alnında aktif olan gazetecilere karşı casusluk yapmasına ve onların mahremiyetlerini ihlal etmesine izin vermiştir.[76]

Tarihsel olarak dijital mahremiyet hakkındaki tartışma, sosyal ağların sunduğu hizmetlerin kullanımından doğan mahremiyet tehlikelerine odaklanmıştır. Bu bağlamda kitlesel gözetim programlarına ilişkin Edward Snowden[77] ifşa ettiği belgeler, devletlerin ve özel şirketlerin kişisel verilere, özel iletişimlere erişme; verileri paylaşma ve paylaşılan verileri manipüle etme gücü karşısında "mahremiyet hakkının" nasıl korunabileceği konusunda küresel bir tartışma başlatmıştır. Aynı zamanda söz konusu belgeler, gözetim faaliyetlerini yasalara tabi tutmanın önemini vurgulamakla birlikte dijital ortamda kişisel verilerin korunma gerekliliği konusunda genel farkındalık eşiğini yükseltmiştir. Bu durum, uluslararası toplumun bilgi akışını ve alışverişini güvence altına almak, alışveriş akışını kontrol etmek için alması gereken tedbirleri ve önlemleri artırmıştır.

[76] Azam Ahmed ve Nicole Perlroth, "Using Texts As Lures, Government Spyware Targets Mexican Journalists And Their Families", New York Times, erişim 21 Şubat, 2022, https://2u.pw/3ln4k.
[77] Edward Snowden, Bireylerin Kişisel Bilgilerini İçeren Toplu Verilere Erişmek, Depolamak ve Analiz Etmek İçin Farklı Ülkelerdeki Ulusal Güvenlik Ajanslarının Uluslararası Şirketlerle Yaptığı İşbirliği İfşa Etmiş Ve Dijital Alanda Mahremiyet Konularının Korunmasının Önemine Dikkat Çekmiştir. "Edward Snowden, Whistle-Blower", New York Times, erişim 13 Mayıs, 2022, https://2u.pw/R2dzx.

Mahremiyet konusundaki yaygın sorunlardan biri verilerin internet ve iletişim hizmetleri sağlayıcıları tarafından tutulması ve yetkilerinin sınırlanmamış olmasıdır.[78] Örneğin; Mısır Bilişim Suçlarıyla Mücadele Yasası'nın 2. maddesi, çok boyutlu gözetime izin vermenin yanı sıra kişisel verileri saklama ve izleme işlemlerini güvence altına alarak dijital iletişimi kapsamlı bir şekilde izlenmesini kolaylaştırmıştır. Bu bağlamda 2. madde, telekomünikasyon şirketlerinin kullanıcıların verilerini 180 gün boyunca saklamasını ve depolamasını zorunlu kılmaktadır.[79] Böylece kullanıcıların iletişim içerikleri, bilgisayarın "IP" adresi ve kullandıkları cihazlar hakkında "meta verileri" hizmet sağlayıcıları tarafından depolanmaktadır. Bu durum, internet ve iletişim hizmetleri sağlayıcılarının, sesli aramalar, yazılı mesajlar, site ziyaretleri ve bilgisayarlarda ile akıllı telefonlarda uygulama kullanımı dahil olmak üzere, kullanıcıların dijital iletişimi hakkında ayrıntılı bilgiler yetkililere teslim etmeleri gerekebileceği anlamına gelmektedir.[80]

Bununla birlikte aynı madde, yukarıda dile getirilen verilerin yanında telekomünikasyon şirketlerinin "Ulusal Telekomünikasyon Düzenleme Kurumu'nun (NTRA) yönetim kurulu tarafından diğer veri listeleri ile ilgili alınan kararlara uymasını" gerektirmektedir. Başka bir deyişle bu durum, şirketlerin yasada toplaması ve depolanması öngörülmeyen verileri NTRA'nın kararı ile toplamak ve depolamak zorunda kalabileceğine işaret etmektedir. Benzer bir şekilde, Ürdün'deki telekomünikasyon şirketleri ile devlet kurumları arasındaki bilgi paylaşımı politikaları hakkında çok az bilgi bulunmaktadır.[81] Ancak 2010 yılında Ürdün mevzuatına vatandaşların mahremiyet haklarına tehdit oluşturan yeni düzenlemeler getirilmiştir. Örneğin; internet kafeleri kullanıcıları izlemek için kameralar kurmak zorunda kalmakla birlikte kullanıcılar, interneti kullanmadan önce kişisel kimlik bilgilerini vermeleri

[78] Law No.175 of 2018, Anti-Cyber and Information Technology Crimes Law, Egypt: Official Journal, erişim 11 Ekim, 2021, https://2u.pw/fXiQW.
[79] Egypt: Official Journal, a.g.e.
[80] Egypt: Official Journal, a.g.e.
[81] "Taelimat Mueadala Litaelimat Tanzim Eamal Marakiz Wamaqahi Alaintirnit Wa'usus Tarkhisiha" (TR: İnternet Merkezleri Ve Kafelerinin Çalışmalarını Ve Ruhsat Verme Esaslarını Düzenleme Yönergesi Değiştirilmiştir), Al-Dustour Gazetesi, erişim 13 Mayıs, 2022, https://2u.pw/1eU1q.

gerekmekte ve kafe sahipleri, kullanıcıların tarama geçmişini en az altı ay tutmak mecburiyetinde kalmaktadır.[82]

Mısır'ın düzenlemelerine dönüldüğünde 2. madde, milli güvenlik yetkililerine kişisel verilere erişim hakkı vermekle birlikte internet ve iletişim hizmetleri sağlayıcılarının bu erişimi kolaylaştırmak için gerekli teknik yardımı sağlamakla yükümlü tutmaktadır. Zira yasaya göre "hizmet sağlayıcıları ve çalışanları, milli güvenlik makamlarının talebi üzerine ve ihtiyaçları doğrultusunda, yetkilerini yasaya uygun olarak kullanmalarına imkân verecek tüm teknik yardımları sağlamakla yükümlüdür" hükmünü içermektedir. Başka bir deyişle yasa, iletişimin izlenmesini belirli bir süre için ve belirli suçları soruşturan kurumlardan alınan izinlere bağlamak yerine güvenlik kurumlarına, kısıtlama veya belirli kriter getirmeksizin kullanıcı verilerini elde etme konusunda geniş yetkiler vermektedir. Aslında bu madde, Mısır Anayasası'nın iletişim araçlarının belirli bir yargı kararı ve belirli bir süre olmaksızın izlenmesini yasaklayan hükümlerine aykırı olup ihlal etmektedir.

Zira, Mısır Anayasa'nın 57. Maddesi, "Mahremiyet hakkı ihlal edilemez, korunması ve tecavüz edilmemesi gerekmektedir" hükmünü içermektedir. Ayrıca aynı anayasa maddesi, "Devlet, vatandaşlarının her türlü kitle iletişim araçlarını kullanma hakkını korumakta ve bu iletişim araçları kesilemez, kapatılamaz veya vatandaşları bunları kullanmaktan keyfi olarak mahrum bırakılamaz. Bahsi geçen durumlar ancak yasayla düzenlenebilmektedir" hükümlerini da dile getirmiştir. Kamu ve özel kurum ve kuruluşlarının, kullanıcıların kişisel verilerini bilgisi ve onayı dışında kullandığı birçok vaka gözlemlenmiş ve bunun sonucunda vatandaşların kişisel e-posta ve sosyal medya hesaplarının hacklendiğini görülmüştür. Böylece Mısırlılar, normal günlük uygulamalarında kişisel verilerini ifşa etmek zorunda kalarak mahremiyet hakları ihlal edilmektedir.[83]

İnternet kullanıcılarının çoğu, internetteki faaliyetleri hakkında kapsamlı bir profilini oluşturmak için çevrimiçi tarama etkinliklerinin ve dijital alışkanlıklarının kaydedildiğini bilmemektedir. Ayrıca bu profil, internet kullanıcılarının dijital kişisel kaydı olarak

[82] Al-Dustour Gazetesi, a.g.e.
[83] Ben-Hassine, a.g.e.

bilinmektedir. Örneğin; kullanıcı bir arama yaparken arama anahtar sözcüğü, aramanın tarih ve saati, İnternet Protokolü (IP) adresi, site ziyaretinin saati ve tarihi ve kullanıcının sayfaya ulaşmak için kullandığı arama motoru bilgileri gibi veriler takip edilebilmekte ve aynı zamanda gönderilen ve alınan bilgiler, aynı zamanda kullanıcının e-posta adresi görünmesi mümkündür. Böylece bu değerli bilgiler ele geçirilip daha sonra çeşitli amaçlarla üçüncü şahıslara da satılabilmektedir.[84]

Bu tür bilgilerin korunmaması, dış gözlemcilerin çevrimiçi hesapları ele geçirmesine, bunların kimliklerini istismar etmesine ve kullanıcıyı kimlik hırsızlığına maruz bırakmasına neden olabilmektedir. İnternet siteleri, kullanıcı bilgilerini kullanıcıları tanımak, reklam eğilimlerini belirlemek ve içerik sunmak için depolamaktadır. Ancak asıl sorun şu ki, internet sitelerinin büyük bir kısmı kullanıcıların mahremiyeti ile ilgili bilgilendirme yapmamasıdır. Bu bağlamda son zamanlarda e-ticaret ve internet reklamcılığı sektörlerinin özdenetimi çerçevesinde, kullanıcının verilerini kullanmadan önce bilgilendirmeye bu kullanımı kabul etme ve reddetme seçeneği sunmaya yönelik bir eğilim oluşmaya başladığını söylemek mümkündür. Hükümetler, zamanla yasal yetki veya kamuya açıklama olmaksızın geniş çaplı gözetim yapmak için daha büyük bir kapasite geliştirmiştir. İhlaller, mahremiyet hakkını zayıflatmak için farklı şekillerde olması mümkündür.

Örneğin; hükümetler, veri bankaları kurma girişimlerinin yanında bilgi teknolojisi sistemleri kullanılarak vatandaşların DNA, parmak izleri ve iris taraması gibi ulusal veri tabanlarının oluşturulması, işlenmesi ve saklanması aracılığıyla vatandaşların kişisel verilerini doğrudan toplamaktadır. Bu anlamda hükümetin iletişim faaliyetlerini izlemesi ve vatandaşların çevrimiçi davranışları hakkında devasa bilgi bankalarının toplanması gibi politikalar halkı kapsamlı bir gözetim altında tutulmasına yol açmıştır. Bu koşullar altında, hükümetin milli güvenliği sağlamak adına hükümetler mahremiyet hakkı tamamen ihlal edilmek üzeredir.[85] Bununla birlikte devlet veri tabanlarının bile sürekli olarak bilgisayar korsanlığına ve siber

[84] Nihad Hassan ve Rami Hijazi, *Digital Privacy and Security Using Windows: A Practical Guide*, 1.b., New York: Apress, 2017, s.6.
[85] Kuznetsova ve Bondarenko, a.g.m., s.80.

saldırılara maruz kalması nedeniyle vatandaşların kişisel verileri üçünce taraflardan da ele geçirilerek mahremiyetleri tehdit edilmektedir.

Bütün bunlar sadece mahremiyet hakkının sınırları tehdit edilmekle kalmayıp hakkın içeriğini daraltmakta ve bireylerin dijital arama ve davranış kalıplarını olumsuz bir şekilde etkilemektedir.[86] Aynı zamanda sosyal medya siteleri, kullanıcıların kendileri hakkında paylaşılanları kontrol ettiğini iddia etmesine rağmen gerçekte kullanıcılar, kendileri hakkında gizlice paylaşılanların yanı sıra başkaları tarafından çıkarılabilen bilgi ve meta veriler üzerinde hiçbir kontrol yetkisi bulunmamaktadır.[87] Zira şirketler, veri otomasyonu yoluyla toplanan verilere dayanarak kullanıcılar üzerinde gözetim faaliyetlerinde bulunabilmektedir. Böylece bireylerin uzun vadede mahremiyetini ihlal etmektedir. Bu alandaki skandallardan biri, 40 milyondan fazla kullanıcının verilerini kötüye kullanan Facebook şirketi ve Cambridge Analytica araştırmacılarını kapsamaktadır. Cambridge Analytica araştırmacılarının kullandığı veri toplama taktiği, Facebook şirketinin ara bağlantı ve veri dağıtımını sağlayan uygulama ara yüzünü kullanmıştır. Oysa Facebook, övündüğü bu sistemin dijital seçeneklerin paylaşıldığı ayrı bir web ağı oluşturduğunu iddia etmiştir.[88] Bu durum, internet ve iletişim hizmetleri sağlayıcılarının topladığı kullanıcı verilerini hizmetlerini pazarlamaktan sorumlu aracılara ve distribütörlere aktarma meşruiyetini tartışma haline getirmiştir.

Web sitelerinde ve sosyal medya platformlarında kullanıcılara sunulan kullanım koşulları, yasal düzenlemelerin önünde bir engel teşkil etmektedir. Bu bağlamda mahkemeler, sosyal medya platformlarında paylaşılan ve açığa çıkan kişisel bilgilerin kamu hukukuna, idari düzenlemelere ve yasalara tabi olup olmadığı ve ne dereceye kadar tabi olabildiği konularını belirlemeye çalışmıştır. Ancak çoğu zamanlarda kişisel dijital mahremiyet, siteye, uygulamaya veya platforma göre farklılaşan kullanım koşullarına tabidir. ABD'nin yaşadığı meşhur bir davada hükümet, davalının suç işlemek için kullandığı iddia edilen bir e-postadan

[86] Kuznetsova ve Bondarenko a.g.m., s.78.
[87] "Facebook Privacy Policy", Facebook, erişim 12 Mayıs, 2022, https://2u.pw/t0S4Y.
[88] Tyler Bettilyon, "Why Good Digital Privacy Legislation Is So Hard to Get Right", OneZero, erişim 14 Şubat, 2022, https://2u.pw/z7orB.

kişisel bilgiler elde etmeye çalışmış ve söz konusu bilgiler, kullanıcının kişisel bilgilerinin yasal sürece uymak için açıklanabileceğini gerektiren ve kişinin daha önce kabul etiği e-posta hizmet şartlarını onaylaması nedeniyle ele geçirilmiştir. Bu durumlarda, kullanıcının söz konusu e-posta hizmet sözleşmesi hükümlerine bilerek onayladığını yoksa baştan okumadığını belirlemek zordur.

Bazı görüşler, internet üzerinden kişisel bilgilerini ve sırlarını ifşa eden kişilerin kendi mahremiyetlerine değer vermediği gerekçesiyle mahremiyet hakkından otomatik olarak feragat ettiğini iddiasını ileri sürmektedir. Ancak özel bilgilerin dijital ortamlarda paylaşmanın mahremiyet hakkının ortadan kalktığı anlamına hiçbir şekilde gelmemektedir. Zira yasal mevzuat, bireylerin kendi kendini ifşa ettikleri senaryolarında bile dijital mahremiyeti korumak için teknolojik gelişmelere ayak uydurarak yakalaması gerekmektedir. Ayrıca özel bilgilerin ifşa edilmesinden kaynaklanan zararlar, geleneksel anlamda "ifşa zararları" adı altında utanç verici özel sırların kamuya açıklanmasından kaynaklanan zararlar olarak ele alınmaktadır. Bu geleneksel anlayış, "mahremiyet beklentilerinin ne zaman makul olduğu ve ABD Anayasası'nın İlk Değişikliği'nin dile getirdiği endişelerinin ne zaman geçerli olduğu olayları belirlenmesini" zorlaştırmaktadır. Bu anlamda söz konusu geleneksel anlayış, sosyal medya platformlarında meydana gelen mahremiyet ihlallerine karşı büyük ölçüde etkisiz kalmaktadır.

Ayrıca bu geleneksel anlayış, hakimlerin makul mahremiyet beklentilerine ilişkin öznel kararlar vermesini gerektirmekle birlikte kamuya açık bilgiler karşısında özel bilgiler kavramını kişisel olarak yorumlanmasına izin vermektedir. Bu anlamda bahsi geçen geleneksel anlayış, " kişinin kendi özel bilgilerini internet üzerinden paylaşmasının sosyal medyanın yarattığı sorunun doğasında bulunduğunu" ileri sürerek kişinin paylaştığı özel bilgileri korumayı reddetmektedir. Mahremiyet beklentisine eşlik eden kişisel bilgilerin yaygın bir şekilde paylaşılması sorunlu bir durum teşkil etmektedir. Zira mahkemeler, kişinin kendi elleriyle internet üzerinden paylaştığı bilgilerin özel bilgiler sayılıp sayılmadığını, her ne kadar bu şekilde olsa da durumun özel olabildiğini belirlemekte zorlanmışlardır. Ayrıca çeşitli hukuk profesörleri ve mahremiyet hukuku uzmanları, tüm kullanıcıların uzun hizmet

şartlarını veya üzerinde anlaşmaya varılan kullanım şartlarını okuduğunu; bu özel şartların geçekte uygulandığını varsaymanın haksız olduğunu ileri sürmüşlerdir.[89]

3. Yasaların Dijital Mahremiyet Hakkına Tanınan Anayasal Güvencelerle Uyumluluğu

İnternet, hiçbir coğrafi sınır tanımadığından dolayı dijital mahremiyet yasalarının dünya çapında uyumlu olması gerekmektedir. Zira internet, sadece yerleşmiş kamu ile özel anlayışlarına değil, aynı zamanda yalnızca kişisel mülkiyeti kapsayan eski mahremiyet yasalarına ve sosyal medyayı kapsamayan yetersiz geleneksel mahremiyet ihlali anlayışlarına ciddi bir şekilde meydan okumuştur. Bu bağlamda dünya genelinde artan dijital mahremiyet ihlalleri daha görünür hale geldikçe mevcut yasalar, bu hakkı korumak için ne yazık ki yeterli olmamıştır. Bu bağlamda hukukçular ve akademisyenler, evrensel ve genel bir çıkar haline gelen dijital mahremiyeti korumak için anayasal bir dijital mahremiyet hakkını savunmaktadır. Zira ciddi bir yasal yükümlülük gerektiren mahremiyetin korunması ancak anayasal bir hak olması ile sağlanabilmektedir. Ayrıca anayasal hakkın bazı ülkelerde zayıf bir hak olması mümkündür. Örneğin, anayasalarında açıkça mahremiyet hakkını savunan bazı ülkelerin bile mahremiyet için çok az koruma sağladığı görülmektedir. Bu alanda anayasal bir hak ihtiyacı göz önüne alındığında çok az ülke, dijital mahremiyete ilişkin anayasal hakları özel aktörlere uygulayarak daha fazla korumaya yönelik adımlar atmıştır.[90]

Böylece dijital mahremiyet yasaları ve özellikle bu alana yönelik yapılan anayasal değişiklikler, mahremiyet hakkının internet, sosyal medya ve diğer ilgili dijital platformlarla olan ilişkisi açısından ele alması gerekmektedir. Zira yasalar, ulusal güvenlik endişeleri ile bireyin mahremiyet hakkı arasında denge kurması gerektiği gibi özellikle internet ve sosyal medya tarafından oluşturulan çevrimiçi ortamı incelemesi acil bir elzem haline gelmiştir. Kişisel mahremiyet kavramı, internet ve sosyal medya etkisiyle ciddi bir şekilde değişmiştir. Ancak ne yazık ki yasalar, gelişmiş teknolojiye ayak uyduramamakta ve bireylere dijital platformlarda yeterli koruma sağlamamaktadır. "Mevcut mahremiyet koruma rejimi, kafa

[89] Daxton Stewart, *Social Media and the Law*, 2.b., Londra: Routledge, 2017, ss.50-74.
[90] Hartzog ve Richards, a.g.m., s.1965.

karıştırıcı ile diğer yasalar ve gelişmiş teknoloji ile çelişkili olan bir dizi yasa ve çözüm yolundan oluşmaktadır".[91] Yüksek Mahkeme, mahremiyet ve kişisel özerklik haklarını birbirinden ayrı durumlar olarak ele almaktadır. Ancak ilişkilere ve faaliyetlere ilişkin kamuoyunun değişmesi bu durumun büyük ölçüde sosyal medya ve "paylaşım" atmosferi nedeniyle kişisel mahremiyetin sınırlarının değişmesiyle birlikte mahremiyet hakkının tanımı sürekli değişmesine sebebiyet vermiştir.

Daha önce bahsi geçen kişisel verileri koruma yasaları incelenip anayasalarla, Örneğin; Mısır Anayasası'yla, karşılaştırıldığında yasalar; anayasanın özel hayat ve mahremiyet haklarını koruyan maddelerini ihlal etmiştir. Örneğin; 2018 yılında çıkan Mısır Bilişim Suçlarıyla Mücadele Yasası'nın 4. maddesi, küresel, bölgesel ve ikili anlaşmalar çerçevesinde yabancı hükümetlerin kişisel verilere erişmesine izin vermektedir.[92] Başka bir deyişle bu yasa, Mısır vatandaşlarının mahremiyet hakkının hem yerel hem de uluslararası ölçekte ihlal edilmesine olanak sağlamaktadır. Ayrıca, söz konusu yasa maddesi, bu tür bilgiler değişimi için herhangi bir şart belirtmediği gibi, saklama süresi veya talep edilen verilerin kullanım kapsamı, kullanım durumunun nasıl işleneceğine ilişkin şartları da detaylandırmamaktadır.[93]

Ayrıca mahremiyeti ve özel hayatı korumakta tek başlarına yetersiz olan anayasa metinleri ve ceza mevzuatı örnekleri arasında de kişisel bilgileri modern teknolojinin tehlikelerinden korumaya amaçlayan Irak yasalarıdır. Örneğin; bu alanı ele alan Irak Ceza Yasası'nın 438. maddesi, çağımızın şartlarına göre özel hayatı korumak için yeterli olmamakta ve artan bilişim suçları ışığında Irak'ta mahremiyeti koruyan özel bir yasa bulunmamaktadır. Ayrıca Ürdün yasaları, mahremiyeti korumak için yeterli dayanaklar oluşturmamaktadır. Zira, Ürdün Ceza Yasası'nın 355. ve 356. maddeleri, gelişmiş modern teknolojiler aracılığıyla kişilerin mahremiyet haklarına yapılan ihlal biçimlerini kapsamamaktadır. Sonuç olarak, dünyanın farklı ülkelerinde yasal mevzuat, özel veri ve bilgileri çok etkin bir şekilde koruyamadığından dolayı son dönemlerde siber suçlar her geçen gün artmaktadır.

---

[91] Hartzog ve Richards a.g.m., s.1965.
[92] Law No.175 of 2018, Anti-Cyber and Information Technology Crimes Law, Egypt: Official Journal, erişim 03 Nisan, 2022, https://2u.pw/fXiQW.
[93] Egypt: Official Journal, a.g.e.

İkinci Bölüm: Filistin ve Ürdün Anayasalarında Dijital Mahremiyet Hakkı

Çalışmamızın birinci bölümde dijital mahremiyet hakkı kavramının ortaya çıkışına yer verdikten sonra, tezin ikinci bölümünde ise dijital mahremiyet konusunun hem Ürdün hem de Filistin anayasalarında yasal ve anayasal olarak ele alınışına değineceğiz. Ürdün ve Filistin mevzuatında öngörülen dijital mahremiyet hakkının yasal kapsamını ve yasal kapsamın bu hakka sağladığı güvenceleri araştıracağız. Mevzuattaki metinlerin ne kadar açık olduğunu ve dijital mahremiyet hakkıyla ne kadar kesiştiğini ele alacağız. Bununla birlikte Ürdün ve Filistin anayasal sistemlerine ve her iki ülkedeki genel dijitalleştirme politikalarına kısaca değinmekte fayda gördük**.**

A. Ürdün Anayasasında Dijital Mahremiyet Hakkının Ele Alınışı:

1. Ürdün Anayasal Sistemi

Ürdün anayasası, Ocak 1952 tarihinde Ürdün'ün ikinci kralı olan Kral Talal Bin Al Hüseyin döneminde ilan edilmiştir. Anayasanın ilk maddeleri, devletin parlamenter monarşi sistemiyle yönetildiğini ve kuvvetler (yasama, yürütme ve yargı) ayrılığı ilkesinin benimsendiğini öngörmüştür. Ürdün anayasası, 9 bölüm ve 131 maddeden oluşmaktadır. Ürdün anayasası, 1952 yılında ortaya çıkan şekline ulaşana kadar üç aşamadan geçmiştir.[94] İlk anayasa aşaması, "Temel Yasa" adıyla bilinen ve 1928 yılında çıkarılan Ürdün anayasasıyla başlamıştır. Temel Yasa'nın maddeleri, aynı yılda imzalanan İngiliz-Ürdün anlaşmasına dayanılarak hazırlanmış ve İngiliz Mandası tarafından tasarlandığı için Ürdün halkının büyük muhalefetiyle karşılaşmıştır. Bundan sonra özellikle Mavera-i Ürdün Emirliği'nin 1946 yılında bağımsızlığına kavuşarak Kral tahtına çıkan Prens Abdullah tarafından yönetilen Ürdün Haşimi Krallığı'na dönüşmesi gibi çeşitli siyasi gelişmelere ayak uydurmak için ikinci anayasa aşaması 1947 yılında gerçekleşmiştir. Filistin'in Siyonizm tarafından işgali gibi birçok büyük siyasi ve ekonomik gelişmelerden sonra gerçekleştirilen

[94] Mahmoud Al-Anaqrah, "Mahatat Tarikhia: Aldustur Al'urduni" (TR: Tarihi İstasyonlar: Ürdün Anayasası), Al-Dustour Gazetesi, erişim 20 Ağustos, 2021, https://2u.pw/c5ttr.

üçüncü anayasa aşaması ise, Ürdün Kralı Talal döneminde 1952 yılında meydana gelmiştir. Zira çeşitli değişikliklerin yapılmasını gerektiren bu dönem, Ürdün nehrinin iki şeriasının birleşmesi (doğu ve batı) dahil olmak üzere çeşitli kararlar alınmasına tanık olmuştur. Bu dönem, Ürdün'de nüfusun ve kültürel yapının değişmesine ve hatta birçok siyasi partinin kurulmasına yol açan siyasi olaylar yaşanmıştır. Bütün bu gelişmelerin ışığında, Ürdün'ün halen yürürlükte olan anayasası 1952 yılında yeni anayasa olarak kabul edilmiştir[95].

1952 yılında kabul edilen Ürdün anayasası, o dönemde dünyanın en modern anayasalarından biri olarak görülmüştür. Bu anayasa 9 bölümden oluşmaktadır. Bu bölümler şu şekildedir: devlet ve yönetim sistemi, Ürdünlülerin hakları ve görevleri, devletin erkleri (yürütme, yasama ve yargı), mali işler, genel maddeler ve yasaların yürürlüğe girmesi ile yürürlükten kaldırması hakkındaki maddelerdir. Bununla birlikte 1952 Anayasası, kuvvetler ayrılığı ilkesini benimsemek, Ürdün halkının Arap ulusal kimliğini anayasanın ilk maddesinde vurgulamak, iktidarın kaynağı olarak milletin ve halkın egemenliği ilkesini savunmak, irsi monarşi sistemini temel almak ve temsili parlamenter sistemini uygulamak gibi temel özellikleri bulunmaktadır. Bununla birlikte anayasa, güvenlik hakkı, bir yerden başka bir yere serbest dolaşım hakkı, yazışmaların gizliliğine saygı hakkı; ikamet yeri seçme özgürlüğü, mülkiyet özgürlüğü, düşünce özgürlüğü; eğitim hakkı, din özgürlüğü, toplanma özgürlüğü ve dernek ve siyasi parti kurma özgürlüğü gibi Ürdün vatandaşlarının kamu hak ve özgürlüklerini düzenlemektedir.[96]

2011 yılında Arap Baharı devrimlerinin başlamasıyla Ürdün rejimi, anayasal hakların güçlendirilmesine yönelik halk taleplerine uymuştur. Bu bağlamda Kral II. Abdullah, anayasa metinlerini gözden geçiren ve önerilerini Ürdün hükümetine sunan bir komite kurma emrini vermiştir. Bunun sonucunda Anayasa Mahkemesinin inşa edilmesi ve bağımsız bir seçim komisyonunun kurulması öngören maddeler dahil olmak üzere, Ürdünlülerin hak ve

[95] Al-Anaqrah, a.g.e.
[96] Al-Anaqrah, a.g.e.

özgürlükleriyle ilgili olan yaklaşık 38 anayasa maddesi düzeltilmiştir. Ayrıca Ürdünlülerin haklarına, özgürlüklerine ve özel hayatlarının gizliliğine her türlü saldırıyı suç sayan 7. Maddede değişiklik yapılmıştır. Üstelik anayasanın 18. maddesi, iletişim mahremiyetinin tüm iletişim araçlarını kapsayacak ve bu araçlara erişmek, el koymak veya engellemek gibi uygulamalar sadece yargı kararıyla sınırlandırılacak şekilde yeniden düzenlenmiştir.[97] Ancak 2014 ve 2016 yıllarında yeni değişiklikler yapılarak başbakan ve bakanlar kurulu imzası olmadan krala veliaht prensi, kral yardımcısı, Ayan Meclisi'nin başkanı ve üyeleri, Anayasa Mahkemesi başkanı ve üyeleri, ordu komutanı, istihbarat direktörü ve jandarma komutanı gibi makamları tek taraflı atama yetkileri verilmiştir.[98]

2. Ürdün ve Dijital Dönüşüm

1990'lı yılların sonunda Kral II. Abdullah anayasal yetkilerini üstlendiğinden beri Ürdün, bilgi ekonomisini geliştirmeye ve bilgilerin inşasına 2004 yılında başlanan e-devleti kurmaya doğru yönelmiştir. Bu alanda Ürdün; Arap dünyasında bilişim ve iletişim teknolojileri sektörünü geliştiren bir merkez haline gelmeye ve uluslararası pazarlara açık dijital bir ekonomi inşa etmeye dayanan bir vizyon benimsemiştir.[99] Bunun için Ürdün, devlet telekomünikasyon şirketleri dahil olmak üzere resmi devlet kurumlarını özelleştirmeye başlayarak şirketler arasındaki rekabet sonucunda ülkede internetin daha fazla yayılmasına zemin hazırlamıştır.[100] Aynı zamanda Ürdün'deki bu iç gelişmelere dünyanın tüm hükümetlerinin ekonomik anlamda yararlanmaya ve yasal çerçevelerini yeni gelişmelerin dayattığı değişimlere göre düzenlemeye çalıştığı büyük bir teknoloji devrimi eşlik etmiştir.[101]

---

[97] 2011 Yılında Yapılan Tüm Değişikliklerle Birlikte Aldustur Al'urduni (TR: Ürdün Anayasası), erişim 07 Ekim, 2021, https://2u.pw/hp9Uq

[98] "Al'urdun: Taedilat Dusturia Jadida Tujib Salahiaa Lilmalik Minfirida" (TR: Ürdün: Krala Tek Taraflı Yetkiler Veren Yeni Anayasa Değişiklikleri", CNN, erişim 28 Ağustos, 2021, https://2u.pw/ziexB.

[99] "Altatawur Altaarikhi Lihayyat Tanzim Qitae Alaitisalat" (TR: Telekomünikasyon Düzenleme Kurumu'nun Tarihsel Gelişimi), Telekomünikasyon Düzenleme Kurumu, erişim 05 Aralık, 2021, https://2u.pw/fEXoD.

[100] "Khaskhasat Alaitisalat Tajriba Najiha Mahadat Wa'ashimat Fi Rafd Alkhazina" (TR: Telekomünikasyonun Özelleştirilmesi Hazineye Katkı Sağlayan Başarılı Bir Deneyim), Amman Change, erişim 14 Ağustos, 2021, https://2u.pw/Ksb5c.

[101] Ahmed Mansur, *Damanat Alhaqi Fi Hurmat Alhayaa Alkhasa Fi Almawathiq Alduwlia Lihuquq Al'iinsan Walqawanin Alwatania (TR: Uluslararası İnsan Hakları Sözleşmelerinde Ve Ulusal Yasalarda Özel Hayatın Gizliliği Hakkına Sağlanan Güvenceler)*, 3.b., Kahire: Arap İdari Gelişim Kurumu, 2019, s.63.

E-devlet uygulamasının Ürdün'de gördüğü ilgiye rağmen, uygulamanın hazırlık düzeyinde bir kısım tutarsızlık bulunmuştur. Zira, internet yaygınlaşıp daha çok sayıda vatandaşa ulaşırken birbirini takip eden hükümetler, bir taraftan da dijital dönüşüm için gereken kurumsal altyapının geliştirilmesi durumuyla birlikte diğer kullanıcıların verilerini, dijital mahremiyetlerini her türlü sızma ve saldırıdan korumak adına, gerek devlet denetim kurumlarına, gerek iletişim hizmeti sağlayıcılarına gerekse verilere ulaşabilen tüm üçüncü taraflara karşı yasal ve anayasal çerçevelerin düzenlenmesi açısından bahsi geçen vakalara ayak uydurmakta zorlanmıştır. Bu anlamda artan dijital kullanım, süreçteki gelişim gibi durumlarla mevcut düzenleyici politikalar ve kullanıcıların dijital hakları yetersiz kalmıştır. Bu durum, nihayetinde internet kullanıcılarının dijitalleşme hizmetlerinden yararlanma konusunda isteksiz olmalarına ve dijital platformları kullanırken özellikle siyasi örgütlenme, siyasi görüşleri paylaşma söz konusu olduğunda bir tür otosansür uygulamalarına yol açmıştır.[102]

Söz konusu otosansür, 2015 yılında kabul edilen Siber Suçlar Yasası'nın yürürlüğe girmesiyle daha da artmıştır. Bilgi ve Araştırma Merkezi ve 7iber dergisi tarafından hazırlanan bir araştırmaya göre, Ürdünlüler arasında dolaşan "birinin onları dinlediği" şeklindeki gelenekselleşmiş bilgi, vatandaşlar arasında büyük bir yaygınlığa sahiptir.[103] Bu durum, fiziksel mahremiyet ihlalini, dijital alana taşındığının önemli bir göstergesi temsil etmektedir. Bunun ışığında Ürdün'deki dijital mahremiyet haklarına ilişkin artan endişeler anlaşılması mümkündür. Dijital mahremiyet, veri koruma ve iletişimin denetimi gibi konularla ile ilgili yasama politikalarına, süreçlerine ilişkin çok az bağımsız ve açık incelemeler yapılmaktadır. Dahası da Ürdün makamlarının denetim yetkileri ve denetim uygulamaları gibi bir konuya ilişkin sınırlı raporlar bulunmaktadır.[104]

---

[102] Mansur, a.g.e., s.65.
[103] Thoraya Rayyes, *Digital Privacy İn Jordan: Perceptions And Implications Among Human Rights Actors*, 1.b., Amman: Information and Research Center, 2015, ss.8-11.
[104] "Stakeholder Report Universal Periodic Review: The Right To Privacy İn Hashemite Kingdom Of Jordan", Jordan Open Source Association, (2018), ss.4-7, erişim 05 Nisan, 2021, https://2u.pw/Ab70I.

İnternetin sadece vatandaşların mahremiyetiyle ilgili sorunlar yaratacağını bekleyen hükümetler, kullanıcıların kamu meseleleriyle ilgili konularda görüşlerini ifade etmelerine olanak tanıyan ve kontrol edilmesi, sınırlandırılması zor olan internetin oluşturduğu yeni alanlarla ilgili de ciddi sorunlar yaşamaktadır. Örneğin; Arap Baharı olayları, Ürdün dahil olmak üzere Ortadoğu hükümetlerini interneti otoriter bir şekilde düzenlemeye itmiştir. Bu bağlamda yayınlar ve yayıncılık ile Siber Suçlar yasaları gibi web sitelerinin oluşturulmasını belirleyen ve çalışmalarını kısıtlayan yasalar belirlenmiştir. Genel olarak, Ürdün'deki çoğu hukuk uzmanı, dijital alanla ilgili yasaların, aslında kullanıcıları korumaktan çok dijital hakları kısıtlamak için düzenlendiği konusunda hemfikirdir. Hükümetler, bu yasaların şantaj, iftira, hakaret ve karalama gibi kullanıcıları internette karşılaştıkları bazı sorunlardan korumak için düzenlendiğini ileri sürerken hukukçular ise Ceza Yasası gibi diğer temel yasalar aracılığıyla kullanıcıları bu sorunlardan korunabildiğini savunmaktadır.[105]

İstatistikler, Ürdün'deki internet kullanıcı sayısının Ocak 2021'in başına kadar ülkenin toplam nüfusu olan 10,24 milyon vatandaştan yaklaşık 6,84 milyon İnternet kullanıcısına tekabül ettiğini göstermiştir. Böylece nüfusun %66,8'ini oluşturan internet kullanıcı sayısı, 2020'nin başına göre %0,8'lik bir artış kazandığı gibi sosyal medya kullanıcı sayısı da %61,5 yaygınlık oranı ile 6,30 milyon kullanıcıya yükselmiştir. Aynı zamanda toplam aramaların %78,2'sini oluşturan 8,01 milyon cep telefonu araması yapılmıştır.[106] Ayrıca 2020 yılında patlak veren Covid-19 pandemisi, özellikle eğitim, iş ve sosyal iletişim gibi faaliyetlerin internet bağlantısı gerektiren dijital faaliyetlere dönüşmesiyle birlikte internete abonelik ve erişim oranlarını artırmıştır.

İnternetin artan yaygınlığına rağmen, Ürdün'deki genişbant abonelikleri hala düşüktür. Ayrıca Ürdün, "Bilgi ve İletişim Teknolojileri endeksinde" 2019 yılına göre dört sıra

[105] "Takhawufat Min Taqyid Alhuriyaat W Aizdiad Habs Alsahafiiyn Baed Taedilat Qanun Aljarayim Aljadida (TR: Yeni Suçlar Yasasında Yapılan Değişiklikler Sonrası Gazetecilerin Özgürlüklerinin Kısıtlanmasından ve Hapis Cezalarının Artmasından Korkulur", Saraya, erişim 09 Nisan, 2021, https://2u.pw/Gb9yM.
[106] "Digital 2021: Jordan", Data Reportal, erişim 13 Ocak, 2022, https://2u.pw/I2fwr.

gerileyerek 73. sırada gelmiştir. Bununla birlikte Ürdün, Birleşmiş Milletler tarafından geliştirilen e-devlet gelişim endeksinin iletişim altyapısı yan endeksinde dünya bazında 85. sırada yer almıştır. Bu bağlamda Ürdün Stratejiler Forumu, dijital uçurumun azaltılması gerektiği ihtiyacına ilişkin politika yapıcılarına tavsiyeleri iletmiştir. Dijitalleştirme alanında Ürdün'ün 2004-2012 dönemindeki performansı, dünya ortalamasından büyük bir farkla daha iyiydi. Ancak 2012 yılından bu yana, Ürdün'ün e-devlet alanını geliştirmekte yavaşlaması nedeniyle Ürdün ve dünya arasındaki bu fark azalmış ve 2018 yılında dünyanın 193 ülkesi arasında 115. sıraya gelmiştir.[107]

Ancak, birbirini takip eden Ürdün hükümetleri, Kraliyet direktifleri doğrultusunda, e-devlet stratejisi ve dijital dönüşüm için (REACH-2021) girişimini başlatmıştır. Söz konusu strateji, interneti yaymayı, telekomünikasyon sektörünü geliştirmeyi, teknolojik sistemlerin geliştirilmesi ve ihraç edilmesi ile ilgilenen özel sektörü güçlendirmeyi aynı zamanda da teknoloji alanlarında üniversite bölümlerinin iyileştirmeyi amaçlamaktadır. Ürdün'ün Dijital Ekonomi ve Girişimcilik Bakanlığı, dünyadaki dijital dönüşümün ilerlemesine ayak uydurmak adına gerekli stratejik değişiklikleri ve gereksinimleri netleştirmek, kamu hizmetleri sunumunu iyileştirmek tüm bunların yanı sıra hükümet performansını yükseltmek için "Ürdün Dijital Dönüşüm Stratejisini 2020" adlı projesini başlatmıştır. Bu strateji, Ürdün'ün 2025 vizyonundan ve 2030 Sürdürülebilir Kalkınma Hedeflerinden ilham aldığı gibi bu alandaki uluslararası tecrübelere, eğilimlere ve uygulamalara dayanmaktadır. Ayrıca Dijital Ekonomi ve Girişimcilik Bakanlığı, kamuoyu görüşlerini almak adına söz konusu stratejinin taslağını aktivistler ve ilgili taraflarla paylaşmıştır.[108] Ancak bu strateji hakkında Ürdün Açık Kaynak Derneği tarafından yapılan yorumlara göre strateji, dijital kimlik kullanılırken özellikle vatandaşların iris taramaları gibi biyometrik verilerinin kullanımı konusunda ileride ele alınacağı gibi henüz hassas kişisel verileri korumayı göz önünde bulundurmamaktadır. Ayrıca kişisel verilerin korunmasına ilişkin yasa tasarısı, hangi kişisel

[107] "Alhukumat Al'iilikturuniat Fi Al'urdun: Nazrat Lisaniei Alsiyasat" (TR: Ürdün'de E-Devlet: Politika Yapıcılara Bir Bakış), Ürdün Stratejiler Forumu, erişim 02 Haziran, 2021, https://2u.pw/deWax.
[108] "Aliastiratijiat Al'urduniya Liltahawul Alraqmii 2020" (TR: Ürdün Dijital Dönüşüm Stratejisi 2020), Dijital Ekonomi ve Girişimcilik Bakanlığı, erişim 02 Haziran, 2021, https://2u.pw/VYLte.

verilerin hassas kabul edildiğini ve hangilerinin daha fazla korumaya ihtiyaç duyduğunu belirtmemektedir. Bu durum, hükümetin biyometrik verilere dayalı herhangi bir dijital kimlik uygulamasını etkinleştirmesine güvenmeyi reddetmek ve bu veriler toplanmadan vatandaşların dijital kimlikten faydalanması için alternatif mekanizmalar sağlamak gibi bir yasal tavsiye gerektirmektedir.[109]

3. Ürdün Anayasasında Dijital Mahremiyet Hakkının Anayasal Ele Alınışı

Daha önce belirttiğimiz gibi, dünyadaki çoğu anayasalar, dijital mahremiyet hakkının korunmasına tam anlamıyla açık ve net bir yer vermemiştir. Ürdün anayasası da bu türden bir anayasadır. Bu anlamda Ürdün anayasasında, dijital mahremiyet hakkını bugün bildiğimiz şekliyle ve dijital gelişme yıllarında sağlanması gereken korumanın kapsamı genişlediği haliyle ele alan hiçbir madde bulunmamaktadır. Köken ve mahiyet itibariyle dijital mahremiyet hakkı ile özel hayat hakkının tek bir doğaya sahip olduğundan, aynı varlığı korumayı amaçladıklarından dolayı bu durum, bizi anayasalarda mahremiyet hakkını veya özel hayat hakkını korumaya yönelik düzenlenen maddeleri aynı zamanda dijital mahremiyet hakkını korumak için kullanma seçeneğine itmektedir. Ancak önceden de belirttiğimiz gibi özel hayat hakkı insanın fiziksel varlığını korumaya odaklanırken dijital mahremiyet hakkı, insanın manevi varlığını koruma eğiliminde olmuştur.[110]

Dolayısıyla Ürdün anayasa koyucusu, anayasada birden fazla yerde mahremiyet ve özel hayata saygı hakları ile ilgili bazı hususları ele alarak geleneksel anlamda mahremiyet hakkına özel hayatın gizliliğine önem verdiğini söylenebilmektedir. Böylece Ürdün anayasası, özel hayatın ve mahremiyetin korunacağına dair güvenceler vererek anayasanın üstünlüğü ilkesine dayanarak bu hakların ihlal edilmesi ve sınırlandırılması hukuka aykırı olduğu anlayışını vurgulamıştır. Bu bağlamda Ürdün anayasasının 7. ve 18. maddeleri, mahremiyet konusunu düzenleyen en önemli maddelerden bazıları sayıldığı gibi konut dokunulmazlığını düzenleyen 10. madde, konutların "Ancak yasada belirtilen hallerde ve

---

[109] "Taeliqat Wamulahazat Ela Aliastiratijiat Al'urduniya Liltahawul Alraqmii 2020" (TR: Ürdün Dijital Dönüşüm Stratejisi 2020 Üzerine Yorumlar Ve Notlar), Ürdün Açık Kaynak Derneği, s.13, erişim 11 Haziran, 2021, https://2u.pw/CEzGo.

[110] Rayyes, a.g.e., s.41.

yasada öngörülen şekilde girilir" olduğunu savunarak konutların kutsal mahremiyeti olduğunun altını çizmiştir. Ürdün anayasasının 7. maddesine gelince, özel hayatın gizliliğine her türlü saldırıyı suç saymanın yanı sıra "kişisel özgürlüğün güvence altına alındığını aynı zamanda Ürdünlülerin haklarına, kamu özgürlüklerine veya özel hayatlarının gizliliğine yönelik her türlü saldırının kanunen cezalandırılan bir suç olduğunu" öngörmektedir.

Bahsi geçen bu durumlardan yola çıkarak anayasa metni, söz konusu saldırının örneğin; hükümet, bireyler, özel şirketler veya basın gibi tüzel kişiler tarafından gerçekleştirilen, tarafı belirlemeden kesin bir şekilde genel bir şekilde düzenlenen bunun sonucunda da özel hayatın, kişisel özgürlükle birleştirdiğini not etmek mümkündür. Bu madde, uluslararası insan hakları standartlarına uymasına rağmen özel hayat kavramı, konut ve özel mülkiyet gibi genellikle fiziksel konularla ilgilenmektedir. Bunun aksine mahremiyet hakkı, hukuk literatüründe genellikle zaman, mekân ve bir manevi varlık olarak kişiyle ilgili mahremiyet anlayışlarını birleştirmektedir. Bununla birlikte anayasanın 18. maddesi, yazışma ve arama özgürlüğü üzerinde herhangi bir kısıtlama uygulanamayacağını ve telefon görüşmelerinin yasa hükümlerine uygun olarak yargı kararı olmadıkça engellenemeyeceğini, toplanamayacağını ve görüntülenemeyeceğini vurgulamıştır.[111] Söz konusu madde, "Her türlü posta ve telgraf yazışmaları, telefon görüşmeleri ve diğer iletişim araçlarının kullanımı gizli kabul edildiğini ve yasa hükümlerine uygun bir yargı kararı olmaksızın denetlenmeye, erişilmeye, el koyulmaya veya engellenmeye tabi olmadığını" açıklamıştır.[112]

Bu madde, özellikle 2014 yılında yapılan değişikliklerden sonra anayasada mahremiyet hakkını ele alan en önemli metinlerden biri haline gelmiştir. Zira bu madde, önceden idari emirlere de açık olduğu halde her türlü iletişim aracını denetleme, el koyma veya dinleme uygulamalarını sadece yargı kararı ile sınırlandırmıştır. Bu değişikliklerin önemine rağmen anayasa metni, özellikle sosyal medya sitelerinin yayılmasıyla daha yaygın hale gelen

[111] Maria Bojdin, "Min Alhaqi Fi Alhayaat Alkhasat 'İilaa Alhaqi Fi Alkhususiat Alraqamia" (TR: Özel Hayat Hakkından Dijital Mahremiyet Hakkına). *Anayasa Hukuku ve İdari Bilimler Dergisi: Berlin*, 2/3 (2019), s.57.
[112] Aldustur Al'urduni (TR: Ürdün Anayasası), erişim 07 Ekim, 2021, https://2u.pw/hp9Uq.

elektronik ve dijital iletişimleri açıkça içermemiştir. Ayrıca son dönemlerde yaygınlaşan sosyal medya siteleri aracılığıyla gerek konuşmaları dinleyerek ve denetleyerek gerekse konuşmaların kayıtlarını ifşa ederek, bu platformlarda mahremiyet hakkı genellikle ihlal edildiği görülmektedir.[113]

Yukarıda belirtilen maddeler ışığında Ürdünlü yasa koyucu; telefon iletişimi ve posta yazışması gibi bazı mahremiyet hakkı örneklerine yer vermiştir. Bununla birlikte yasa koyucu, modern elektronik iletişim araçlarından doğrudan bahsetmeyi ihmal etmesine rağmen bağlı kılındığı metne, sosyal medya platformları üzerinden yapılan iletişime uygulanabilecek "diğer iletişim araçları" ifadesini eklemiştir. Dijital mahremiyet hakkı kavramı nispeten yeni olması ve sınırları Ürdün için hala belli olmaması gibi nedenlerle anayasada doğrudan bahsedilmemiş olabilir ancak bu tezin yazıldığı tarihe kadar dijital mahremiyet hakkını herhangi bir yasa veya mevzuatta ele alınmaması bu hakka karşı anayasal ihlallerine kapı aralamaktadır. Bu durumda mahremiyet hakkı, yalnızca konuşmalar denetlendiğinde değil, aynı zamanda dijital işlemlerin sağladığı büyük verileri hacklanmaya ve temel ile anayasal hakları ihlal edecek bir şekilde amaçları dışında kullanılmaya karşı herhangi bir koruma garantisi verilmediğinde de ihlal edilebilmektedir.[114]

Uluslararası yükümlülüklere gelince Ürdün, İnsan Hakları Evrensel Beyannamesi'ni bununla birlikte Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'yi onaylamıştır. Bunları onaylandıktan sonra uluslararası anlaşmalar, devlette yasama kaynaklarından biri olarak kabul edildiği gibi bunların hükümleri olağan yasalardan daha öncelikli değerlendirmekte ve devlet ile kamu makamları bunlara uymak ve saygı göstermekle yükümlü olmaktadır. Ürdün Yargıtayı'nın bir davada verdiği bir karara göre "... ikili veya uluslararası anlaşmalar bağlayıcı kabul edilir ve uygulanmalıdır ve çelişmeleri halinde uygulamada iç hukuktan daha

[113] Rayyes, a.g.e., s.43.
[114] Rayyes, a.g.e., s.45.

yüksektir ...” diye bir hüküm vermiştir.[115] Ayrıca Ürdün, 1990 yılında Çocuk Haklarına Dair Sözleşme'yi de onaylamıştır. Bütün bu anlaşmalar mahremiyet hakkını açık bir şekilde desteklemektedir.[116] Aynı şekilde Ürdün, mahremiyet hakkını destekleyen İslam'da İnsan Hakları Kahire Bildirgesi'ni Ağustos 1990 tarihinde imzalamıştır.[117] Bununla birlikte Ürdün, maddelerinden birinde her bireyin kendi özel hayatına ve iletişimine keyfi müdahalelerden yasalarla korunmasını öngören Arap İnsan Hakları Sözleşmesi'ne katılmıştır.[118]

B. Filistin Anayasasında Dijital Mahremiyet Hakkının Anayasal ve Yasal Ele Alınışı

1. Filistin Anayasal Sistemi

Filistin'de hâkim siyasi koşullar nedeniyle Filistinliler, Osmanlı döneminden beri kendi kendilerini yönetme fırsatına sahip olmamışlardır. Osmanlı Filistin dönemde yürürlükte olan hukuk sistemi, Osmanlı İmparatorluğu'nun yasaları ve anayasalarıdır. Birinci Dünya Savaşı'ndan sonra Filistin, İngiliz Mandası altında düşmüştür. Manda yönetimi, yasal bir değişim sürecine başlatarak 1922 Filistin Anayasası'nı çıkarmıştır. 1948 yılında İngiliz Mandasının sona ermesinden sonra ve Nakba (Felaket) Savaşı'nın bir sonucu olarak Filistin, her biri farklı bir siyasi sistem tarafından kontrol edilen üç siyasi bölgeye bölünmüştür. Bu durum, bugüne kadar görülebilecek bir şekilde Filistin'deki hukuk sistemine yansımıştır.[119] Bir yandan işgalci Siyonist güçleri Filistin topraklarının %78,5'i üzerinde “İsrail Devleti”ni kurulduğunu duyurmuştur. Diğer yandan Ürdün, 1949 yılında Doğu Kudüs ve Batı Şeria topraklarını Ürdün egemenliğine ilhak ederek Ürdün yönetiminde Ürdün nehrinin iki şeriasının birliğini ilan etmiştir. Bu bağlamda 1952 yılında Filistinli üyelerin de yer aldığı

---

[115] Nofan Al-Ajarma, “Alhaqu Bihimayat Alkhususiat Fi Daw' Taedil Almada (23) Min Qanun Mukafahat Alfasad” (TR: Yolsuzlukla Mücadele Yasasının (23) Maddesinde Yapılan Değişiklik Işığında Mahremiyet Hakkının Korunması), Ammon Haber Ajansı, erişim 02 Nisan, 2021, https://2u.pw/QPCUm.

[116] “Stakeholder Report Universal Periodic Review: The Right To Privacy İn Hashemite Kingdom Of Jordan”, Jordan Open Source Association, (2018), s.6, erişim 05 Nisan, 2021, https://2u.pw/Ab70I.

[117] “Qarar Alearab Bialmusadaqat Ealaa Almithaq Alearabii Lihuquq Al'iinsan” (TR: Arapların Kararı Arap İnsan Hakları Sözleşmesini Onaylamaktır), Al Jazeera Net, erişim 22 Ocak, 2022, https://2u.pw/2CRD7.

[118] Arab Charter On Human Rights, erişim için: http://hrlibrary.umn.edu/instree/loas2005.html.

[119] Yasemin Khamis ve Asım Khalil, “Waqie Alnizam Aldusturii Watatawuruh: Murajaeat li'ahami Al'ahdath Walqararat Aldusturia Khilal Aleam 2018” (TR: Anayasal Sistemin Gerçekliği Ve Gelişimi: 2018 Yılındaki En Önemli Anayasal Olay Ve Kararların Gözden Geçirilmesi), *Birzeit Hukuk Çalışmaları Serisi*, 5/11 (2019), s.3.

Ürdün meclisi, yeni siyasi koşulları dikkate alan ve Batı Şeria ile Doğu Kudüs'ün Ürdün Haşimi Krallığı'na ilhakını düzenleyen bir anayasa kabul etmiştir. Böylece söz konusu Ürdün Anayasası, İngiliz Mandasının 1922 yılında Filistin'de uyguladığı anayasanın yerini almıştır. İngiliz Mandası tarafından kurulan Filistin anayasası. Gazze Şeridi'ne gelince ise, Mısır'dan ayrı kalmasına rağmen Mısır yönetimine girmiştir. Ayrıca Mısır hükümeti, 1955 yılında Gazze'nin Temel Yasasını kabul etmiş ve aynı zamanda Filistin'in 1922 manda anayasasını sürdürmüştür.[120]

Daha sonra1988 yılında Ürdün nehrinin iki şeriasının idari ve siyasi ayrılmasından sonra Filistin Kurtuluş Örgütü, Cezayir'de yapılan Filistin Ulusal Konseyi'nin bir konferansında bağımsızlık ilanını onaylamıştır. Bu durumdan hareketle yeni anayasa hazırlama fikrini önermiştir. Ancak gerçek anayasa hazırlama projeleri, İsrail işgal hükümeti ile Filistin Kurtuluş Örgütü arasında 1993 yılında imzalanan Oslo anlaşmasından sonra başlamıştır. Oslo Anlaşmasına göre Filistin Yönetimi, Batı Şeria ve Gazze Şeridi topraklarını yöneten idari ve yasal bir organ olarak kurulmuştur. Filistin Yasama Meclisi'nin Filistin Temel Yasası'nı 1997 yılında geçiş dönemi için geçici bir anayasal belge olarak kabul etmeye karar vermesine rağmen söz konusu belge, 2002 yılına kadar onaylanmamıştır. Filistin Temel Yasası, siyasi rejime başbakanlık makamını oluşturmaya ilişkin 2003 değişikliği her dört yılda bir yasama meclisi ve cumhurbaşkanlığı seçimlerinin yapılmasına ilişkin 2005 değişikliği gibi birçok değişiklik geçirmiştir.[121]

Şüphesiz ki İsrail işgal rejiminin Filistin toprakları üzerindeki kontrolünün Filistin'deki yasal sistemin statüsünü diğer ülkelere göre farklı kılmıştır. Örneğin Filistin, anayasadan bahsedilirken siyasi koşulların yasal bakışlarla açıkça karıştığı bir yerdir. Zira 1999 yılında Oslo Anlaşmasının geçiş döneminin sona ermesiyle birlikte sahadaki fiili gerçek

[120] Asım Khalil, "Eamaliat Tahdir Aldustur Alfilastinii Watariqat Tabaniyh: Limadha Kayfi? Walimadha Alan?" (TR: Filistin anayasasını hazırlama ve kabul etme süreci: neden nasıl ve neden şimdi?), *Dirasat*, 36/2 (2009), ss.223-242.
[121] Khalil, a.g.m., s.230.

değişmemiştir. Batı Şeria'da Yahudi yerleşim birimlerinin inşaatları devam etmekte ve Filistin köylerini ve şehirlerini ayıran ayrım duvarı gerçek bir Filistin devletinin ortaya çıkmasını fiili olarak engellemektedir.[122]

Öte yandan, 2001 yılında ilk tasarısını tamamlayan Filistin devletine anayasa tasarısı hazırlamak göreviyle 1999 yılında bir anayasa komitesi atanmış, ancak bu komisyonun işiyle ilgilenen olmamıştır. 2012 yılında Birleşmiş Milletler Genel Kurulu Filistin'i üye olmayan gözlemci bir devlet olarak tanımış ve Filistin Yönetimi resmî belgelerde kendisini "Filistin Devleti" olarak adlandırmaya başlamıştır. Aynı zamanda Filistin Temel Yasası, geçiş döneminin sona ermesinden sonra Filistin devletinin yeni anayasanın yürürlüğe girmesine kadar çalışmalarını uzatma olasılığını öngören yasanın 115. maddesine dayanarak işlemeye devam etmiştir. Anayasa Komisyonu 273 maddelik bir anayasa tasarısını hazırlayarak 2015 yılında tamamlamış ancak bu tezin yazıldığı tarihe kadar söz konusu anayasa tasarısı onaylanmamıştır.[123]

2. Filistin'de Mahremiyet: Çifte Standartlı Yasal Süreç

Filistin'de mahremiyet hakkı konularını tartışmak kolay değildir. Zira bu konu, diğer ülkeler bağlamında olduğundan daha karmaşık görünmektedir. Filistinlileri yöneten birçok otorite bulunmakta ve onlar için geçerli olan yasal sistemler farklılaşmaktadır. Örneğin; Filistin toprakları veya 1967 toprakları adlı bölgeleri (Batı Şeria, Doğu Kudüs ve Gazze Şeridi), 1967 yılından beri İsrail işgali altında yaşamakta ve buralardaki Filistin nüfusu birden fazla yasal sisteme tabi tutulmaktadır.[124] Zira bu bölgeler, Doğu Kudüs ve Yahudi yerleşimciler için İsrail medeni yasası uygulandığı gibi Batı Şeria'da Ürdün medeni yasası, İsrail askeri yasası ve Filistin Yönetimi tarafından çıkarılan kararnameler uygulanmaktadır. Gazze Şeridi'ne

[122] Aziz Kaed, "Qara'a Fi Mashrue Aldustur Alfilastinii Almuaqat" (TR: Geçici Filistin Anayasası Taslağı Üzerinde Bir İnceleme*), Filistin Bağımsız Vatandaş Hakları Komisyonu*, *Yasa Geliştirme Projesi Serisi*, 17/9 (2000), s.67.
[123] Khamis ve Khalil, a.g.m., s.6.
[124] Kaed, a.g.m., s.61.

gelinde ise, Mısır medeni yasası ve Gazze'deki hükümetin talimatları kullanılmaktadır. Bunlara ek olarak İsrail ile Filistin Yönetimi arasında imzalanan anlaşmalar da uygulanmaktadır.[125]

Filistin nüfusunun ikamet ettiği yerlerde karşılaştığı sorunları anlamak ve gereken korumayı sağlamak oldukça karmaşık görünmektedir. Filistinlilerin verilerini, özgürlüklerini ve fiziksel ile dijital mahremiyetlerini ciddi bir şekilde koruyan yasalar düzenlemek oldukça zor bir iş temsil etmektedir. Filistinli internet kullanıcıları, askeri işgal yasalarına tabi olmaları ve İsrail'in Filistin bilişim ve iletişim teknolojilerinin altyapısını kontrol etmesi gibi birçok zorlukla karşı karşıya kalmaktadır.[126]

Batı Şeria'da Filistinliler, kendilerini ikili bir hukuk sistemine tabi bulmaktadır. Bunların birincisi, Ürdün yasalarının bazı bölümleri ve Filistin Yönetimi tarafından uygulanan Filistin Temel Yasası'dır. İkinci sistem ise, Batı Şeria'yı işgal eden İsrail'in çıkardığı askeri emirlerdir. Bu bağlamda İsrail, 1967 yılında Batı Şeria'yı işgal ettiğinde İngiliz Mandası tarafından yürürlüğe koyulan olağanüstü savunma sistemini uygulandığını duyurmuş ve daha sonra bunu birkaç askeri emirle desteklemiştir. Bu askeri emirler arasında, aynı yılda 1967'de çıkarılan ve barışçıl ifadeye kapsamlı bir yasak getiren "kışkırtma ve propaganda eylemlerinin önlenmesine" ilişkin 101 Sayılı askeri emir bulunmaktadır. 2010 yılında çıkarılan ve Ceza Yasası olarak bilinen 1651 Sayılı askeri emir "kamu güvenliğine veya kamu düzenine zarar verecek bir şekilde bölgede [Batı Şeria] sözlü veya başka herhangi bir şekilde kamuoyunu etkilemeye teşebbüs edenleri" on yıl hapis cezasına çarptırmaktadır.[127]

[125] Tezin Amaçları Doğrultusunda, Filistin Yönetimi Tarafından Çıkarılan Filistin Yasalarına Tabi Olan ve İsrail İşgali Altında Kalan Batı Şeria'ya Odaklanacağız.
[126] Kaed, a.g.m., s.58.
[127] Khamis ve Khalil, a.g.m., s.9.

Aynı zamanda "Eylemleri veya hedefleri ile düşman bir kuruluş için övgü, savunuculuk veya destek beyanları yayınlanmasını" bir "provokasyon eylemi" olarak kabul etmektedir. Bu emir de "bölge otoritelerine karşı ihlaller" gibi muğlak ifadeler içermektedir. Bu emirler, uluslararası insan hakları yasalarını ihlal etmekte ve içinde yer alan kavramların geniş ve muğlak ifadeler, Filistinlilerin temel haklarında ana kısıtlamalara yol açmaktadır.[128] Buna karşılık, işgal altındaki Batı Şeria topraklarındaki yerleşimlerde ikamet eden İsrailli yerleşimciler, İsrail ceza hukuku, sağlık sigortası hukuku ve diğer hukuk dalları dahil olmak üzere İsrail medeni hukukuna ve ayrıca askeri komutan tarafından yalnızca İsrail vatandaşları için geçerli olan özel mevzuata tabidir.

Dolayısıyla Batı Şeria'daki Filistinliler, İsrail Mahremiyet ve Veri Koruma Yasası ve İsrail Mahremiyet Otoritesinin yönergeleri de dahil olmak üzere İsrail yasalarına tabi değildir. İsrailli yerleşimcilerin denetlenmesi konusunda ciddi kısıtlamalar varken, Filistin halkı tamamen İsrail istihbaratının sürekli casusluk ve gözetim faaliyetlerine[129] maruz kalmaktadır.[130] İsrail'in 1991 yılında Uluslararası Medeni ve Siyasi Haklar Sözleşmesi de dahil olmak üzere insan haklarıyla ilgili uluslararası sözleşmeleri onaylamış olmasına rağmen, bu sözleşmelere karşı yükümlülüklerinin sadece kendi coğrafi sınırları içinde

[128] İnsan Hakları İzleme Örgütü (Human Rights Watch), "İsrail ordusu geniş kavramları dar yorumlamak yerine oluşan belirsizliği istismar etmekte ve gazeteciler ile aktivistler gibi temel haklarını kullanan Filistinlilerin tutuklanmasını haklı çıkarmak için ceza yasasını keyfi ve ayrımcı bir şekilde kullanmaktadır" şeklinde bir çıkarımla bu duruma raporlarından birinde işaret etmiştir. BKNZ: "Born Without Civil Rights Israel's Use Of Draconian Military Orders To Repress Palestinians İn The West Bank", Human Rights Watch, s.28, erişim 25 Ocak, 2022, https://2u.pw/1QBJo.

[129] Örneğin; İsrail hükümeti, sosyal medya siteleri tarafından sağlanan algoritmik tahminlere dayanan ve şüphelilerin tespit edilmesini sağlayan bir polis sistemi geliştirmiştir. Aynı zamanda bu sistem, İsrail istihbaratının Filistinli hesaplara rutin bir şekilde hacklamasına izin vermekte, Filistinlilerin özel bilgilerini elde edip biriktirerek depolamasına alan açmaktadır. İsrail istihbaratı, bu bilgiler aracılığıyla Filistinlilere şantaj yaparak onları kendi ajanlarına dönüştürmeye çalışmaktadır. BKNZ: "Facebook And Palestinians: Biased Or Neutral Content Moderation Policies?", The Arab Center for Social Media Advancement, (2018), ss.7–10, erişim 25 Eylül, 2021, https://2u.pw/gUNAP.

[130] "A Threshold Crossed Israeli Authorities And The Crimes Of Apartheid And Persecution", Human Rights Watch, erişim 25 Eylül, 2021, https://2u.pw/DqJ3T.

olduğunu ve bu nedenle hayatlarının tüm yönlerini kontrol ettiği 1967 yılında işgal edilmiş Filistin topraklarında ikamet eden Filistinlileri kapsamadığını savunmaktadır.[131]

3. Filistin Hükümetinin Dijitalleşmeye Yönelişi

İşgal koşulları nedeniyle Batı Şeria, bilgi teknolojisi sektörünün büyümesinde ve dijital ekonominin gelişmesinde belirgin bir gecikme yaşamaktadır. Uluslararası Telekomünikasyon Birliği tarafından 2017 yılında yayınlanan Uluslararası Bilgi ve İletişim Teknolojileri Gelişim Endeksi'nde Batı Şeria ve Gazze Şeridi, diğer Arap ülkeleri veya gelişmekte olan ülkelerle karşılaştırıldığında ortalamanın çok altında kalarak 176 ülke arasında 123. sırada gelmiştir. Ayrıca Batı Şeria ve Gazze Şeridi, henüz Uluslararası e-Devlet Gelişmişlik Endeksine dahil edilmemiştir.[132]

Öte yandan, Filistin'in karşı karşıya olduğu ikili zorluklara rağmen Bilgi ve İletişim Teknolojileri sektörü, 2018 yılında 3G hizmetlerinin başlatılması ile büyük bir niteliksel sıçramaya tanık olmuştur. Dünya Bankası tarafından hazırlanan bir raporda, Filistin Otoritesinin kötüleşen ekonomik durumla mücadele etmek için dijital ekonomiye yatırım yapmanın önemini göstermektedir. Bu önem, özellikle dijital teknolojilerin ve politikaların önemli bir rol oynadığı Covid-19 pandemisi ile açıkça görülmüştür. Zira Covid-19 pandemisi nedeniyle derinleşen ekonomik kriz, dijital iletişim ve çözüm teknikleri yoluyla dünya çapında hafifletilmiştir.[133] 2021 yılı itibarıyla Batı Şeria ve Gazze Şeridi'ndeki internet yayılım oranı, 5,16 milyonluk toplam nüfusun 3,65 milyon kullanıcıya ulaşarak yaklaşık %70,6 oranında kalmıştır. Sosyal medya yayılım oranı ise, 3,10 milyon abone olan yaklaşık %69,1'e ulaşırken cep telefonu abonelik sayısı, 4,35 milyon olan %84,2 oranına yükselmiştir.

---

[131] Birleşmiş Milletler, mahremiyet hakkına yönelik geniş çaplı ihlaller dahil olmak üzere Filistin halkına yönelik büyük insan hakları ihlallerinin kaynağının devam eden İsrail işgali olduğunu birçok kez vurgulamıştır. BKNZ: "Information Received From The State Of Palestine On Follow-Up To The Concluding Observations On İts İnitial And Second Periodic Reports 2020", Birleşmiş Milletler, erişim 21 Ocak, 2022, https://2u.pw/LGjl6.

[132] "Tatwir Alkhadama Alraqamia Fi Aldifa Algharbia Waqitae Ghaza" (TR: Batı Şeria ve Gazze Şeridi'ndeki Dijital Hizmetleri Geliştirmek, Dünya Bankası, s.8, erişim 21 Ocak, 2022, https://2u.pw/j2cUu.

[133] Dünya Bankası, a.g.e., s.9.

Dijitalleşme sektöründeki iyi büyümeye rağmen dijital altyapının alanında ciddi bir gelişim yaşanmamaktadır.[134] Ayrıca Filistin Yönetimi, dijital ekonomi için bir strateji belirlemek, bilgiye erişimle ilgili yasa ve mevzuatları güncellemek ve kullanıcıların mahremiyetini garanti altına almak için kişisel verileri ile internete güvenli erişim hakkını korumak gibi politikalarla dijital dönüşüm gündemini desteklemek için kapsamlı yasal ve düzenleyici çerçeve bir benimsememiştir.

4. Filistin Temel Yasası'nda Mahremiyet ve Özel Hayatın Gizliliği Haklarının Anayasal Ele Alınışı

Daha önce de belirttiğimiz gibi, Filistin anayasası henüz onaylanmamış ve anayasal belge statüsünde olan Filistin Temel Yasası, geçiş döneminin 1999 yılında sona ermesine rağmen hala uygulanmaktadır. Filistin Temel Yasası, uluslararası sözleşmeler tarafından onaylanan insan haklarını ve temel hakları kapsamakta ancak diğer anayasalar gibi açıkça dijital mahremiyet hakkına değinmemektedir. Bu nedenle -Ürdün Anayasası'yla yaptığımız gibi- mahremiyet ve özel hayatın gizliliği haklarının aynı doğaya sahip tek bir kaynaktan geliştiğini kabul ederek özel hayatın gizliliği hakkı ile ilgili maddelere bakacağız.

Filistin Temel Yasası, özel hayatın gizliliğine yönelik her türlü saldırıyı suç saymaktadır. Bu bağlamda yasanın 32. maddesi, "bireyin kişisel özgürlüklerine ve özel hayatının gizliliğine ve Filistin Temel Yasası ve Filistin yasaları ile güvence altına alınan diğer hak ve kamu özgürlüklerine yönelik her türlü saldırıdan kaynaklanan cezai veya medeni dava, zamanaşımı ile düşmeyen bir suç sayılır ve Filistin Yönetimi, zarara uğrayanlara adil tazminat verilmesini garanti eder." hükmünü içermektedir. Söz konusu madde, aynı ilkeye dayanması gerekçesiyle kişisel özgürlükler ile özel hayatın gizliliğini vurgulayarak birleştirmektedir. Aynı zamanda bu madde, özel hayatın gizliliği gibi hak ve özgürlüklerin ihlallerine ilişkin

[134] "Digital 2021: Palestine", Data Reportal, erişim 13 Ocak, 2022, https://2u.pw/4GBM3.

suçların zamanaşımı ile düşmeyeceğini ve zarara uğrayanların adil bir tazminat hakkına sahip olacağını öngörmektedir.

Filistin Temel Yasası, adli arama süreci ve özel hayat hakkıyla olan ilişkisine ilişkin iki gönderme yapmıştır. Birincisi bireylerin, ikincisi ise evlerin aranmasıyla ilgilidir. Bu iki madde, yetkililerin özel hayat hakkını ihlal eden istisnai tedbirler almasına yargı kararıyla izin verilen durumları ve kriterleri belirtmektedir. Örneğin; 11. madde, "1- Kişisel özgürlük, güvence altında dokunulmaz doğal bir haktır. 2- Hiç kimse, yasallar çerçevesinde bir yargı kararı dışında tutuklanamaz, aranamaz, hapsedilemez, herhangi bir kısıtlama ile özgürlüğü kısıtlanamaz veya hareket etmesi engellenemez. Önleyici tutukluluk süresi ancak yasalarla belirlenir. Cezaevlerini düzenlemek için çıkarılan yasaların öngördüğü yerler dışında tutukluluk veya hapis verilemez." hükümlerini öngörmektedir. 17. madde ise, "Evler dokunulmazdır. Yasallar çerçevesinde gerekçeli bir yargı kararı dışında gözetlenemez, girilemez ve aranamaz. Bu maddenin hükümlerini ihlal etmekten kaynaklanan tüm sonuçlar hükümsüz olacak ve bunun sonucunda zarar gören herkes, Filistin Yönetimi tarafından garanti edilen adil bir tazminat alma hakkına sahip olacaktır." emirlerini düzenlemiştir.[135]
Filistin Temel Yasası, iletişim gizliliğiyle ilgilenmeyip, gizliliği ele almamıştır. Filistin Temel Yasasının yazışma ve haberleşme gizliliğine ilişkin herhangi bir açık metni bulunmamaktadır. Filistin anayasasının çeşitli taslakların farklı versiyonları, yazışma ve haberleşme gizliliği ile ilgili bir maddeye yer vermiştir. Yukarıdaki 11. ve 17. maddelere baktığımızda, Filistin Temel Yasası'nın özel hayat hakkı için sadece geniş bir koruma sağladığını ve bu hakkı sadece konutların ve yerlerin gizliliği gibi geleneksel ve maddi bir anlayışla yorumladığını görmek mümkündür.[136]

Uluslararası yükümlülüklere gelince ise, Filistin'in 2012 yılının sonunda Birleşmiş Milletler'de üye olmayan gözlemci bir devlet olarak tanınmasından sonra Filistin Yönetimi,

[135] Khalil, a.g.m., s.229.
[136] Khalil, a.g.m., s.232.

2014 yılında Uluslararası Medeni ve Siyasi Haklar Sözleşmesi ve Çocuk Hakları Sözleşmesi dahil olmak üzere birçok uluslararası anlaşmayı ve sözleşmeyi imzalamıştır. Örneğin; Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'nin 17. maddesi, "1. Hiç kimse, özel hayatına, ailesine, meskenine veya yazışmalarına keyfi veya hukuka aykırı bir şekilde müdahalelere ya da onurunu veya itibarını kirleten hukuka aykırı saldırılara maruz bırakılamaz. 2. Herkes bu tür saldırı ve müdahalelerden hukuk tarafından korunma hakkına sahip" gibi hükümlere yer vermektedir.[137]

C. **Dijital Mahremiyet Hakkına Sağlanan Anayasal ve Yargısal Güvenceler**

Siyasi ve ekonomik hakları anayasa metinlerinde vurgulamak onlara büyük önem atfetmektedir. Anayasa, temel hakların pozitif hukukta korunmasını ve güçlendirilmesini garanti eden en önemli araçtır.[138] Bu bağlamda mahremiyet hakkının doğasını açıklamak için çeşitli görüşler ortaya çıkmıştır. Birinci görüş, bu hakkın kişisel haklar kategorisinde olduğunu savunurken ikinci görüş, onu insan odaklı kişisel haklar bağlamında değerlendirmeye tercih etmiştir. Bununla birlikte üçüncü bir görüş, mahremiyet hakkını ayni haklar kategorisinde ele alırken başka bir görüş, bu hakkı manevi haklar genelinde ve fikri mülkiyet (telif) hakları özelinde incelemiştir. Ancak hukukçuların çoğunluğu, bu hakkın kişisel haklar kapsamına giren bir istisna olarak değerlendirmiştir. Zira yasal mevzuat, ihlallere karşı mahremiyet hakkını koruyacak kurallar düzenlemediği için kişisel haklar kapsamına girmiştir.[139]

Bu bağlamda hukuk kişisel hakları, "Kişiliğin bileşenlerine, unsurlarına ve bireysel ile sosyal çeşitli doğal ve ahlaki tezahürlerine dayanan haklar" olarak tanımlamıştır. Aynı zamanda bu

---

[137] "Fi 'Aeqab Aindimam Filastin 'İilaa Jumlat Min Alaitifaqiaat Alduwalia" (TR: Bir Sürü Uluslararası Sözleşmeye Katılımının Ardından Merkez, Filistin'in Uluslararası Ceza Mahkemesi'ni Kuran Roma Sözleşmesi'ne Derhal Katılması İçin Çağrısında Bulunuyor), Filistin İnsan Hakları Merkezi, erişim 21 Şubat, 2022, https://2u.pw/neEYn.

[138] Nefis Medanat, "Qimat Alhuquq Walhuriyaat Almuetaraf Biha Fi Aldustur Al'urduni" (TR: Ürdün Anayasasında Tanınan Hak ve Özgürlüklerin Değeri), *Mu'tah Araştırma ve Çalışma Merkezi*, 11/1 (1996), s.242.

[139] Bojdin, a.g.m., s.53.

haklar türü, bireyin kişiliğini geliştirmek ve onu başkalarının saldırganlığına karşı korumak amacıyla bireyin kişilik bileşenleri üzerindeki çeşitli yetkilerini ve unsurları ifade etmektedir. Bununla birlikte çeşitli yasal mevzuat, mahremiyet hakkını korumak için medeni sorumluluk kurallarına dayanmakla yetinmemiş ve aynı zamanda bu hakkı yasa metinlerimde açıkça yer vererek hukuki koruma da sağlamıştır.[140] Bu bağlamda Fransız yasa koyucu, bu yorumu benimsemiş ve 1804 tarihli Fransız Medeni Yasasının 9. maddesinde özel hayatın gizliliği hakkını da kişisel haklardan saymıştır. Aynı şekilde Ürdünlü yasa koyucu, bu yorumu benimsemiş ve Ürdün Medeni Yasasının 48. Maddesi, insan doğasına bağlı haklar adı verilen bir grup hakka yer vermiştir. Ayrıca yasa, "Kişisel haklarından birine hukuka aykırı bir saldırıya uğrayan kişi, uğradığı zararın tazmini ile bu saldırının durdurulmasını isteyebilir" hükmüyle bu hakları korumuştur.[141]

Yukarıda da bahsettiğimiz gibi özellikle teknolojik değişimlerin artan hızı ve izleme tekniklerinin gelişimi nedeniyle dijital mahremiyet hakkının kapsamı, sürekli bir gelişme ve genişleme sürecine girmiş ve özel hayatın gizliliği kavramını aşarak önemli ölçüde genişlemiştir. Bu bağlamda dijital mahremiyetin önceden bilinen klasik mahremiyet anlayışının bir türü olmasına rağmen kişisel veriler ve bilgi sistemleri gibi yeni ve gelişmiş teknolojilere ve internetin kamusal doğası ve veri mülkiyeti gibi bu teknolojilerle ilgili sorunlara bağlılığı nedeniyle dijital mahremiyeti korumak adına klasik mahremiyet ve özel hayatın gizliliği hakları için geliştirilen klasik yasal hükümlerin uygunluğu ve etkinliği sorgulanmaktadır. Bu nedenle bazı hukukçular, dijital mahremiyetin bağımsız bir hak olduğunu ve özel hayat hakkı kapsamında olan hakların bir parçası olmadığını ileri sürmüşlerdir.

[140] Hamudi Hamudi, "Almaswuwlia Altaqsiria Alnaajima Ean Antihak Alhaqi Fi Alkhususit Eabr Alintirnit" (TR: Dijital Mahremiyet Hakkının İhlalinden Kaynaklanan Haksız Fiil Sorumluluğu), *Hukuk ve Siyaset Bilimleri Dergisi*, 8/1 (2019), ss.320-322.
[141] Saad El-Bishtawy, "Alhimaya Aldusturia Lilkhususia Almaelumatia" (TR: Dijital Mahremiyetin Anayasal Koruması), *Ürdün Kütüphaneler ve Bilgi Dergisi*, 52/2 (2017), s.110.

Bu konu, hukukçular arasında derin bir tartışma yaratmış ve Google Spain adıyla bilinen meşhur dava bu hukuki tartışmanın en önemli örneklerinden biri olmuştur. Aslında bu tartışma, Avrupa İnsan Hakları Sözleşmesine ve Avrupa Birliği Temel Haklar Şartı'na kadar uzanmaktadır. Zira her ikisinde de mahremiyet ile ilgili hükümler yer almış ve aynı zamanda özel hayata saygı hakkı AB hukukunda genel bir ilke olarak korunmuştur. Ancak Avrupa Birliği Temel Haklar Şartı, 8. maddede dijital mahremiyet anlayışının en temel hakkı olduğu için kişisel verileri koruma hakkı ile ilgili hükümler içermişken Avrupa İnsan Hakları Sözleşmesi, dijital mahremiyete ve özellikle kişisel verilerin korumasına ilişkin hükümlere yer vermemiştir. Bu bağlamda Google Spain davasında mahkeme, verdiği kararda mahremiyet hakkını genel bir şekilde ele alan ve kişisel verileri koruma hakkını kapsamayan Avrupa İnsan Hakları Sözleşmesi metnine dayanmıştır.[142]

Strazburg Mahkemesi ve Avrupa İnsan Hakları Mahkemesi, Avrupa İnsan Hakları Sözleşmesinde yer alan mahremiyet teriminin Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine mutabık olduğu yorumunu benimsemiştir. Avrupa Birliği Temel Haklar Şartı hükümlerine baktığımızda, mahremiyet ve veri koruma arasında açık bir ayrım olduğunu ve kişisel verileri koruma hakkının öznel kapsamı ve kişisel kapsamı açısından bu iki hakkın tamamen eş anlamlı olmadığını görmemiz mümkündür.[143] Ayrıca "şartın 8. Maddesi, sadece veri korumayı mahremiyetten farklı değerlendirmekle yetinmemiş ve aynı zamanda kişisel verileri koruma hakkı için 2. ve 3. fıkralarda belirtilen bazı güvencelere yer vermiştir. Bu bağlamda Avrupa Birliği Temel Haklar Şartı, kişisel verilerin belirli amaçlar için ve ilgili kişinin rızasına veya yasala belirlenmiş başka bir meşru temele dayalı olarak adil bir şekilde işlenmesi gerektiğini belirttiği gibi her kişinin kendisiyle bağlantılı olarak toplanan verilere erişme ve bunları düzeltme hakkına sahip olduğunu savunmuştur. Aynı zamanda şart, kişisel

[142] Hamudi, a.g.m., s.318.
[143] Hamudi, a.g.m., s.319.

verileri koruma hakkı ile ilgili kuralların bağımsız bir otoritenin denetimine tabi olması gerektiğini vurgulamıştır.[144]

Söz konusu iki hakkın, önemli derecede iç içe olmasına rağmen, tamamen eş anlamlı olmadığı ve her bir hakkın kapsamı, hakkın sınırları konusunda önemli farklılıkların olduğu sonucuna varılabilmektedir. Bu farklılık, tezin konusuyla ilgili başka bir soruna işaret etmektedir. Bu sorun, anayasaların özellikle dijital mahremiyet hakkını ne ölçüde koruduğu ile ilgilidir. Başka bir deyişle dünya genelinde ve Arap ülkeleri özelinde anayasaların çoğunluğu, özel hayatın gizliliği hakkının korunmasına yer varmışken belirttiğimiz gibi dijital mahremiyetin en önemli temeli olan kişisel verileri koruma hakkını tanıyan hükümleri bulunmamaktadır. Anayasaların bu hakka yer vermemesi nedeniyle dijital haklar, özel hayatın gizliliği hakkına benzerliği etkisiyle anayasalarda bu hakka sağlanan güvencelere ve hükümlere tabi olmaya devam edecektir. Bu bağlamda en yüksek yasalar olarak anayasalar, hakları ayrıntılı metinlerle değil, umumi sıfatlarıyla ele alıp onlara genel bir ilke olarak işaret etmekte ve ayrıntılar meselesini yasalara bırakmaktadır. Aynı şekilde yargı, dijital mahremiyet ve kişisel verileri koruma hakkı ile ilgili kararlarında anayasaların genel ilkelerinden başlayarak yasaların ayrıntılı hükümlerine kadar incelemektedir. Bu bölümde, varsa dijital mahremiyet ve genel olarak mahremiyet hakkı ve özel hayatın gizliliği hakkı için anayasaların sağladığı güvencelere bakacağız.

1. Ürdün Anayasasında ve Filistin Temel Yasası'nda Dijital Mahremiyet Hakkının Anayasal Güvenceleri

Daha önce de belirttiğimiz gibi, dünyada çoğu ülkelerin anayasaları, dijital mahremiyet hakkının korunmasına doğrudan atıfta bulunmamıştır. Ürdün anayasası da aynı durumdadır. Zira Ürdün anayasası, bugün bildiğimiz şekliyle ve hızlı teknolojik gelişme yıllarının gerektirdiği geniş koruma anlayışıyla dijital mahremiyet hakkını ele alan hiçbir madde

[144] Juliane Kokott ve Christoph Sobotta, "The Distinction Between Privacy And Data Protection In The Jurisprudence Of The CJEU And The Ecthr*", International Data Privacy Law*, 3/4 (2013), s.224.

içermemektedir. Dijital mahremiyet hakkının mahiyeti, kökeni ve koruduğu varlık açısından özel hayatın gizliliği hakkı ile aynı olduğu varsayımını ileri sürerek mahremiyet veya özel hayatın gizliliği hakkının korunmasına ilişkin madde ve hükümleri dijital mahremiyet hakkına yansıtma seçeneği ile karşı karşıya bırakmaktadır. Ancak daha önce belirttiğimiz gibi özel hayat hakkı fiziksel varlığı korumaya odaklanırken dijital mahremiyet, doğası gereği insanın manevi varlığını korumaya yönelmektedir.[145]

Bilgisayarların özel hayat konusundaki tehlikesine ilişkin farkındalık, Batı ülkelerinde 1970'lı yıllardan beri artmaya başlamış ve bu ülkelerin birçoğu, mahremiyet ihlallerini suç saymak adına farklı yasalar ve kararlar ortaya koymuştur. Özel hayatın korunması, Fransız hukukunda uzun bir döneme dayanmaktadır. Fransız yargısı, esnekliği ve yasal metinleri gerçeğe uygun olacak aynı zamanda da adaleti sağlayacak şekilde uyarlama gücünden ötürü böyle bir hakkı tanımada öncü bir rol oynamıştır. Bu bağlamda çeşitli araştırmalar, Fransız hukukunun özel hayat hakkını ve bunun sınırları ile nasıl korunacağı hususları öne çıkartılmasında önemli katkılar sağladığını ileri sürmektedir. Fransız yasa koyucu, 1970 yılında özel hayata saygı hakkını bağımsız bir hak olarak açıkça destekleyen bir yasa çıkarmıştır. 17 Temmuz 1970 tarihinde çıkarılan yasanın 22. Maddesi, "Herkes özel hayatına saygı gösterilmesi hakkına sahiptir ve yargı, zarar gören tarafın tazminat hakkına dokunmamak kaydıyla, özel hayat hakkına saldırıyı önleyecek veya durduracak her türlü koruma, hapsetme ve diğer tedbirler için karar verilebilir ve acil durumlarda bu tedbirler, nöbetçi mahkeme hâkimi tarafından da kararlaştırılabilir" hükmünü içermektedir.[146]

Fransa, bireylerin özel hayatlarına ilişkin kişisel verilerin korunmasını garanti altına alan 1978 tarihli 78-17 sayılı yasa gibi verilerin sanal ortamda işlenmesine ilişkin bir dizi yasa çıkarmaya devam etmiştir. Ayrıca yeni Fransız Ceza Yasası da dijital mahremiyet ile ilgili suçlar içermiştir. Ceza Yasasının 226-1. Maddesi, Kişisel Veriler ve Özgürlükler için Ulusal

[145] Khamis ve Khalil, a.g.m., s.4.
[146] Lami, a.g.e., s.116.

Veri Komitesi'nin izni ve onayı olmaksızın elektronik verilerin işlenmesini suç saymış ve suçlu bulunanları bir yıllık hapis ve üç yüz avro para cezasının yanında cezayı alenen yayınlamak gibi ek cezalar kararlaştırmıştır. Fransız yasa koyucu, sanal bilgilerin bozulmasına, yok edilmesine veya yetkisiz kişilerce erişilmesine karşı güvenliğini sağlamak için her türlü önlemi almadan verileri işleyen herkese beş yıl hapis ve iki milyon avro para cezası vermiştir. Ceza Yasasının 226-20. Maddesi, nominal verilerin hukuka aykırı olarak saklanması suçunu içermiş ve bahsi geçen komitenin onayı olmaksızın daha önce talep edilen veya önceki bildirimde yer alan süreden daha uzun bir süre için nominal veriler şeklindeki bilgileri saklayan kişiye bir yıl hapis ve üç yüz bin avro para cezası ile cezalandırmıştır.[147]

Bununla birlikte Ceza Yasasının 226-21. Maddesi, nominal verilerin işleme amacından sapma suçuna yer vermiştir. Kayıt sınıflandırma, sınıflandırılan kaydı aktarma veya diğer herhangi bir işleme prosedürü sırasında nominal verileri elde eden ve verilerin yasada öngörülen nihai varış yerini değiştiren herkesi beş yıl hapis ve iki milyon avro para cezasıyla mahkûm etmiştir. Buna ilaveten Ceza Yasasının 226-22. Maddesi, nominal verilerin hukuka aykırı olarak ifşa edilmesi suçunu ele almış ve kayıt, dinleme, aktarma veya dijital işemenin diğer herhangi bir işlemiyle açıklanması ilgili kişinin itibarını veya özel hayatının gizliliğini ihlal edecek nominal veriler alıp ifşa eden her kişi için bir yıl hapis ve yüz bin avro para cezası ile cezalandırmıştır. Ancak aynı madde, söz konusu ifşanın ihmalkarlık nedeniyle meydana gelmesi halinde suçlu, elli bin avro para cezasına çarptırılacağını ve bu tür davaların ancak mağdurun şikâyetiyle başlayacağını belirtmiştir.[148]

Fransız yasa koyucu, mahremiyetin daha fazla yasal korunmasını sağlamak için yeni yasal düzenlemeler geliştirmeye devam etmiştir. Geleneksel metinleriyle ceza hukuku, dijital tehlikeler karşısında bireylerin özel hayatını ve mahremiyetini korumada yetersiz olduğunu

[147] Lami, a.g.e., s.118.
[148] Suzan Al-Ustath, "İntihak Hurmat Alhayat Alkhasa Eabr Al-İntarnit: Dirasa Muqarana" (TR: Özel Hayatın Gizliliği Hakkını Internet Üzerinden İhlali: Karşılaştırmalı Bir Çalışma), *Şam Üniversitesi İktisadi Ve Hukuki Bilimler Dergisi*, 29/03 (2013), s.433.

ortaya çıkmıştır. Bu çabalar, ceza durumunu dijital ortamda işlenmesiyle ilgili 1980 yılında çıkan yasa örneğinde olduğu gibi verilerin işlenmesinden kaynaklanan yasal sorunları çözmeyi hedefleyen çeşitli yasal düzenlemeyi ortaya çıkartmayı içermiştir.[149]

Öte yandan ABD Anayasasının mahremiyet hakkına açık bir yer vermemesine rağmen Amerikan hukukçular, mahremiyetin ve onu herhangi bir saldırıdan korumanın önemine dikkat çekmiştir. İlk başta bu hakkı korumakla emsal davalara tanık olmayan Amerikan yargısı, mahremiyet hakkını tanıma yetkisinin yasa koyucunun tekelinde olduğunu ve bu hakkın manevi boyutu nedeniyle onu hedef alan saldırılar karşısında tazmin etmenin zor olduğunu açıklamıştır. ABD Yüksek Mahkemesi, insanların duygularını incitmenin aslında ahlak kurallarına girdiğini ve toplumda sempatik bir kamuoyu oluşturmakla ilgili olduğunu belirtmiştir. Ancak hayatın gelişmeye devam etmesiyle birçok Amerikan hukukçu, emsal davalar olup olmadığına bakılmaksızın mahremiyet hakkının önemine inanmıştır. Bu nedenle Amerikan yasa koyucusu, 1968 yılında ABD Kongresi tarafından kabul edilen yolcu araçlarında ve sokaklarda suçla mücadeleye ilişkin bir yasa da dahil olmak üzere mahremiyetin belirli yönlerinin korunmasıyla ilgili çeşitli yasalar çıkarmıştır. Telefon görüşmeleri ve kişisel konuşmaları izinsiz bir şekilde yapılan dinleme, dinlenilen sesi kaydetme eylemlerine karşı korunmasını ve bu eylemleri yapanların suçlu sayılmasını öngörülmüştür.[150]

ABD, verileri ve ona erişim hakkını korumak için 1970 yılında bir yasa çıkarmıştır. Bundan sonra 1974 yılında çıkan ve 1976 yılında değişikliğe uğrayan 393-94 sayılı mahremiyet yasası, 1973 ile 1976 yıllarında yayınlanan gözetim ve teftiş suçlarıyla ilgili iki yasa çıkarılmıştır. Bununla birlikte 1974 yılında çıkarılan 93-380 sayılı Eğitim ve Özel Hayat Haklarının Korunması Hakkında Yasa ve 1978 yılında çıkarılan 95-630 sayılı Mali Verilerin Korunması Hakkında yasa gibi daha sonra çeşitli yasalar da çıkarılmıştır. Ayrıca Amerikan

[149] Lami, a.g.e., s.121
[150] Al-Ustath, a.g.e., s.423.

yasa koyucu, iletişimin izlenmesini ve içeriklerinin paylaşılmasını yasaklayan 1986 tarihli Dijital İletişim Mahremiyet Yasası'nı da çıkarmıştır.[151] 1994 yılında çıkan Yasa Uygulama Yasası (CALEA) için İletişim Yardımı yasası, devletin ileri teknolojiye soruşturması ve müdahalesinin bir mahkeme kararına dayanmasını şart koşmuştur. 1998 yılında ise web siteleri yöneticilerinin 13 yaşın altındaki çocuklara ait herhangi bir kişisel bilgiyi yayınlamasını yasaklayan ve bunları yayınlamak için önceden ebeveynlerinden izin almalarını zorunlu kılan Çocukların Çevrimiçi Gizliliğini Koruma Yasası kabul edilmiştir.[152] Ayrıca bankacılık ve kredi sektörü kartlarını ve çalışma ilişkilerini düzenleyen genel yasalar geliştirmiştir.[153]

Bunlardan yola çıkarak ABD hukukundaki mahremiyet hakkı, federal anayasada yer alan veya mahkemeler veya yasama organları tarafından tanınan ilkelerin bir bileşimi olduğu görülmektedir. Ancak dijital verilerin işleme süreçleri karşısında mahremiyeti ve özgürlükleri koruyan yasalar koymakta öncü bir rol üstlenen Fransız yasa koyucunun aksine ABD hukuku, mahremiyeti düzenleyen yasaların çokluğuna rağmen, ilgili kişilerin özel verilerini doğrudan hükümlerle korumadığı ve genel hükümlerle yetindiği sonucuna varılmak mümkündür.[154]

Dijital mahremiyet için anayasal güvenceler sağlamanın önemi, anayasal kuralların ülkedeki diğer tüm hukuk kurallarından daha üstün olmasıdır. Dolayısıyla bu hakkı ihlal eden herhangi bir yasa veya yasal düzenlemenin anayasaya aykırı olması nedeniyle geçersiz sayılmaktadır. Daha önce de belirttiğimiz gibi, Ürdün anayasası ve Filistin Temel Yasası da dahil olmak üzere dünyanın çoğu ülkelerinin anayasası dijital mahremiyet hakkının korunmasından bahsetmemiştir. Bu nedenle burada, dijital mahremiyet hakkı ile sağlanan güvencelerin türü açısından farklı olmasına rağmen doğa ve köken açısından benzer olan özel hayatın gizliliği

[151] Lami, a.g.e., s.121.
[152] Al-Ustath, a.g.e., s.417.
[153] Hamudi, a.g.m., s.324.
[154] Al-Ustath, a.g.e., s.423.

hakkının Ürdün ve Filistin anayasalarından sahip olduğu anayasal güvenceleri ele alacağız. Önceki literatür tartışmalarında dile getirdiğimiz gibi, özel hayatın gizliliği hakkının fiziksel varlığı korumakla ilgilendiği ancak dijital mahremiyet hakkının doğası gereği insanın kişisel manevi varlığına odaklandığını açıkladık.[155]

Ürdün anayasa koyucusu, 1952 anayasasında yer alan anayasal ilkeler doğrultusunda anayasanın Ürdünlülerin Hakları ve Görevleri başlıklı İkinci Bölümü aracılığıyla her Ürdün vatandaşı için tüm hakların ve kamu özgürlüklerinin korunmasını güvence altına almıştır. Söz konusu bölüm, bireysel ve toplumsal haklara ilişkin bir dizi maddeyi içermiştir. Buna göre ifade ve düşünce özgürlüğü, din özgürlüğü ve özel hayatın gizliliği hakkı bireysel haklar kategorisinde yer almaktadır. Özel hayatın gizliliği hakkı, bireyin özel çevresini korumayı hedeflediği gibi onun özel alanına başkalarının girişini kabul etmemesi, medeni durumunu açıklamayı reddetmesi veya konutunu istediği şekilde seçmesi gibi alanları ele alan hükümlerden oluşmaktadır.[156]

Anayasanın 7. Madde, "kişisel özgürlükler güvence altına alınmıştır ve Ürdünlülerin haklarına, kamu özgürlüklerine veya özel hayatlarının gizliliğine yönelik her saldırı kanunen cezalandırılabilecek bir suçtur" hükmünü içermiştir. Bu hakkın anayasaya dahil edilmesi, devlet veya bireyler tarafından ihlal edilemeyecek anayasal bir hak haline getirmektedir. Bu yasal metin, devlet, bireyler, özel şirketler veya basın olursa olsun bu hakka yönelik saldırıyı gerçekleşen taraflara bakmaksızın genel ve açık bir şekilde düzenlenmiştir. Ancak, genellikle konut ve özel mülkiyet başta olmak üzere fiziksel yönlerle ilgilenen özel hayatın gizliliği kavramının aksine mahremiyet kavramı, yer ve zaman bakımından mahremiyetin bir kişiyle ilgili birçok yönünü ve kişi ile ilgili manevi varlığı kendi içinde birleştirmektedir.[157]

[155] Al-Ustath, a.g.e., s.424.
[156] Medanat, a.g.m., s.244.
[157] Medanat, a.g.m., s.248.

Anayasanın 10. maddesi, meskenlerin dokunulmazlığını vurgulayarak yasada belirtilen haller dışında girilemeyeceğini belirtirken 14. madde ise, dini tören ve inançların örf ve adetlere uygun olarak icra edilmesi özgürlüğünün kamu düzenine veya ahlaka aykırı olmadığı sürece devletin koruduğunu açıklamıştır. Anayasanın 15. maddesi, tüm ifade araçlarıyla düşünce ve ifade özgürlüğü, bilimsel araştırma özgürlüğü, sanatsal ve sportif yaratıcılık; basın, basım ve yayın özgürlüğü gibi çeşitli haklar öngörmüştür. 18. madde ise, yazışma ve telefon görüşmelerinin gizliliğini ve bunların yargı kararı olmadan ele geçirilmesinin yasaklanmasını öngörerek özel hayatın gizliliği hakkını korumuştur. Söz konusu madde, "tüm posta ve telgraf yazışmaları, telefon görüşmeleri ve diğer iletişim araçları gizli kabul edilir ve yasa hükümlerine göre yargı kararı olmadan izlenmeye, ele geçirilmeye, engellenmeye veya müsadere edilmeye tabi tutulamaz" hükmüne yer vermiştir.[158]

Anayasa maddelerinin önceki incelemesinden yola çıkarak anayasa yasa koyucunun yazışmaların gizliliği ve konutun dokunulmazlığı gibi korunması gereken özel hayatın gizliliği hakkının bazı yönlerine yer verdiğini görüyoruz. Ayrıca bu hakkın bazı yönlerinin anayasanın özünde doğrudan sıralanması, yasa koyucunun özel hayatı farklı unsurlarıyla sınırlı kalmadan örnek vererek koruma ve muhafaza etme konusundaki istekliliğinden kaynaklandığını söylemek mümkündür. İfade şu şekildedir: "yasal anlamda kavram, kapsayıcılık ve bütünlük adına tek bir anlam için kullanılırsa belirli bir sayı ile sınırlandırılmadan tüm bireyler için kesin bir anlam kazanmaktadır. Genel kavramlar, kapsayıcılık ve bütünlük göstergesi olduğundan dolayı gerekçe olmadan özelleştirilememektedir. Bu nedenle genel, geçerli gerekçe olmasan özelleştirilirse yasal olarak geçersiz bir yorum sayılmaktadır. Aynı zamanda genel bir anlamla kullanılan her yasal metin, kapsayıcılık anlamını taşıması özelleştirmek için açık gerekçelere sahip olması gerekmektedir". Diğer taraftan ise bazı uzmanlar, anayasa koyucusunun anayasaya sadece vatandaşların özel hayatın gizliliği haklarının önemini vurgulayıp koruyan genel bir hüküm dahil etmesi veya bu genel hükmün altında hakkın kapsamına giren tüm unsurları sıralaması

[158] Medanat, a.g.m., s.249.

gerektiğini savunmuştur. Ancak başka bir görüş, anayasanın genel bir hüküm içerip özel hayatın gizliliği hakkının unsurlarına dahil edilebilecekleri ekleme işini yasama organına bırakılması gerektiğini belirtmiştir.[159]

Filistin Temel Yasası dahil olmak üzere birçok Arap anayasasının aksine Ürdün anayasası, mahremiyet hakkıyla ilgili bir saldırıya maruz kalanlara adil bir tazminatın verilmesini güvence altına almamıştır. Genel anlamda Ürdünlü yasa koyucu, Medeni Yasa hükümlerinde saldırıya uğrayan herkese verilen zararın karşılığına tazminat verilmesi ilkesine yer vermiştir. Yukarıda bahsi geçen anayasal metinlere ve özellikle 18. madde metnine baktığımızda, Ürdünlü yasa koyucunun telefon iletişimi ve posta yazışması gibi örneklerle mahremiyet hakkını ele aldığı sonucuna varıyoruz. Gelişmiş iletişim araçlarından doğrudan bahsetmeyi ihmal eden Ürdünlü yasa koyucu, anayasa metne "diğer iletişim araçları" tabirini ekleyerek aynı hükümleri sosyal medya gibi yeni iletişim araçlarına uygulama fırsatını vermiştir. Dijital mahremiyet kavramı nispeten yeni olduğunu ve Ürdün için sınırları hala belirlenme sürecinden geçtiğini- ki bu nedenle bu haktan anayasada doğrudan bahsedilmediğini- kabul etmemiz mümkündür. Ancak bu tezin yazıldığı tarihe kadar dijital mahremiyet hakkının herhangi bir yasa veya mevzuatta ele alınmaması, dijital işlemlerin sağladığı devasa verileri yalnızca yazışmaları ele geçirme tehlikesi değil, aynı zamanda hackleme veya farklı amaçlar için kullanma gibi yasa dışı eylemlere karşı herhangi bir yasal korumayı garanti etmeksizin kullanıcıların mahremiyetlerini ihlallere karşı maruz bırakmaktadır. Ürdünlü yasa koyucu, yazışma kavramını e-posta mesajlarını ve akıllı mesajlaşma uygulamalarını içerecek şekilde genişlettiyse de bu korumayı telekomünikasyon şirketleri, internet servis sağlayıcıları ve benzeri kamu veya özel kurumların veri sistemlerinde saklanan verilerin korunmasıyla sınırlandırmıştır.

[159] Al-Ajarma, a.g.e.

Ürdün mevzuatının kapsamlı bir incelemesi sonucunda, özel hayatın gizliliği hakkına sağlanan anayasal güvencelerin özellikle kişisel verilerin korunması bağlamında diğer mevzuat ve yasalara geniş bir şekilde yansıtılmadığını görmek mümkündür. Ürdün hukuk sistemi, mahremiyet hakkına Ceza Yasası, Siber Suçlar Yasası ve iletişim Yasası gibi çeşitli yasalar arasında dağılmış ayrı yasal hükümlerle yalnızca kısmi koruma sağlamaktadır. Aynı zamanda söz konusu kısmi koruma, önemli eksikliklerle dolu olmakla birlikte belirli durumlar için geçerli olacak şekilde tasarlanmıştır. Buna ilaveten söz konusu yasal hükümler, bilişim alanındaki büyük gelişmelere aynı zamanda da İnternet'teki devasa kişisel verilerin miktarına uygun olmayan geleneksel metinler temsil etmektedir. Kişisel Verileri Koruma Yasası Tasarısı, daha gelişmiş bir metin olmasına rağmen henüz Mevzuat ve Görüş Kurulu'nda bekletilmektedir.

Filistin'deki genel durum, Ürdün'ünkinden çok farklı değildir. Ancak Filistin durumu, daha karmaşık halde olup Filistin halkının kişisel özgürlüğü, özel hayatın gizliliği ve elbette dijital mahremiyet ile ilgili güvencelerin sayısı azalmaktadır. Filistin Temel Yasası, özel hayatın gizliliği hakkına yönelik her türlü saldırıyı suç saymaktadır. Yasanın 32. maddesine göre, "Filistin Temel Yasası veya yasalar ile teminat altına alınan kişisel özgürlükler, özel hayatın gizliliği hakkı ve benzeri hak ve kamu özgürlüklerine yapılan her saldırı cezai ve medeni davaları zamanaşımına tabi olmayan bir suçtur. Filistin Yönetimi bu suçtan zarar görenler için adil bir tazminat garanti etmektedir". Bahsi geçen madde, Ürdün anayasası gibi aynı ilkeye dayandıkları gerekçesiyle kişisel özgürlükleri ve özel hayatın gizliliği hakkını birlikte ele almıştır. Aynı zamanda bu madde, hak ve özgürlüklerin ve özel hayatın gizliliği hakkının ihlallerine ilişkin suçların zamanaşımına uğramayacağını belirttiği gibi zarara uğrayanlara adil tazminat hakkı tanımaktadır.

Filistin Temel Yasası, arama süreci ve özel hayatla ilişkisi ile ilgili iki gönderme içermiştir. Birincisi bireylerin aranmasına ilişkin iken ikincisi, evlerin aranması ile ilgilidir. Bu iki madde, yetkililerin özel hayatın gizliliği hakkını yargı kararıyla aşacakları istisnai tedbirler

almasına izin verilen kuralları ve durumları belirtmektedir. Anayasanın 11. Maddesinde, “1- Kişisel özgürlük doğal bir haktır, garantilidir ve dokunulmazdır. 2- Hiç kimse, yasa hükümlerine uygun yargı kararı olmadıkça tutuklanamaz, aranamaz, hapsedilemez, özgürlüğü herhangi bir şekilde kısıtlanamaz ve hareket etmesi engellenemez” hükmünü içermiştir. 17. Madde ise, "konutlar dokunulmazdır kutsaldır. Yasa hükümlerine uygun gerekçeli bir yargı kararı olmaksızın izlenmez, girilemez ve aranamaz. Bu madde hükümlerine aykırı hareket edilmesinin tüm sonuçları hükümsüzdür. Bu durumdan kim zarar görmüşse, Filistin Yönetimi'nin güvence altına aldığı tazminat hakkına sahip olacaktır." hükmünü öngörmüştür. Filistin Temel Yasası, iletişimin mahremiyetine ilişkin herhangi bir maddede ele almayıp bu konuyla ilgili herhangi bir açık hükmü bulunmamakta ve hatta mahremiyeti geleneksel anlamda inceleyen metinlere yer vermemektedir.

Filistin anayasasının farklı taslak metinleri, iletişim ve yazışmaların mahremiyetine ilişkin bir maddeye yer vermiştir. İletişim Yasası'nın usul maddeleri, iletişime ve yazışmaların saldıran eylemleri suç saymıştır. İletişim Yasası'nın 92. Maddesi, "İletişim ağları aracılığıyla bir mesajın içeriğini engelleyen, değiştiren veya silen veya başkalarını bu eylemi gerçekleştirmeye teşvik eden kişilerin bir aydan az ve altı aydan fazla olmamak üzere hapis cezası veya 50 Ürdün dinarından az ve 200 Ürdün dinarından fazla olmamak para cezası veya her ikisi ile cezalandırılır" hükmünü öngörmektedir. Yukarıdaki maddelere baktığımızda, Filistin Temel Yasası'nın, evlerin ve yerlerin gizliliği gibi özel hayatın gizliliği hakkının geleneksel ve fiziksel doğasına özgü yalnızca belirsiz bir koruma sağladığı sonucuna varıyoruz. Ayrıca, Filistin Temel Yasası'nda yer alan anayasal hükümler, dijital özel hayata ilişkin kişisel bilgileri korumak için tek başına yeterli değildir. Bu hükümler, çok geleneksel olduğu gibi mahremiyetin ihlali ve bireylerin dijital haklarının ihlali açısından en büyük riski temsil eden verileri kapsamamaktadır.

Bütün bunlardan yola çıkarak 2016 yılındaki anayasa değişikliklerinde dijital mahremiyete ve kişisel verilerin korunmasına yer veren Cezayir anayasasının aksine Ürdün anayasası ve

Filistin Temel Yasası, dijital mahremiyeti tam anlamıyla ele almamıştır. Cezayir anayasasının 46. Maddesi, her türlü iletişim ve yazışmanın gizliliği ve kişisel nitelikteki verilerin işleme sürecinde korunması da dahil olmak üzere, bireyin ve ailesinin mahremiyetinin dokunulmazlığına karşı eylemleri açık bir şekilde suç saymıştır.[160] Ürdün ve Filistin'de her iki anayasa, özel hayatın gizliliği hakkını kişisel haklar içerisinde kabul ederek anayasal bir hak olarak güvence altına almaktadır.[161]

Ancak kapsamlı bir incelemeden sonra söz konusu yasal hükümler, modern teknolojinin getirdiği riskler karşısında kişisel verileri korumak için yeterli olmadığı için sadece özel hayata geleneksel koruma sağladığı ortaya çıkmaktadır. Ayrıca bu hakkı düzenleyen maddeler, modern teknolojileri kullanarak ihlal edilebilen ve devlet kurumları, özel sektör şirketleri ve diğerlerini hedef alan bireyler tarafından saldırıya uğrayabilen dijital mahremiyeti kavramakta zorlanmaktadır. Bu nedenle bu iki anayasanın manevi haliyle bireylerin dijital mahremiyetine tam olarak güvenceler sağlamadığını tespit ettik ve bundan sonra anayasa hükümleriyle uyumluluğu veya aykırılığı açısından değerlendirmek adına yasalar ve yönetmelikler gibi diğer mevzuatlara bakacağız. Aslında ne Ürdünlü ne de Filistinli yasa koyucu, kişisel verileri başta olmak üzere veri korumasını düzenleyen bir yasayı onaylamamış ve bu nedenle bu konuyla ilgili farklı yasalarda dağılan çeşitli hükümleri tartışacağız.

2. Ürdün ve Filistin'de Dijital Mahremiyet Hakkına Tanınan Yargısal Güvenceler

Yasaların anayasaya uygunluğunun denetimi, yasa ve yönetmeliklerin, diğer tüm yasal düzenlemelerden daha üstün olan anayasaya uygunluğunu sağlamak için etkili bir araç olması nedeniyle genel anlamda anayasanın üstünlüğünü güvence altına almak ve hukuk devleti ilkesini korumak için önemli bir ilkedir. Bu denetim süreci, olağan mevzuatın anayasa hükümlerine uygunluğundan ve yasama makamlarının anayasal ilkelere uymasından emin olmak için çok faydalıdır. Ayrıca yasaların anayasaya uygunluğunun denetlenmesinin önemi,

[160] Cezayir Anayasası, erişim, 27 Şubat, 2022, https://2u.pw/mGGBp.
[161] Khamis ve Khalil, a.g.m., s.9.

anayasayı korumak, mevzuat hiyerarşisinin en üstünde tutmaktır. Böylece tüm yasalar, anayasanın sınırları içinde kalacaktır. Bu bağlamda Ürdün ve Filistin'deki Anayasa Mahkemeleri, Anayasa'ya aykırılık iddiasıyla iptal davası veya itiraz yolu gibi çeşitli yöntemlerle yasaların anayasaya uygunluğunu denetleme görevini üstlenmiştir.

Filistin ve Ürdün'deki Anayasa Mahkemeleri kayıtlarını incelediğimizde, farklı kapsamlarıyla dijital mahremiyet hakkına ilişkin herhangi bir karara rastlamadık. Bu durum, dijital mahremiyet hakkına ilişkin yasal düzenlemelerin oldukça yeni kabul edilmiş olmasına bağlamak mümkündür.

D. Ürdün, Filistin ve Avrupa Birliği Arasında Dijital Mahremiyet Hakkının Anayasal Ele Alınışının Karşılaştırılması

Ürdün ve Filistin anayasaları, dijital mahremiyet hakkına ilişkin doğrudan hükümlere yer vermezken Avrupa Birliği Temel Haklar Şartı, dijital mahremiyet hakkının doğrudan korunmasını öngörmüştür. Bu bağlamda ilk olarak genel bir karşılaştırılma ile başlıyoruz ve ardından maddelerinin benzerliği nedeniyle Ürdün ve Filistin anayasalarının özel bir karşılaştırılmasını yapıyoruz.

Ürdün ve Filistin anayasaları, doğrudan dijital mahremiyet hakkıyla ilgili herhangi bir hüküm vermemekte benzeşmektedir. Ancak bu iki anayasa, özel hayatın korunmasını sağlayacak hükümlere yer vererek vatandaşların özel hayatlarının ihlal edilmesini kanunen cezalandırılabilecek bir suç olarak ele almışlardır. Söz konusu hükümler, konutların dokunulmazlığının yanı sıra özel hayatın gizliliğini ve mahremiyetini de korumuştur. Aynı zamanda bu hükümler, kamu kurumların bu hakları ihlal edecek veya tehdit edecek her türlü eylemine yasal sınırlamalar getirmiştir. Aslında Ürdün ve Filistin anayasaları bu konuyu hemen hemen aynı şekilde ele alarak anlaşmıştır. Konutların dokunulmazlığı ve özel hayatın korunması ile ilgili hükümler, Ürdün Anayasası'nın 7, 8, 10 ve 17 numaralı maddelerinde

belirtilirken[162] aynı hükümler, Filistin Temel Yasası'nın 11 ve 17 numaralı maddelerinde ele alınmıştır.

Diğer taraftan ise 2000 yılının aralık ayında yürürlüğe giren Avrupa Birliği Temel Haklar Şartı, kişisel verilerin korunmasını her bireye tanınan bir hak olarak açıkça yer vermiştir. Şartın 8. Maddesi, kişisel verilerin uygun bir şekilde ve belirli amaçlar için işlenmesini zorunlu kılmıştır. Ayrıca verilerin işlenmesi için en az bir tanesinin yerine getirilmesi gereken iki koşul koşmuştur. Birinci koşul, veri sahibinin rızasını almak iken ikincisi koşul, bu verilerin kullanım ve işleme amacının yasayla belirlenmiş meşru bir amaç olmasıdır. Söz konusu madde, tüm tarafların bu koşullara bağlılığını denetlemekle görevli bağımsız bir kurulun kurulmasını öngörerek sona ermiştir.[163] Bu madde, dijital mahremiyet hakkını doğrudan ve açık bir şekilde öngörmesi, bu hakkı diğer tüm haklardan bağımsız olarak düzenlenmesi ve sahibinin rızası olmadan verilerin işlenmesinin sadece yasada öngörülen durumlarla sınırlandırılması gibi çeşitli avantajlara yer vermiştir. Ayrıca tüm tarafların (kamu ve özel) bu koşullara bağlılığını denetleyecek bağımsız bir organın oluşturulması, yasaya olan güveni artıracak ve onun etkin uygulamasını sağlayacak tarafsız denetimi güçlendirmeye yönelik önemli bir adım oluşturmuştur.

Ürdün ve Filistin anayasaları arasındaki farklılıklara gelince, bunları iki noktada özetlemek mümkündür. Birinci nokta, Filistin Temel Yasasının özel hayatın gizliliğini ihlal etme suçuna ilişkin yasal güvencelerin artırdığına bağlıdır. Diğer nokta ise özellikle 2014 yılında meydana gelen değişiklikten sonra Ürdün Anayasanın 18. maddesiyle ilgilidir. Bunların şöyle özetebiliyoruz:

1-Ürdün anayasası, "kişisel özgürlüğün güvence altına alındığını aynı zamanda Ürdünlülerin haklarına, kamu özgürlüklerine veya özel hayatlarının gizliliğine yönelik her türlü saldırının kanunen cezalandırılan bir suç olduğunu" belirtmiştir. Diğer taraftan ise Filistin anayasasındaki buna benzer metin şöyleydi: "Filistin Temel Yasası veya yasalar ile teminat altına alınan kişisel özgürlükler, özel hayatın gizliliği hakkı ve benzeri hak ve kamu özgürlüklerine yapılan her türlü saldırıdan kaynaklanan cezai veya medeni davanın

[162] Aldustur Al'urduni (TR: Ürdün Anayasası), erişim 07 Ekim, 2021, https://2u.pw/hp9Uq.
[163] "Charter of Fundamental Rights of the European Union", *Official Journal of the European Union* 83/53 (2010), s.380.

zamanaşımı ile düşmeyen bir suç olduğunu ve Filistin Yönetimi bu suçtan zarar görenler için adil bir tazminat garanti ettiğini" öngörmüştür. Bundan yola çıkarak Filistin anayasasındaki maddenin, Ürdün anayasasındaki muadiline nazaran daha fazla koruma sağladığını görüyoruz. Zira Filistin anayasasındaki madde, suçun zamanaşımına uğramadığını öngördüğü ve bunun kamu otoritesi tarafından işlendiğini varsayarak mağdurun maruz kaldığı zararın tazmini için bu otoriteye garantör olarak baktığı nedeniyle daha sağlam bir koruma vermiştir. Bunun aksine Ürdün anayasası, söz konusu ihlali herhangi bir ayrıntı vermeden suç olarak değerlendirmekle yetinmiştir.[164] [165] [166]

2- 2014 yılındaki değişiklikten sonra Ürdün anayasasının 18. Maddesi, "tüm posta ve telgraf yazışmaları, telefon görüşmeleri ve diğer iletişim araçları gizli kabul edilir ve yasa hükümlerine göre yargı kararı olmadan izlenmeye, ele geçirilmeye, engellenmeye veya müsadere edilmeye tabi tutulamaz" olarak düzenlenmiştir. Bu madde, tüm ihlal ve gözetimlere karşı yazışma ve telefon görüşmelerinin gizliliğine anayasal bir koruma sağlamıştır. Aynı zamanda madde metninde dijital iletişimden açıkça söz edilmese bile, "ve diğer iletişim araçları" cümlesinin eklenmesi, dijital iletişim araçlarının bu hükme dahil olduğu şeklinde yorumlanması mümkündür. Diğer taraftan ise Filistin Temel yasası, bu hükme veya bunun benzerine yer vermemiştir.[167]

[164] Aldustur Al'urduni (TR: Ürdün Anayasası), erişim 07 Ekim, 2021, https://2u.pw/hp9Uq.
[165] "Qarar Alearab Bialmusadaqat Ealaa Almithaq Alearabii Lihuquq Al'iinsan" (TR: Arapların Kararı Arap İnsan Hakları Sözleşmesini Onaylamaktır), Al Jazeera Net, erişim 22 Ocak, 2022, https://2u.pw/2CRD7.
[166] Arab Charter on Human Rights, erişim için http://hrlibrary.umn.edu/instree/loas2005.html.
[167] "Al'urdun: Taedilat Dusturia Jadida Tujib Salahiaa Lilmalik Minfirida" (TR: Ürdün: Krala Tek Taraflı Yetkiler Veren Yeni Anayasa Değişiklikleri", CNN, erişim 28 Ağustos, 2021, https://2u.pw/ziexB.

Üçüncü Bölüm: Dijital Mahremiyet Hakkının Kapsamı ve Bu Alandaki Filistin ile Ürdün Yasal Mevzuatının Anayasal İlkelere Uyumu

A. Dijital Mahremiyet Hakkının Kapsamı

Önceden de belirttiğimiz gibi internet ortamı, bireylerin kişisel verilerini toplaması, toplanan verileri depolaması, değiştirmesi ve aktarmasından dolayı mahremiyet hakkı ve kamu özgürlükleri için açık ve gerçek bir tehdit haline getirilmiştir. Söz konusu tehdit, özellikle kültürel, sosyal ve ticari faaliyetlerin fiziksel dünyadan sanal dünyaya taşınmasıyla endişe verici boyutlara ulaşmıştır. Bu gelişmelerin gölgesinde otoriteler, yeni ve çeşitli araçlara dayanarak bireyleri izleme ve bireylerin hareketlerini takip etme konusunda büyük güçler kazanmıştır. Bilgi sistemlerinin gelişmesi ve dijital alanın genişlemesi nedeniyle mahremiyetin hedef alınabileceği alanlar artmıştır. Böylece, günümüzde mahremiyet veya özel hayat haklarının kapsamı, artık sadece barınma, yazışma ve sağlık gibi maddi unsurlarla sınırlı kalmamış ve dijital mahremiyeti oluşturan yeni unsurları da içerecek şekilde genişlemiştir. İnternetin hala gelişmekte ve genişlemekte olduğunu ve dolayısıyla dijital mahremiyet hakkı kapsamı da genişlemeye devam ettiğini göz önüne serildiğinde dijital mahremiyet hakkının ihlal edilme olasılıkları artmaktadır. Bu bağlamda dijital mahremiyet hakkı kapsamının en önemli alanlarını aşağıda olduğu gibi özetleyebiliriz:

1. Kişisel Verilerin Korunması

Kişisel veriler, bilet rezervasyonu, dijital alışveriş, ev faturalarını ödeme veya devlet hizmetlerine erişim gibi bilgilerin sağlanmasını gerektiren dijital işlemler yoluyla işlenen tüm verilerdir. Böylece kişisel veriler, bir kimlik numarasına veya bir takım kişisel bilgiye dayanarak doğrudan veya dolaylı sıfatıyla bir kişinin kimliğinin tespit edilmesini sağlamaktadır. Ayrıca ATM yoluyla veya yaşanan hızlı dijital gelişme sayesinde bilgisayar ve akıllı cihazlar gibi yeni elektronik ortamlar aracılığıyla yapılan işlemlerde kişisel veriler kullanılmaktadır.[168] Bununla birlikte kişisel veriler iki türe ayrılmaktadır; birinci tür sayılar,

[168] Al-Ustath, a.g.e., s.429.

harfler ve simgelerden oluşan bir e-ticaret işlemini tamamlamak için gereken şifreler ile parmak izi ve iris gibi biyometrik veriler gibi kimliği belirleyen verilerdir. İkinci tür ise; etnik köken, siyasi görüş, dini inanç veya sağlık durumu gibi kişilerin özel hayatıyla ilgili özel nitelikli kişisel verilerdir. Bu verilerin kaynağı genellikle kamu ve özel kurumların veri tabanları ve çeşitli kuruluşların bilgi sistemleri olduğu gibi son yıllardaki gelişmelerle sosyal medya ağlarında paylaşılan bilgiler de bu kapsama girmiştir.[169]

Kişisel verilerin büyük çoğunluğu, veri tabanları ve bilgi sistemleri içinde depolanmaktadır. Böylece bilgi sistemlerinin; kişisel verilerin üretildiği, işlendiği, saklandığı ve paylaşıldığı alan olarak dijital mahremiyet hakkı kapsamına girdiğini söylemek mümkündür. Budapeşte Siber Suçlar Sözleşmesi'ne göre bilgi sistemleri, "Bir grup cihazın birbirine bağlantılı ve bağlı olması ve en az bir cihazın bir programa göre verileri otomatik olarak işlemesi" olarak tanımlamıştır. Bu bağlamda resmî kurumlar, e-devlet ve dijital kimlik gibi uygulamaların ortaya çıkmasıyla birlikte sunduğu hizmetlerin çoğu bilgi sistemleri üzerinden yürütmeye başlamıştır.[170]

Aynı zamanda ağ erişim verileri, otomatik olarak işlendiği hususunda benzer olan çok sayıda veriyi içeren en önemli kişisel verilerden biri olarak görülmektedir. Başlangıçta bağlantı verileri, 2006 yılında yayınlanan verilerin korunmasına ilişkin kapsamda Avrupa Birliği direktifine göre kişisel veri ağı içerisinde bulunamamıştır. Direktif, söz konusu verileri "bir internet bağlantısı veya iletişim hizmeti sonucunda elde edilen veya işlenen her veri" olarak tanımlamıştır. Bu veriler, ağ bağlantının kendisiyle ilgili olup bağlantının kaynağını ve sağlayıcısını tanımaya imkân verirken bir meta veri olarak iletişimin içeriğine değinmemektedir. Ağ erişim verileri, kişisel veriler olarak kabul edilip edilmediği ve dolayısıyla aynı yasal sisteme tabi olup olmadığı konusunda hukukçular ve anayasacılar

[169] Moufida Mubarakiya, "Alhimaya Alqanunia Lilhaqi Fi Alkhususia Alraqamia Fi Alqanun Aljazayirii" (TR: Cezayir Hukukunda Dijital Mahremiyet Hakkının Yasal Korunması), *Şeriat Ve Ekonomi Dergisi: Prens Abdul Qader İslami Bilimler Üniversitesi*, 7/13 (2018), ss.463-466.
[170] Mubarakiya, a.g.m., s.464.

arasında yoğun bir tartışma konusu haline gelmiştir. Bu bağlamda kişisel veriler, 1995 yılında yayınlanan kişisel verilerle ilgili Avrupa Parlamentosu direktifi etkisiyle ilk kez Fransız hukukunda ortaya çıkmıştır. Bu direktif, kişisel verileri "fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen gerçek bir kişiye (veri öznesine) ilişkin tüm bilgiler" olarak tanımlamıştır.

Kişisel verilerin bu tanımı, bahsettiğimiz gibi ağ erişim verilerinin kişisel veriler kategorisinde olup olmadığı konusunda hiçbir netlik kazanamamıştır. Bu yasal belirsizlik durumu, mahkemelere taşınan ve bu tanımları temel alan bir sürü davanın arka planında yasal uyuşmazlıklar yaratmıştır. Söz konusu tanıma harfiyen dayanan Fransız mahkemeleri ağ erişim verilerini kişisel veri olarak kabul etmezken Avrupa'da başka yargı mercileri farklı bir şekilde değerlendirmiştir. Belirsizlik durumu, Avrupa Parlamentosu 1995 tarihli Avrupa Direktifini yeniden gözden geçirmek için müdahale edene kadar devam etmiştir. Avrupa Birliği, 2016 yılında kişisel veriler kavramını cihazların dijital tanımlayıcısı olan İnternet Protokolü adresi (IP Adresi) dahil olmak üzere internet ağındaki bir kişinin kimliğinin belirlenmesine yol açan dijital verileri içerecek şekilde genişleten[171] 679 Sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nü (GDPR) kabul etmiştir.[172]

Konu ile ilgili Ürdün'de çeşitli yerel mevzuatlarda kişisel verilerin korunmasına değinilmediği gibi bu hakkı açık ve net bir şekilde koruyan bir yasal düzenleme bulunmamaktadır. 2015 Ürdün Siber Suçlar Yasası'nın 2. Maddesi bilgi sistemlerinin bir tanımını sunmuştur. Buna göre bilgi sistemleri, "verileri veya bilgileri elektronik yollarla inşa etmek, verileri göndermek, gönderilen verileri teslim etmek, işlemek, depolamak, yönetmek

[171] Hamza Ben Azza, "Alnizam Alqanuniu Libayanat Aliatisal Bishabakat Alintirnit" (TR: İnternet Bağlantı Verilerinin Hukuk Sistemi), *Siyaset Bilimi Ve Hukuk Dergisi, Arap Demokratik Merkezi,* 4/23 (2020), s.134.
[172] Samida, a.g.e., s.205.

veya elektronik olarak görüntülemek için kullanılan program ve araçlardır".[173] Buna rağmen söz konusu yasa, bilgi sistemlerine yetkisiz bir şekilde girme ve kişisel verileri kopyalama ihlallerini ele almamıştır. Ancak yasanın 3. maddesinde olduğu gibi bilgi sistemlerinin yasa dışı hacklenmesini bir suç olarak saymıştır. Aynı yasa, 2. maddesinde verileri "kendi içinde hiçbir anlamı olmayan sayılar, harfler, semboller, şekiller, sesler, görüntüler veya grafikler" olarak tanımlarken bilgiyi "işlenmiş ve anlamlı bir hale gelen veriler" olarak tarif etmiştir.[174] 2007 tarihli Ürdün Bilgi Edinme Hakkı Yasası, verilerin korunmasıyla ilgili bazı maddeleri içermiştir. Örneğin; yasanın 10. Maddesi, "Din, ırk, cinsiyet veya renk ayrımcılığına yol açacak kişisel bilgileri paylaşılmaz." olduğunu belirtmiştir. Aynı yasanın 13. maddesi de ilgili yetkililere bazı istisnalar dışında belirli bilgileri vermekten kaçınma hakkı tanımıştır. Bu bilgiler arasında çalışmamızın konusuna ilişkin veriler: "1) Kişilerin eğitim, sağlık ve kariyer kayıtları ile banka hesapları ve havaleleri. 2) Devlet daireleri ile posta, telgraf, telefon veya diğer teknik yollarla kişisel ve gizli nitelikteki yazışmalar ve bunlara verilen cevaplar"dan oluşmaktadır.[175]

Filistin mevzuatına gelince ise, internetteki kişisel verilerin korunmasını düzenleyen net bir yasa olmaması konusunda Ürdün mevzuatına benzemektedir. Filistinli yasa koyucu, Filistin Siber Suçlar yasasında bilgi sistemlerinin bir tanımını yapmamıştır. Ancak söz konusu yasanın 2. maddesinde geçiş verileri gibi kişisel verilerin bazı türlerine tanım getirmiştir. Yasa geçiş verilerini, "gönderim kaynağı, varış yeri, alınan rota, saat, tarih, hacim, süre ve iletişim hizmetinin türünü gösteren bilgi teknolojisi aracılığıyla oluşturulan herhangi bir sanal veri veya bilgi" olarak tanımlamıştır. Yasanın, 33. Maddesinde belirtildiği gibi geçiş verilerini sadece savcılığın siber suçlar bağlamında kullanıcıların verilerini el koyma hakkı kapsamında ele almıştır. Yasa, şifreyi şu şekilde tanımlamıştır: "Bilgi sistemlerine ve benzer teknolojilere erişmek ve kimliği doğrulamak için kullanılan her şey; böylece şifre, semboller

[173] 27 Sayılı 2015 Tarihli Qanun Aljarayim Al'iilikturunia (TR: Siber Suçlar Yasası), erişim 11 Aralık, 2021, https://2u.pw/7F4G7.
[174] Siber Suçlar Yasası, a.g.e.
[175] 2007 Tarihli Qanun Daman Haqi Alhusul Ealaa Almaelumat (TR: Ürdün Bilgi Edinme Hakkı Yasası), erişim 26 Aralık, 2021, https://2u.pw/6w3II.

ve parmak, göz ile yüz izlerini içeren geçişi verilerinin bir parçasıdır". Yasanın şifre tanımı, 26. maddesinde olduğu gibi, kullanmak amacıyla bir şifreyi sahip olan herkese ceza verilebildiği bağlamında dile getirmiştir.[176]

Yukarıdaki analizin sonucunda, Ürdün ve Filistin yasal sistemlerinin kişisel verilerin anayasal ve yasal anlamda koruma sağlamak konusunda hala geniş boşlukları olduğunu ve ikisinin mahremiyet hakkını açıkça savunan birçok bağlayıcı uluslararası anlaşmayı onayladıklarına rağmen kullanıcılar için gerçek koruma sağlayacak yasal düzenlemeler koymadıklarını söylemek mümkündür.

2. *İletişimin Mahremiyeti*

Günümüzde iletişim ve yazışmaların çoğu, e-posta, sosyal medya ağları ve cep telefonları başta olmak üzere teknolojinin sağladığı hizmetler aracılığıyla yürütülmektedir. Bu bağlamda kullanıcılara özel mesajları inceleme, yanıtlama ve arşivleme fırsatını sunan e-posta hizmeti, İnternet'te en yaygın kullanılan iletişim araçlarından biridir. Ancak diğer hizmetler gibi E-posta, mesajların hacklenme ve belirli programlar aracılığıyla içeriklerinin çalınma durumları mümkündür.[177] Ayrıca dijital mahremiyet hakkına yapılan sürekli ihlaller, aslında abonelik anlaşmaları aracılığıyla sistem içinde yer edinmiştir. Zira "internet aboneleri, öncelikle yetkili internet sağlayıcılarından geçmek zorunda olduğundan kullanıcıların sağlayıcılarla abonelik sözleşmelerini yapmalarını gerektirmektedir. Söz konusu abonelik sözleşmelerinde internet sağlayıcıları, genellikle mesajların içeriği ve ağ üzerinden iletilen her şeyden sorumlu olmadıklarını belirtmektedir. İnternet sağlayıcıları, sözleşmeyi tek taraflı olarak değiştirmek, ağ siteleri arasındaki hareketleri izlemek, elde edilen bilgileri sayfa yöneticilerine veya istatistik ve reklam şirketlerine aktarmak ve son olarak, isterlerse kullanıcıların mesajlarını okumak gibi yetkiler sağlayan maddeler de

[176] 10 Sayılı 2018 Tarihli Filistin Qarar Biqanun Bishan Aljarayim Al'iilikturunia (TR: Siber Suçlar İle İlgili Yasa Hükmünde Kararname), erişim 19 Aralık, 2021, https://2u.pw/76693.
[177] Ben Azza, a.g.m., s.126.

eklemektedir".[178] Teknolojinin internet üzerinden sunduğu iletişim hizmetleri, e-postada olduğu gibi yazılı mesajlar alışverişi ile yetinmeyip, Skype ve Zoom gibi uygulamalarla kullanıcıların internet üzerinden sesli ve görüntülü görüşme yapmalarını sağlayan hizmetlerle genişlemiştir. Bireylerin dijital mahremiyeti yeni farklı tehditlerle karşı karşıya olmaya başlamıştır.[179]

Son yıllarda sosyal medya siteleri, içeriğe erişim, düzenleme, yayınlama, değiştirme ve yorum yapmaya olanak sağlayan en önemli alanlardan birine dönüşmüştür. Böylece sosyal medya siteleri, "ortak ilgi alanlarına sahip kullanıcıların ücretsiz bir şekilde hesap oluşturarak siteye katılmalarını sağlayan çevrimiçi iletişim platformları" olarak tanımlanabilmektedir. Zamanla bu siteler, artık sadece iletişim kurmak ve arkadaş bulmak için kullanılmaktan ziyade birçok özellik sunan ve reklamlarla kâr amacı güden siteler haline gelmiştir. Facebook örneğinde olduğu gibi bu siteler, siyasi hareketlerde ve seçimlerde aktif bir şekilde de kullanılmıştır. Dijital dünyanın devam eden hızlı gelişmeleriyle birlikte özellikle özel hayat gizliliğinin çiğnenmesi ve mahremiyetin ihlal edilmesi gibi sosyal medya ağlarında meydana gelen ihlaller, çeşitli endişeler gündeme getirmektedir.[180]

Son zamanlarda sosyal medya ağları, özellikle siyaset alanında bireyler ve siyasi eğilimleri hakkında bilgi toplamak için sık sık kullanılmanın yanı sıra dünyanın farklı yerlerinde yapılan seçimlerinde seçmenleri etkilemek için önemli bir araç haline gelmiştir. Örneğin; Facebook, 2016 ABD seçimlerinde milyonlarca kullanıcıyla ilgili kişisel bilgilerini eski Başkan Donald Trump'ın seçim kampanyasıyla bağlantılı Cambridge Analytica şirketine sızdırmakla suçlanmaktadır.[181] Ayrıca son aylarda sosyal medya ağları, özellikle Facebook

---

[178] Mamdooh Bahr, *Himayat Alhaya Alkhasa Ela Alintirnti: Dirasa Muqarana (TR: İnternette Özel Hayatın Korunması: Karşılaştırmalı Bir Çalışma),* 1.b., Kahire: Dar Al-Nahda Al-Arabiya, 2020, s.70.
[179] Bahr, a.g.e., s.70.
[180] Ben Azza, a.g.m., s.118.
[181] "Fadihat Kambiridj 'Analitika: Fis Buk Takshif 'Ana Tasrib Albayanat 'Adar Bi87 Milyun Mustakhdam" (TR: Cambridge Analytica Skandalı: Facebook, Veri Sızıntısının 87 Milyon Kullanıcıyı Etkilediğini Duyurdu), France 24, erişim 08 Nisan, 2022, Https://Bit.Ly/3dpiwcn.

ve Instagram gibi sitelerdeki Filistinli ve Filistin'i destekleyen içeriklere yönelik birçok saldırı düzenlemiştir. Konu ile alakalı birkaç rapor, Facebook'un İsrail otoriteleriyle Filistinlileri izlemek ve Filistin mahremiyetini ihlal etmek için iş birliği yaptığını belirtmiştir.[182]

Dünyanın yasal sistemlerinin çoğu, iletişim ve yazışmaların herhangi bir şekilde çalınmasını veya dinlenmesini suç saymasına rağmen birçoğu, devletin ve toplumun güvenliğinin korunması ve ulusal güvenliği korumak adına suçlarla mücadele edilmesi ile ilgili hususlar için özel konuşmaların izlenmesine izin verdiği için, konuşmaların mahremiyetine kısıtlamalar getirmektedir. Bu bağlamda terör olaylarının, uyuşturucu kaçakçılığının ve insan ticareti suçlarının yayılması nedeniyle bazı hukukçular, casusluk, gözetleme ve dinleme operasyonlarının yasallığını kişisel bilgilerden elde edilen kanıtların kapsamının sınırlı kalması ve istisnai kullanım için olması şartıyla savunmaktadır. Diğer taraftan ise bazı hukukçular bu izleme ve gözetleme operasyonlarını reddetmekte ve özel hayatın en önemli unsuru olan özel görüşmenin mahremiyeti ihlal edildiğini vurgulayarak casusluğun insan hakları ihlali olduğunu ileri sürmektedir.[183]

Örneğin, ABD Anayasası'nın Dördüncü Değişikliği, makul bir mahremiyet beklentisine sahip olmayan halka açık yerlerde gerçekleşse bile bireylerin konuşma mahremiyetinin korunma hakkını tüm kabul edilemez müdahalelere karşı savunmaktadır. Bu nedenle ABD Yüksek Mahkemesi, telefon konuşmalarını gözetlemenin ciddi bir özgürlük ihlali olduğuna karar vermiştir. Amerikan mevzuatının aksine Fransız yasa koyucu, eski ceza yasasında kişisel konuşmaların korunmasını özel bir yer kriteri ile ilişkilendirmiştir. Başka bir deyişle eski Fransız Ceza Yasası, halka açık bir yerde konuşulduğunda konuşmacıların kendi özel hayatının sırları hakkında başkalarının bilgisi olmasına rıza gösterdiğine dair yasal bir

[182] Anan Abushanab, "Israel's Control Of The Palestinian ICT Infrastructure And Its Impact On Digital Rights", *The Arab Center For Social Media Advancement*, (2018), s.16.
[183] Bojdin, a.g.m., s.66.

karinenin mevcudiyeti olduğunu kabul etmiştir. Böylece Fransız mevzuatı, özel ve kamusal konuşmaları ayırt etmek için özel yer kriterini belirlemiştir. Ancak yeni Fransız Ceza Yasası, halka açık bir yerde gerçekleşse bile konuşmaları dinlemeyi, kaydetmeyi veya çalmayı suç saymıştır.[184]

Aynı şekilde Ürdün anayasası, telefon konuşmalarının yargı emri olmadan dinlenemeyeceği veya toplanamayacağı şartını koştuğu gibi Ürdün Ceza Yasası, aramalara veya herhangi bir iletişim türüne her türlü saldırı veya casusluk eylemini suç sayan çeşitli hükümler içermiştir.[185] Filistin yasal sisteminde ise İletişim Yasası, iletişim ağları aracılığıyla bir mesajı çalan, engelleyen veya ifşa eden herkesi cezalandırmıştır.[186] Buna rağmen hem Ürdün hem de Filistin yasal sistemleri, telefon aracılığıyla yapılan iletişimleri incelemekle yetinmiş ve modern iletişim araçlarını ele almamıştır.

3. Unutulma Hakkı

Bu hak, sanal dünyanın çeşitli sitelerinde kullanılan kişisel verilerle ve bunların akıbeti ile ilgili tartışmalarından doğmuştur. Bu hak, kullanıcıların kendileri paylaşmış olsun ya da başkaları tarafından yayınlanmış olsun, özel hayatlarıyla ilgili bilgileri içeren ve kullanıcıların mahremiyetine zarar verebildiği gibi geleceklerine, ailelerine ve mesleki hayatlarına olumsuz sonuçları olabilen linkleri ve bilgileri internetten kaldırma olanaklarını sağlamaya amaçlamaktadır. Aslında bu hakkın fikri, bireyin yaşamının bir döneminde yaptığı hatalar veya verdiği bilgiler ne olursa olsun, internetteki herkes tarafından erişilebilir kalmasını istemeyebildiği gibi silinmesini ve bir daha hatırlatılmamasını talep edebildiği temeline dayanmaktadır. Unutulma hakkının tesis edilmesi için bu temellerden yola çıkarak çalışmalar başlatılmışken özellikle ağ erişim verileri bağlamında bu hakkı koruyabilecek ve

[184] Lami, a.g.e., s.76.
[185] Aldustur Al'urduni (TR: Ürdün Anayasası), erişim 07 Ekim, 2021, https://2u.pw/hp9Uq.
[186] Alqanun Al'asasi Alfilastini (TR: Filistin Temel Yasası), erişim 14 Aralık, 2021, https://2u.pw/X0CSY.

uygulayabilecek mekanizmalar oluşturmak adına hukukçular tarafından çeşitli sorular ortaya atılmıştır.[187]

Bu mekanizmaların en önemlisi, dijital web siteleri operatörleri için zorunlu olan ve unutulma hakkının etkinleştirilmesi için en önemli araçlardan biri olduğu için dijital unutulma hakkı ile eş anlamlı kabul edilen dijital silinme hakkıdır. Öte yandan, düzeltme hakkı, işlemeyi sınırlama hakkı ve sınıflandırmadan çekilme hakkı da dahil olmak üzere dijital unutulma hakkının güçlendirilmesine zemin hazırlayan başka mekanizmalar da bulunmaktadır. 2016 yılında yayınlanan Avrupa Direktifinin (GDPR) 17. maddesinde unutulma hakkı, silinme hakkı ile şart koşulmuştur. Söz konusu madde, bireyin kişisel verilerinin silinmesi için bir talepte bulunabileceğini ve ağ sorumlularının bunları silmekle yükümlü olduğunu belirtmiştir. Ancak söz konusu direktif, bu hakkı toplanan kişisel verilerin amaçlara ulaşmak için artık gerekli olmadığı durumlar gibi belirli sınırlarla kısıtlamıştır.[188]

Avrupa direktifinin yürürlüğe girmesinden sonra Fransız yasa koyucu, Bilişim ve Özgürlükler Yasasının 40. maddesini değiştirmiştir. Böylece değiştirilmiş madde, "kimliğini kanıtlayabilen herhangi bir gerçek kişi, durum ne olursa olsun, verileri işleyenlerden, özellikle yanlış, eksik, muğlak ve güncelliğini yitirmiş olan veya kullanılması, iletilmesi ve kaydedilmesi yasak olan kişisel verilerin düzeltilmesi, güncellenmesi, etkisizleştirilmesi, güvence altına alınması veya silinmesi gibi taleplerde bulunabilir" şeklinde düzeltilmiştir. Arap dünyasına gelince Cezayir anayasası, özellikle 2016 yılında yapılan değişikliklerle kişisel verilere özel önem vermiştir. Buna ilaveten Cezayir, Haziran 2018 tarihinde kişisel verilerin işlenmesi alanında gerçek kişilerin korunmasına ilişkin özel bir yasa çıkarmıştır. Dijital unutulma hakkının en önemli garantörü olarak silinme ilkesine açıkça atıfta bulunmamasına rağmen söz konusu yasa, 35. maddesinde bireylerin işlenmesi hukuka uygun

[187] Ben Azza, a.g.m., s.124.
[188] Ben Azza, a.g.m., s.127.

olmayan kişisel verilerin verileri işleyenlerden ücretsiz olarak güncellemesini, düzeltmesini, kapatılmasını veya silinmesini talep edebileceğini ileri sürmüştür.[189]

Ayrıca 0409 sayılı Bilgi ve İletişim Teknolojilerinin Tehditlerini Önlenmeye İlişkin Yasa'nın 11. Maddesi, hareketlere ilişkin verilerin -yani ağ erişim verilerinin- veriliş tarihinden itibaren bir yılı geçmemek üzere saklanacağı hükmünü içermiştir. Bu hüküm, ağ erişim verilerinin belirsiz bir süreyle saklanamayacağını ve belli bir süreden sonra silineceğini ima etmiştir.[190] Ürdün'de Kişisel Verileri Koruma Yasası Tasarısı- tezin yazıldığı tarihe kadar onaylanmamış- unutulma hakkını öngörmektedir. Zira tasarının son versiyonundaki 20. Madde, ilgili kişinin, kendisi ile ilgili işlenen kişisel verilerin silinmesini veya kimliğinin saklanmasını talep etme hakkına sahip olduğunu ve veri işlemekten sorumlu tarafların gereken gerekçeler oluştuğunda bu talebi uygulamakla yükümlü olduklarını belirtmiştir. Ancak Ürdünlü yasa koyucu, Fransız yasa koyucu ve Avrupa direktifinin aksine silinme hakkını sınırsız kılmamış ve birinin meydana gelmesi şartıyla silinme hakkını meşrulaştıran bir dizi gerekçeyle düzenlemiştir.[191]

Bu gerekçeler: A) Kişisel verilerin toplanma amacı dışında bir amaç için işlenmesi. B) İlgili kişinin kendi kişisel verilerinin işlenmesine ilişkin onayını geri çekmesi. C) kişisel verilerin yasa dışı bir şekilde işlenmesi. D) İşlemeden sorumlu tarafın yasal veya sözleşmeden doğan bir yükümlülüğünün yerine getirmesi için kişisel verilerin silinmesinin gerekli olması. Aynı maddenin C bendi de unutulma hakkını yasa tasarısının 15. maddesinde belirtilen istisnalar ile kısıtlamıştır. Ayrıca yasa tasarısının 18. maddesi, kişisel verilerin düzeltilmesini talep etme, onları güncelleme ve erişme hakları gibi unutulma hakkına destekleyici farklı mekanizmalar öngörmüştür.[192] Filistinli yasa koyucuya gelince, bu hakka hiçbir yasasında değinmemiştir. Aynı zamanda sivil toplum örgütleri ile insan hakları aktivistlerinin eksiksiz

[189] Bahr, a.g.e., s.81.
[190] Bojdin, a.g.m., s.62.
[191] Ben Azza, a.g.m., s.149.
[192] Muswadat Qanun Himayat Albayanat Alshakhsia (TR: Kişisel Verileri Koruma Yasası Tasarısı), erişim 14 Aralık, 2021, https://2u.pw/UrcWK.

bir veri koruma yasasının çıkarılması için çağrıda bulunmasına rağmen Filistin Yönetimi, kişisel verilerin korunmasına ilişkin bir yasa çıkarma niyeti olmadığı görünmektedir.[193]

B. Ürdün ve Filistin'deki Dijital Mahremiyetle İlgili Yasaların Anayasal İlkelere Uyumu

Ürdün ve Filistin yasal sistemlerinde dijital mahremiyet ve kişisel verilerin korunması ile ilgili özel yasalar yoktur. Ancak bu konuyla ilgili birkaç yasaya dağılmış bir dizi yasal hüküm vardır. Aynı zamanda Ürdün ve Filistin ceza yasaları, gelişmiş yeni iletişim araçları ve bunların kullanımları ile ilgili mahremiyeti ele almamıştır. Bu bağlamda Siber Suçlar Yasası ve İletişim Yasası gibi yasalar, genel anlamda mahremiyetin bazı meselelerini ele alan ve iki ülkedeki dijital mahremiyete değinen yasalardan görülmektedir. Bu kısımda, bu metinlerin en önemlilerini ele alarak uyumluluk ve aykırılık açısından anayasal ilkelerle ilişkisini tartışacağız ve Ürdün ve Filistin mevzuatındaki siber suçlar yasalarına daha ayrıntılı bir şekilde inceleyeceğiz.

1. Ürdün'deki Dijital Mahremiyetle İlgili Yasaların Anayasaya ve Anayasal İlkelere Uyumu

1.1 Dijital Mahremiyet Hakkının Ürdün Mevzuatındaki (Yasal) Ele Alınışı

Aşağıda dijital mahremiyet hakkının çeşitli kapsamlarıyla ilgili maddeler içeren Ürdün mevzuat ve yasaları incelemeye alacağız. Ayrıca bu maddelerin dijital mahremiyeti koruyan Ürdün anayasasında yer alan güvencelerle ne ölçüde uyumlu olduğunu inceleyeceğiz. Aynı zamanda bu maddelerin mahremiyet hakkı kavramında meydana gelen hızlı gelişmeleri ve bunun modern gelişimini ne ölçüde dikkate aldıklarına değineceğiz.

-Kişisel Verileri Koruma Yasası Tasarısı: 2014 yılında İletişim ve Bilgi Teknolojileri Bakanlığı (şu anda Dijital Ekonomi ve Girişimcilik Bakanlığı), gerçek kişilerin kişisel

[193] Khamis ve Khalil, a.g.m., s.11.

verilerini yasa hükümlerine bağlı ilgili kuruluşlar tarafından gereken yasal korumanın sağlanması ve dijital ortamda ile çeşitli uygulamalarında güvenin artırılması amacıyla kişisel verileri koruma yasası tasarısını geliştirmeye çalışmıştır. O dönemde yasanın ilk tasarısı genel istişareye sunulmuştur. Bahsi geçen istişareyi yorumlayan bazı aktivistler, uzmanlar, hukukçular anları ve sivil toplum kuruluşları katılmıştır. İkinci aşamada bakanlık, aldığı görüş ve yorumlara dayanarak yasa tasarısı üzerinde bazı değişiklikler yapmıştır. 2017 yılında ilgili makamlarla istişarelerde bulunmak üzere yeniden gündeme getirmiştir. Ardından Dijital Ekonomi ve Girişimcilik Bakanlığı, yasa metninin dördüncü tasarısını sunmuştur.

Söz konusu yasa tasarısı, dijital verilerin korunmasına ilişkin bazı uluslararası standartlara uymuştur. Örneğin; yasa tasarısının 14. maddesi, verileri kontrol eden tarafın veri sahibinin verilerini kullanmak için önceden açık yazılı veya elektronik onayını alması gerektiğini ve 16. maddede belirtildiği gibi kullanıcının bu onayını istediğinde çekebildiğini öngörmüştür. Bu bağlamda eğer verileri kontrol eden tarafın bu kurallara uymazsa yasal sorumluluğa tabi olacağı belirtilmiştir. Ayrıca yasa tasarısının 21. maddesi, verileri kontrol eden tarafın veriler üzerinde gerçekleştirmeyi planladığı işlemlerin amacı, süresi ve bu verilerin paylaşılacağı üçüncü kişiler dahil olmak üzere farklı ayrıntıları açıklamasını zorunlu kılmıştır.[194]

Yasanın uygulanmasını sağlamak ve veri sahiplerinden gelen şikayetleri almak amacıyla "Kişisel Verileri Koruma Kurulu" adı altında yasayla bir kurul oluşturulması öngörülmüştür.[195] Bu kurul, kişisel verilerin korunmasına ilişkin politikaları oluşturmak ve

[194] Muswadat Qanun Himayat Albayanat Alshakhsia (TR: Kişisel Verileri Koruma Yasası Tasarısı), erişim 14 Aralık, 2021, https://2u.pw/UrcWK.

[195] Önerilen Kurulun Yapısı Şunlardan Oluşur: Başkan Olarak Bakan, Bakan Tarafından Atanan Veri Koruma Komiseri, Temsilciler Meclisi Hukuk Komitesinin Başkanı, Ulusal İnsan Hakları Merkezi Mütevelli Heyeti Başkanı, İnsan Hakları Genel Komiseri, Bilgi Edinme Hakkını Güvence Altına Alma Yasası Gereği Görevlendirilen Bilgi Komiseri, Güvenlik Kurumlarından İki Üye ve Kişisel Verilerin Koruması Alanında Deneyimli ve Uzman 3 Üye. Muswadat Qanun Himayat Albayanat Alshakhsia (TR: Kişisel Verileri Koruma Yasası Tasarısı), erişim 14 Aralık, 2021, https://2u.pw/UrcWK.

onaylamak, veri kullanma onayını alma, onayı geri çekme ile ilgili prosedürler için talimatlar yayınlamak, yayınlanan talimatla kişisel verilerin aktarımı ve değişimi için izinler çıkartmak, veri işlemesinden sorumlu taraflara karşı yapılan şikâyet ve taleplerin karara bağlanması için mekanizmaları kurmak ve gerekli işlemlerin yapılması gibi bir sürü görevle görevlendirilmiştir. Aynı zamanda yasa tasarısının 4. maddesi, Dijital Ekonomi ve Girişimcilik Bakanı'nın kurula başkanlık etmesini ve kurulun güvenlik kurumlarından iki üyenin bulunmasını önermiştir.[196]

Daha önce hükümetten ve bakanlıklardan daha fazla sayıda temsilci içeren kurulun öneri ve yorumlardan sonra yeniden yapılandırılma sürecine girmiş olsa da dernekler ve sendikalar gibi sivil toplum kuruluşlarının temsilcilerinin olmaması ve tüm üyeleri hükümet tarafından atanan bir denetim organına dönüşmesi gibi nedenlerle kurulun bağımsızlığı konusunda hala bazı endişeler bulunmaktadır. Zira bu durum, Dijital Ekonomi ve Girişimcilik Bakanlığı'nın gerçekleştirmeye çalıştığı hedefler arasında çıkar çatışması oluşturabilmektedir. Bununla birlikte kurulun güvenlik kurumlarından iki üyesinin olması, kurulun şimdi önerilen yapısıyla faillerin özelde güvenlik kurumları ve genelde yürütme organı olması halinde mahremiyet ihlali şikayetlerini soruşturulup soruşturulamayacağı konusunda şüphe uyandırmaktadır. Bu durum, dijital mahremiyet hakkı konusunda tam yetkilendirilmiş bir kurulun kuruluşu için bağımsızlık şartını ön plana koyan veri koruma ile ilgili küresel yasa ve direktiflerin önerdiği en iyi uygulamalara zıttır.

Öte yandan yasa tasarısı, güvenlik kurumları veya tasarının gibi bazı tarafların veri sahiplerinin onayı ve yargı makamların emri olmadan "güvenlik gerekçeleri" gibi geniş istisnalarla verilere el koyulmasına izin vermektedir. Aynı istisnalar, yasa tasarısının 15. maddesinde belirtildiği gibi başsavcılara da tanınmıştır.[197]

[196] Muswadat Qanun Himayat Albayanat Alshakhsia (TR: Kişisel Verileri Koruma Yasası Tasarısı), erişim 14 Aralık, 2021, https://2u.pw/UrcWK.
[197] Kişisel Verileri Koruma Yasası Tasarısı, a.g.e.

Kişisel Verileri Koruma Kurulu'nun bağımlılığı ve yasa tasarısında olan veri ifşasına ilişkin geniş istisnalar, Kişisel Verileri Koruma Yasası'nı uygulamak durumları dahilinde ana hedef ve amaçlarına ulaşmak için önemli bir engel oluşturmaktadır. Ayrıca bu anlayış, Kişisel Verilerin Korunmasına İlişkin Avrupa Direktifi[198] ve Asya-Pasifik Ekonomik İşbirliği ilkeleri[199] gibi kişisel verilerin korunmasına ilişkin küresel uygulamalarla açıkça çelişmektedir. Aynı zamanda kişisel verilerin tanımlanması durumunda yasanın öngördüğü istisnaların azaltılması, veri türleri arasında hassasiyetlerine göre ayrım yapılması -yasa tasarısının hassas veri tanımı, hassas veri türleri arasında biyometrik verileri açıkça içermemektedir- veri işlemesine ilişkin düzenleyici kısıtlamaları özel sektörün vatandaşların verileriyle yaptığı işlemlerle sınırlanmayıp kamu sektörünün verileri yasa kapsamına dahil edilmesi gerekmektedir. Bu bölümün yazıldığı tarihe kadar, söz konusu yasa tasarısı henüz onaylanmamış ancak 2021 yılının mart ayında, Mevzuat ve Görüş Kurulu bu yasa üzerindeki çalışmalarını bitirerek onaylanması için anayasal prosedürleri takip etmesi için hükümete göndermiştir.[200]

Bununla birlikte önerilen yasa tasarısı, bilgi teknolojisinin yaygın kullanımından gittikçe gündeme gelen ve dijital hakların önemli bir parçası olan unutulma hakkını da kapsamaktadır. Aslında bu hak, vatandaşlara kişisel verilerini ve belirli bir hizmet veya araç tarafından toplanan bilgilerini çevrimiçi olarak istedikleri zaman silme ve yok etme hakkı vermektedir. Bu bağlamda Avrupa Adalet Divanı'nın Google-İspanya (Google Spain)[201] davasında verdiği karardan sonra Ürdün'de Avrupa Birliği ile unutulma hakkı ile ilgili

[198] Directive Of The European Parliament On The Protection Of İndividuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, Eur-Lex, erişim için: https://2u.pw/uVD90
[199] OECD Privacy Principles, Organisation for Economic Co-operation and Development, erişim 19 Ekim, 2021, https://2u.pw/w69LG.
[200] Halid Al-Kuda, "Eabir Lilhudud Bi'athar Rajei: Al'urduni Yadfae Biqanun Lihimayat Albayanat Alshakhsia" (TR: Sınırları Geçen ve Geriye Dönük Etkili Bir Yasa: Ürdün Kişisel Verileri Korumak İçin Bir Yasa Hazırlıyor), Al-Rai, erişim 09 Mayıs, 2022, https://2u.pw/eQqUO.
[201] Nader Salha, "Digital Rights Mapping In The MENA Region", *The Arab Center For Social Media Advancement*, (2021), s.13.

görüşmeler yapılmıştır. Kişisel verileri koruma yasası tasarısı, unutulma hakkını, ilgili kişinin kişisel verilerini silmesine veya saklamasına olanak tanımak olarak tanımlamakta ancak bu hakkı yukarıda da belirtildiği gibi 15. Madde ile getirilen istisnalarla da sınırlandırmaktadır.

-Ceza Yasası: Ürdün Ceza Yasası, ikinci bölümde namus ve özgürlüklere karşı suçlar bağlamında özel hayata saldırı suçlarını ele alınmıştır. Bu bağlamda Ürdünlü yasa koyucu, 347. maddede konut dokunulmazlığının ihlali ile ilgili farklı hükümler içermiştir. Örneğin: sahibinin izni olmadan başkasının konutuna giren herkesi en fazla altı ay hapis cezası ile cezalandırmıştır. Ayrıca söz konusu konut ihlalinin şiddeti kullanarak geceleyin ve birden fazla kişi tarafından meydana geldiğinde madde, suçu işleyenleri bir aydan bir yıla kadar hapis cezasını vermektedir. Aynı zamanda 348. madde, kişinin veya ailenin sırrı olan her şeyi temsil eden özel hayatı ihlal suçunun altı ayı geçmemek üzere hapis ve iki yüz Ürdün dinarı para cezası ile cezalandırılmasını öngörmüştür. Ayrıca aynı madde, ihlalin tekrarı durumunda cezanın daha ağırlaştırılacağını belirtmiş ve "ses kaydı yapma, fotoğraf çekme veya dürbünle izleme dahil olmak üzere her ne suretle olursa olsun gizlice dinlemek veya izlemek suretiyle başkalarının özel hayatına tecavüz eden kişi, mağdurun şikâyeti üzerine altı aydan az üzere hapis ve iki yüz Ürdün dinarı para cezası ile cezalandırılır: İhlalin tekrarı halinde ceza iki kat artırılır" hükümlerini vurgulamıştır.

Yasanın 355. maddesine gelince, kişi veya ailelerin hayatlarına ilişkin kişisel verilerin yayınlanmasını hapis ve para cezası ile cezalandırılabilecek bir suç olarak kabul edilmiştir. Zira söz konusu madde aşağıdaki durumlarda;

1. Görevi veya resmi konumu nedeniyle resmi sırları elde edenler ve bu sırları, bunlara erişme yetkisi olmayanlara veya kamu yararına uygun olarak iş doğası gereği böyle bir erişimi gerektirmeyen kişilere verenler için,
2. Resmi bir işi veya devlet hizmetini ifa ederken gizli belgeler, çizimler, planlar, formlar veya bunların kopyalarını tutma hakkına sahip olmadan veya işinin doğası gereği gerektirmeden bulunduranlar için,
3. Mesleği gereği bir sırrın farkında olup haklı yasal bir sebep olmaksızın ifşa edenler için,

3 yılı geçmemek üzere hapis cezası hükmünü içermiştir.

Bu madde, bireylerin özel hayatlarını korumak için önemli bir maddedir. Ancak aynı zamanda söz konusu madde, kamu sektörüne aşırı bilgi toplama yetkisine yasal bir temel sağlamıştır. Zira madde, toplumu suçlardan koruma bahanesi ile belirli taraflara toplanması yasaklanan bilgilerin toplamalarına izin vererek özel hayatla ilgili kamu kurumları tarafından kanunen elde edilen gizli bilgiler nedeniyle bireyleri karşı koyamadığı otoritelerin elinde bir rehin haline getirmektedir.[202]

Aynı şekilde Ürdün Ceza Yasası'nın 356. maddesi, "Telefon İşleri Dairesi'nde işi ve konumu gereği ulaştığı bir telefon görüşmesini ifşa eden kişiye altı ay hapis cezası veya yirmi Ürdün dinarına kadar para cezası uygulanır" hükmünü içermektedir. Bununla birlikte yasanın 357. maddesi, "Kendisine gönderilmeyen bir mektubu veya telgrafı kasten imha eden veya açan kişi beş Ürdün dinarı geçmemek üzere para cezası ile cezalandırılır" hükmünü vermiştir.[203]

Yukarıdaki maddelere baktığımızda, Ürdün ceza mevzuatının dijital mahremiyetin özel doğasını ve internet üzerinden özel hayatın ihlalini dikkate almadığını, hiçbir maddesinde yeni iletişim araçlarını ve kişisel verilerin korunmasını doğrudan ele almadığını görüyoruz. Bu nedenle Ürdünlü yargı ve hukuku sistemi, bir mektubu kasten imha etmek veya açmak gibi fiziksel davranışlarla ilgilenen Ceza Yasası'nın geleneksel metinlerine dayanmış ve dolayısıyla modern dijital iletişim şekillerini suç kapsamının dışında bırakmıştır. Ancak iletişim yasası gibi diğer yasal metinlerinde dijital iletişim ile ilgili bazı detayları bulabiliyoruz. Sonuç olarak kapsamlı bir incelemeden sonra Ürdün Ceza Yasası'nın ülkede

[202] Lami, a.g.e., s.49.
[203] 1960 Tarihli 16 Sayılı Qanun Aleuqubat Al'urduni (TR: Ürdün Ceza Yasası), erişim 23 Ekim, 2021, https://2u.pw/GFIb0.

anayasal ilkelerle uyumlu olduğu ancak çağın doğası ve dijital mahremiyetle ilgili yasal ve anayasal sorunlarla uyumlu olmadığı söylemek mümkündür.

-İletişim Yasası: Bu yasa, mahremiyet hakkına ilişkin ancak çoğu telefon görüşmeleri ve bunların dinleme eylemleri ile ilgili ilgili, çeşitli maddeler içermektedir. 56. Madde, "telefon görüşmeleri ve özel iletişim, yasal sorumluluk altında ihlal edilemeyecek gizli hususlar olarak kabul edilir" hükmünü belirtmiştir. Ancak bu madde, geleneksel iletişimle ilgili mahremiyeti korumasına rağmen, dijital ve elektronik iletişim araçlarına açık bir atıfta bulunulmamıştır. Ayrıca yasanın 71. maddesi, "konumu gereği gördüğü veya hukuki dayanağı olmaksızın kaydettiği herhangi bir iletişimin içeriğini veya telefon mesajını bir kamu veya özel iletişim ağı aracılığıyla paylaşan veya yayan kişi, bir aydan bir yıla kadar bir hapis cezası, 100 Ürdün dinarından 300 Ürdün dinarına kadar para cezası veya her ikisi ile cezalandırılacağını" hükmünü içermiştir. Bununla birlikte yasa, bir mesajın içeriğini silme, ele geçirme ve hatta bu eylemi teşvik etme ihlali için bir ceza öngörmüştür.

Anayasanın 76. Maddesine göre, "iletişim ağları aracılığıyla bir mesajın içeriğini ele geçiren, engelleyen, değiştiren veya silen ya da başkalarını bu eylemi gerçekleştirmeye teşvik eden kişilerin bir aydan az ve altı aydan fazla olmamak üzere hapis cezası veya 50 Ürdün dinarından az ve 220 Ürdün dinarından fazla olmamak üzere para cezası veya her ikisi ile cezalandırılır".[204] 77. Madde ise, "İletişim ağları üzerinden başka bir kişiye iletmesi gereken bir mesajı gizleyen, kopyalayan, ifşa eden veya açıklanmayan telefon numaraları ve gönderilen veya alınan mesajlar dahil olmak üzere abonelerden birine ait verileri ele geçiren kişi ya da iletilmesi talep edilen mesajların iletilmesini reddeden ruhsat sahibi veya kurum altı ayı geçmemek üzere hapis veya bin Ürdün dinarını geçmemek üzere para cezası veya her ikisi ceza ile cezalandırılır" hükmünü içermiştir.

[204] 1995 Tarihli ve 13 Sayılı Qanun Alaitisalat Al'urduni (TR: Ürdün İletişim Yasası) ve Değişiklikleri, erişim 19 Ekim, 2021, https://2u.pw/ru11b.

Bu maddelerin incelenmesiyle, özellikle anayasanın 18. Maddesi başta olmak üzere anayasa maddelerindeki hükümlerle uyumlu olduğu ancak hala yeni iletişim araçları ve internet gibi hususları ele alınmaması dahil birçok sorun olduğunu görüyoruz. Ayrıca bu yasanın önemli başka bir sorunu, İletişimin mahremiyetini geleneksel bir şekilde yorumlayarak koruması ve telekomünikasyon şirketlerinin elinde bulunan İnternet'in devasa kişisel verileri görmezden gelmesidir. İletişim Yasası'nın 29. maddesinin G bendi uyarınca, internet servis sağlayıcılarının iletişimi denetlemeye ilişkin adli ve idari talepleri yerine getirmek için gerekli kolaylıkları sağlaması ruhsat verme koşullarından bir tanesi olarak düzenlemiştir. Bu bende göre, "ruhsat sahipleri, iletişimi denetlemeye ilişkin adli ve idari talepleri yerine getirmek adına ilgili taraflara gerekli kolaylıkları sağlamasını gerekir".

Ancak Ürdün Anayasası'nın 18. maddesi, iletişimleri takip etme sürecini sadece yasa hükümlerine göre yargı kararının alınmasıyla sınırlandırmasına rağmen bu hüküm, denetimi düzenleyen ve vatandaşların mahremiyetini sağlayan mevzuat ve yasalara çevrilmemiştir. Örneğin: Dijital iletişimle ilgili olarak kolluk kuvvetlerinin ve istihbarat teşkilatlarının yetkilerini özel olarak düzenleyen herhangi bir yasa bulunmamaktadır.[205] Ayrıca denetim yetkileri, mahremiyet hakkıyla ilgili anayasal standartlara uygun olarak yasayla açıkça tanımlanması gerekmektedir.[206]

-Medeni Yasa: Ürdünlü yasa koyucu, Medeni Yasa'nın 48. Maddesinde, "Kişilik haklarından birine hukuka aykırı bir saldırıya uğrayan herkes, bu saldırının durdurulmasını ve uğradığı zararın tazmin edilmesini isteyebilir" hükmünü bulundurmuştur.[207] Bu metinde yasa koyucu, özel hayat dahil olmak üzere kişisel haklardan herhangi birine yönelik herhangi

[205] "Surveillance And Data Protection İn Jordan", Internet Legislation Atlas, erişim 11 Ocak, 2022, https://2u.pw/8axFJ.
[206] Salha, a.g.m., s.13.
[207] 1976 Tarihli ve 43 Sayılı Alqanun Almadani Al'urduni (TR: Ürdün Medeni Yasası), erişim 07 Nisan, 2021, https://2u.pw/SqIT8.

bir saldırıyı kapsayan genel bir dil kullanmakta ve herhangi bir saldırıya maruz kalan herkes için tazminat hakkına yer vermektedir.

-Ceza Muhakemeleri Usulü Yasası: Bu yasa, başsavcının kişilerin mesajlarını veya aramalarını denetlemeye ne zaman karar verme yetkisine sahip olduğu belirtmektedir. 88. maddede, "başsavcı, gerçeği ortaya çıkarmak için faydalı olduğu zaman posta ofislerindeki tüm mektuplar, gazeteler, yayınlar ve paketlerin yanında telgraf ofislerindeki tüm telgraf mesajlarına da el koyabilir ve aynı zamanda telefon konuşmalarını denetleyebilir" hükmü geçmektedir. Bu madde, Ürdün Anayasası'nın yazışma ve telefon görüşmelerinin mahremiyetini koruma altına alan ve yargı kararı olmadan ele geçirilmelerini yasaklayan 18. maddesi ile uyumludur.

-Suçu Önleme Yasası: Mahkeme kararıyla masum olmalarına rağmen valiye insanları idari olarak tutuklama yetkisini veren bu yasa, Ürdün'deki hukuk çevreleri arasında en tartışmalı yasalardan biridir. Ayrıca yasa, valinin bazı kullanıcıların telefon konuşmalarına el koymasını ve bunları dinlemesini açıkça düzenleyen bir metin olmamasına rağmen yasanın 5. maddesinin A bendi, iletişim araçlarıyla ilişkilendirilebilen "Bir kişi, yetkili huzuruna çıkarıldığı zaman hakkında işlem yapılan haberin doğruluğunu araştırmaya başlanır ve dinlenmesi gereken diğer deliller dinlenir" hükmünü içermektedir. [208] Bu maddenin valiye iletişimle ilgili erişim yetkisini doğrudan vermemiş ancak hiç bir sınırlama getirmeksizin kullanılan genel dil, geniş uygulamalara zemin hazırlayarak valiye bu yetkiyi dolaylı bir şekilde vermiştir.

-Terörle Mücadele Yasası: 2006 yılında çıkan Terörle Mücadele Yasası, mahremiyet hakkına herhangi bir müdahalenin yasal, gerekli ve orantılı olmasını sağlamak için gerekli

[208] 1954 Tarihli 7 Sayılı Qanun Mane Aljarayim Al'urduni (TR: Suçu Önleme Yasası), erişim 25 Ekim, 2021, https://2u.pw/l0oSo.

maddi ve usule ilişkin çeşitli güvencelerden yoksundur. Terörle Mücadele Yasası, "güvenilir bilginin" ne olduğuna veya hangi faaliyetlerin "terörist faaliyet" olarak kabul edildiğine dair net bir tanım yapmadan başsavcıya "terörist faaliyetler" ile ilgili "güvenilir bilgilere" dayanarak bir kişiyi gözetim ve denetim altına alma yetkisini vermektedir. Yasanın 4. maddesi, "başsavcı, bir kişi veya grubun herhangi bir terör eylemiyle bağlantılı olduğuna dair güvenilir bilgi alırsa, şüphelinin ikametgahı, hareketleri ve iletişim araçları üzerinde denetim uygulayabilir" hükmünü içermektedir.

Mahremiyet Hakkına İlişkin Kapsamlı Periyodik İncelemeye göre "güvenilir bilgi", Avrupa İnsan Hakları Sözleşmesi[209] gibi insan hakları yasalarının belirlediği standartlardaki "makul şüphe" düzeyine çıkmamakta ve bu nedenle bu bilgilere dayanarak denetime veya tutuklama emrine izin verilmesi çok geniş bir takdir yetkisi sağlandığı anlamına gelmektedir.[210] Bu bağlamda raporlar, son yıllarda Terörle Mücadele Yasası uyarınca "terörist grupları çevrimiçi olarak desteklemek" nedeniyle bazı kişilerin yargılandığını ve bu yargılamalardaki çoğu vakaların şüphelilerin WhatsApp sohbetlerine, cep telefonlarına veya kişisel bilgisayarlarına kaydedilen içeriğe dayandığını ileri sürmektedir.[211]

-Basın ve Yayınlar Yasası: Bu yasa, kitap, gazete, dergi ve benzeri tüm basılı ve yazılı literatürün yanında yayınevleri ve matbaa sahipleri, yayın ve ifade özgürlüğü ve aynı zamanda özel hayatın korunması ile ilgili yasal meseleleri ele almıştır. Yasanın 4. Maddesi, gazetecilik pratiğinde özel hayat ve ona saygı ile ilgilenmiş ve "hukuk sınırları içinde ve özgürlüklerin, hakların ve kamu görevlerinin korunması ve başkalarının özel hayat özgürlüğü ve gizliliğine saygı çerçevesinde basın, haber, bilgi ve yorum sağlama görevini serbestçe yerine getirir ve düşünce, kültür ve bilimin yayılmasına katkıda bulunur" hükmünü

[209] "Human Rights And Arrest, Pre-Trial Detentıon And Administrative Detention", Office of the United Nations High Commissioner for Human Rights, s.169, erişim 13 Nisan, 2021, https://2u.pw/ttWBO.
[210] "Stakeholder Report Universal Periodic Review: The Right To Privacy İn Hashemite Kingdom Of Jordan", Jordan Open Source Association, (2018), s.9, erişim 05 Nisan, 2021, https://2u.pw/Ab70I.
[211] "State Of Privacy Jordan", Privacy International, erişim 05 Şubat, 2022, https://2u.pw/WUECq.

benimsemiştir. Sanal haber sitelerinin yaygınlaşmasıyla birlikte Ürdün hükümeti, Basın ve Yayınlar Yasasında değişikliklerle yaparak sanal haber siteleri gibi sanal gazetecilik faaliyetlerini yasa kapsamına dahil etmiş ve değiştirilmiş yasanın 49. Maddesi bu alanla ilgilenmiştir.

Yasa, tüm basın sitelerinin kayıtlı ve ruhsatlı olmasını şart koşmuştur. Bununla birlikte yasa, sanal basın materyallerine yorum yapanların fikir ve ifade özgürlüğüne ve mahremiyet hakkına kısıtlamalar getirmiştir. Bu değişikliklerle birlikte haber sitesi sahiplerini ve çalışanlarını kullanıcılar tarafından yapılan yorumlardan sorumlu kılınmış ve site sahibi ile genel yayın yönetmeni, sanki yayınladıkları bir basın haberiymiş gibi kullanıcı yorumlarından sorumlu tutulmuştur. Ayrıca söz konusu değişiklikler, haber sitelerinin yorum içerikleri ve bunları yazanlarla ilgili tüm bilgiler de dahil olmak üzere, yayınlanan kullanıcı yorumlarının kaydını en az altı aylık bir süre boyunca tutmasını zorunlu kılmıştır. Dijital mahremiyete ilişkin 49. Maddenin hükümleri ise şu şekildedir;

C- Sanal basında yayınlanan yorumlar, sanal basın servisinin, sahibinin ve baş editörünün müştereken ve müteselsilen sorumluluğunda olan bir basın materyali olarak kabul edilir.

D- Sanal basın, haberin konusu ile ilgili olmayan bilgi veya olguları içeren veya gerçekliği doğrulanmamış veya bu yasa veya başka bir yasa hükümlerine göre suç teşkil eden yorumları yayımlayamaz.

E- Sanal basın servisi, yorumları gönderenlere ve yorumun konusuna ilişkin tüm bilgileri içermesi şartıyla yayınlanan yorumların kaydını altı aydan az üzere saklar.

F- Bu yasa hükümlerine aykırı hareket etmeleri halinde sanal basın servisi, sahibi, baş editörü ve basın materyalinin yazarının cezalandırılması, yorum gönderenleri yürürlükteki mevzuat uyarınca hukuki sorumluluktan kurtarmaz.[212]

[212] 1998 Tarihli 8 Sayılı Qanun Almatbueat Walnashr (TR: Basın ve Yayınlar Yasası ve Değişiklikleri), erişim 08 Ekim, 2021, https://2u.pw/LbtmN.

Madeni Yasa-Ulusal Dijital Kimlik: Ürdün Hükümeti, e-devlet projesi kapsamında 2016 yılında normal kişisel kimlik kartını (medeni durum kimliği) 144 KB'lık bir çipe sahip olan yeni bir akıllı ulusal kimlik kartıyla değiştirmeye başladığını duyurmuştur. Bu akıllı kart aracılığıyla dijital ve alfanümerik bilgiler kaydedilebilmekte ve iris taraması, parmak izleri ve elektronik imza teknolojisi gibi biyometrik verileri saklanabilmektedir. Akıllı kimlik kartı, cinsiyet, Arapça ve İngilizce ile ad-soyadı, doğum yeri, ikamet bölgesi, kan grubu gibi 18 veri alanı bulunmakta ve ilerleyen aşamalarda kartın sağlık sigortası, maaş, oy kullanma faaliyetleri ve seçimlere katılım gibi bilgileri içermesi beklenmektedir. Şimdilik akıllı kartların veri tabanının merkezi ve erişime izni olan taraflar hakkında herhangi bir bilgi bulunmamaktadır. Aynı zamanda Ürdün Medeni Yasası'nda şu anda bilgi mahremiyetini (dijital mahremiyeti) düzenleyen ve bu verilere yasa dışı erişimi cezalandıran herhangi bir madde yer almamaktadır. Akıllı kimlik kartının yayınlanmasını düzenleyen özel düzenlemelerin olmaması ve aktif bir veri koruma yasasının olmaması, bu tür girişimleri kişisel verilerin işlenmesi ve bu verilerin güvenliğini garanti edilmesi konusunda zayıf bırakmaktadır. Bu konuyla ilgili kararların çoğu, diğer ilgili paydaşların sınırlı gözetimi ve katılımıyla doğrudan Başbakan ve Bakanlar Kurulu tarafından kabul edilmiştir.[213]

İnternet Kafeleri ve Merkezleri Yönergesi: 2010 yılından itibaren İnternet Kafeleri ve Merkezleri Yönergesi'ne vatandaşların dijital mahremiyetini tehdit eden yeni düzenlemeler eklenmiştir. Örneğin bu yönergenin 5. maddesi, internet kafeleri ve merkezlerinin girişini kapsayan güvenlik kameralarının kurulmasını zorunlu kılmıştır. Ayrıca bu yönerge, müşterilerin kendi ulusal kimlik numaralarını, kullandıkları cihazların numarası ve kullanılan saat ve tarih dahil olmak üzere kendileri hakkında tanımlayıcı bilgiler vermelerini gerektirmiştir. Aynı zamanda yönerge, kafe sahiplerine kullanıcılar tarafından girilen siteleri girme tarihleri ve saatleri ile en az 6 aylık bir süre boyunca kaydetme zorunluluğu getirmiştir.[214]

---

[213] "State Of Privacy Jordan", Privacy International, erişim 05 Şubat, 2022, https://2u.pw/WUECq.
[214] "Taelimat Mueadala Litaelimat Tanzim Eamal Marakiz Wamaqahi Alaintirnit Wa'usus Tarkhisiha" (TR: İnternet Merkezleri Ve Kafelerinin Çalışmalarını Ve Ruhsat Verme Esaslarını Düzenleme Yönergesi Değiştirilmiştir), Al-Dustour Gazetesi, erişim 13 Mayıs, 2022, https://2u.pw/1eU1q.

Ayrıca 2016 yılında söz konusu yönergenin 5. maddesinde yeni değişiklikler yapılarak, internet kafeleri sahiplerinin internet kullanıcıların çevrimiçi iken terör veya yasa dışı faaliyetlerde bulunmalarını önlemek için "tüm teknik düzenlemeleri ve önlemleri" almaları zorunlu kılınmıştır. Ancak yönergedeki değişiklikler, yanlış anlama, yorumlama ve suiistimal için alan bırakacak şekilde internet kafeleri sahiplerinin uyması gereken prosedür ve düzenlemelerin tam olarak ne olduğunu belirtmemiş ve bu durum, dijital mahremiyet hakkının kaçınılmaz olarak çeşitli ihlallere maruz kaldığı anlamına gelmektedir.[215]

-SIM Kartlar: Cep telefonları kullanmak için bir SIM kartı kaydı yapmak zorunludur. Ürdün'de bir SIM kart edinmek isteyen herkesin, kartı etkinleştirmesi ve kayıt işlemini tamamlaması için Ürdünlü ise kişisel kimliğini ve Ürdünlü değilse pasaportunu ibraz etmesi gerekmektedir. Bu bağlamda SIM kartı kaydı, kullanıcıların anonim olarak iletişim kurma ve hareket etme imkanlarını sınırladığı gibi kullanıcıların yetkililer tarafından izlenmesini ve denetlenmesini kolaylaştırmaktadır. Buna ilaveten Telekomünikasyon Düzenleme Kurumu, 2018 yılında SIM kart sahiplerinin hatlarını etkinleştirmek için parmak izini kullanmak gibi biyometrik bilgilerini göndermeyi gerektiren yeni düzenlemeler devreye sokma niyetini açıklamıştır.[216] Bu çerçevede telefon hatlarının parmak izi ile etkinleştirme uygulamasının

[215] Aljarida Alrasmia 2016 (TR: Resmî Gazete), İnternet Merkezleri ve Kafelerinin Çalışmalarını ve Ruhsat Verme Esaslarını Düzenleme Yönergesine 2016 Yılında Çıkan Güncellenmiş Hali. Maddenin Metni: İnternet Merkezi Veya Kafesi Sahibi Ve Çalışanları, Aşağıdakileri Durumları Önlemek İçin Tüm Teknik Düzenlemeleri Ve Önlemleri Almalıdır: A. Terör Eylemlerinin Gerçekleştirilmesini Kolaylaştırmak, Terör Eylemleri Gerçekleştiren, Fikirlerini Destekleyen Ya Da Finanse Eden Bir Grup, Kuruluş Veya Derneğe Destek Sağlamak Veya Ürdünlüleri Ya Da Onların Mülkiyetlerini Düşmanca Misilleme Eylemleri Riskine Maruz Bırakmak Gibi Herhangi Bir Eylemde Bulunmak İçin Bilgi Sistemini Veya İnterneti Kullanmak Veya Bir Web Sitesi Oluşturmak. B. Fuhuşu Teşvik Eden, Dini İnançları Rencide Eden, Çekişmeleri Kışkırtan, Rejimi Tehdit Eden veya Uyuşturucu, Tütün ve Tıbbi Uyuşturucu Kullanımını Teşvik Eden Herhangi Bir Görsel, İşitsel Veya Metinsel Materyaline Erişmek, erişim 17 Ekim, 2021, https://2u.pw/FGDwN.

[216] "Alaitisalat Sataetamid Basmat Alyad Litawthiq Khutut Alhatif" (TR: Telekomünikasyon Düzenleme Kurumu, Telefon Hatlarını Etkinleştirmek İçin Parmak İzini Kullanacak), Roya Haber, erişim 13 Mayıs, 2022, https://2u.pw/IxXe0.

2020 yılında başlatılması beklenilmekteydi ancak Covid-19 pandemisinin araya girmesi bu uygulanmanın hayata geçirme mekanizmalarının belirtilmesini engellemiştir.[217]

Bu uygulamalar, kullanıcıların gizliliğini ihlal etme olasılığını artırdığı gibi kişisel verileri koruma yasasının çıkarılması için acil ihtiyacı yükselmektedir. Aynı zamanda, bu ihlallerle mücadele etmek için söz konusu yasanın etkinleştirilmesinin önemine rağmen mevcut yasa tasarısı, kişisel verilerin tanımlarken biyometrik verilere yer vermemiştir. Bu durum, yasanın onaylanması halinde bu tür davalar için etkinliği konusunda endişeleri artırmaktadır.

-Akıllı yolcu Taşımacılığı Uygulamalarının Ruhsatlarına İlişkin Yönetmelik: 2018 yılında Kara Taşımacılığı Düzenleme Kurumu, Uber ve Careem gibi akıllı ulaşım uygulamalarının ruhsatlarına ilişkin bir yönetmelik yayınlamıştır. Bu yönetmeliğin 5. Maddesi, Kara Taşımacılığı Düzenleme Kurumu'na yargı izin almadan veya gerekçe göstermeden ruhsat alan şirketlerin veri tabanlarına erişme ve talep edilmesi halinde, hizmet sağlayıcısı ve yolcu ile ilgili verileri ele geçirme yetkisini vermiştir. Söz konusu maddeye göre, "ruhsat sahiplerinin, Ürdün'de yürürlükte olan mevzuata ve aşağıdakilere uyacaktır:
A- "Başta hizmet sağlayıcısı, araç, yolcu ve yolculuk ile ilgili olanlar olmak üzere veri tabanında mevcut olan verileri talep etmesi halinde yetkiliye vermek.
B- Veri tabanında bulunan verileri akıllı uygulamalarla yolcu taşıma amacı dışında kullanmamak".[218]

Ancak bu madde, şirketlerin bu uygulamaları kullanan yolcu verilerini belirtilen amaç dışında kullanmasını yasaklamasına rağmen, bu hükme uyulmaması durumunda herhangi bir ceza öngörmemiştir. Bu bağlamda tezin yazıldığı tarihe kadar kişisel verileri koruma yasası

[217] "Dirasat Mashru Altawthiq Al'iiliktruni Likhutut Alhatif Bishumulia 'Akthar Bizili Korona" (TR: Covid-19 Pandemisi Gölgesinde Telefon Hatları İçin Elektronik Dokümantasyon Projesinin Daha Kapsamlı İncelenmesi)Al-Mamlaka, erişim 14 Ocak, 2022, https://2u.pw/IxXe0.
[218] 2018 Tarihli 9 Sayılı Nizam Tanzim Naql Alrukaab Min Khilal İstikhdam Altatbiqat Aldhakia (TR: Akıllı Yolcu Taşımacılığı Uygulamalarının Ruhsatlarına İlişkin Yönetmelik), erişim 07 Ekim, 2021, https://2u.pw/XK9U3.

henüz onaylanmamış olması nedeniyle kullanıcıların mahremiyetinin ihlal edilme olasılığı artmaktadır. Ayrıca farklı veri tabanlarına erişim yetkisi, Ürdün hükümetinin kullanıcıların hareketlerini ve faaliyetlerini takip etmesine zemin hazırlayarak bireylerin mahremiyetlerini ihlal etmesine ve kişisel verileri koruma ilkelerini çiğnemesine olanak tanımaktadır.

1.2 Ürdün Siber Suçlar Yasası

1.2.1 Ürdün Siber Suçlar Yasası'nda Dijital Mahremiyet Hakkının Ele Alınışı

Siber Suçlar Yasası, 2010 yılında çıkarılan ve o dönemde feshedilen Temsilciler Meclisi'nin yokluğunda geçici bir yasa olarak kabul edilen ve büyük bir tartışma yaratan geçici dijital Bilgi Sistemleri Yasası'na alternatif olarak 2015 yılında onaylanmıştır.[219] Bununla birlikte 2015 tarihli Ürdün Siber Suçlar Yasası, görüş ve ifade özgürlüğü hakkının geniş bir şekilde kısıtlaması nedeniyle yasal anlamda eleştirilen tartışmalı bir yasa olarak görülmektedir. İnsan Hakları İzleme Örgütü (Human Rights Watch) Siber suçlar Yasasını Ürdün'de kamusal özgürlüklere ve ifade özgürlüğüne daha fazla kısıtlama getirdiği için birden fazla raporunda eleştirmiş ve yasanın Uluslararası Medeni ve Siyasi Haklar Sözleşmesi gibi tüm bireylerin ifade özgürlüğü hakkını garanti eden uluslararası sözleşmelerle çeliştiğini ileri sürmüştür.[220]

Ayrıca bu yasa, ağırlıklı olarak Ceza Yasası gibi diğer yasalardaki suç işleme yollarına odaklanmış ancak o yasalardaki cezaları artırmakla birlikte sosyal medya kullanıcılarının bir takım günlük faaliyetlerini suç çemberi içinde almıştır. Ayrıca yasa, suç kastını veya niyetini dikkate almamış ve tüzel ile özel kişiler arasında da ayrım yapmamıştır. Öte yandan yasa, siber suçları azaltmak için bazı garantiler vermekte ve bilgisayar korsanlığını ile dijital ortamda gerçekleştirilen bazı yasa dışı faaliyetleri cezalandırmaktadır. Ürdünlü yasa koyucu, Siber Suçlar Yasasında mahremiyete yönelik dijital saldırılarının cezalandırılması konusunda

[219] Reem Al-Masry, "Qanun Aljarayim Al'iilikturunia: Alsaytart Ela 7 Milyun Mustakhdam Lilintirnit" (TR: Siber Suçlar Yasası: 7 Milyon İnternet Kullanıcısı Üzerinde Kontrol), Hiber Magazine, erişim 06 Ağustos, 2021, https://2u.pw/5Ni8g.
[220] "Jordan 'Fake News' Amendments Need Revision", Human Rights Watch, erişim 11 Ağustos, 2021, https://2u.pw/BsSY3.

açık ve spesifik hükümler sunmazken özellikle 3-8 maddelerde, bilgisayar korsanlığı veya bilgi sistemlerine yasadışı erişim gibi bu hakkın ihlalini içeren diğer suçlarla ilgili hükümlere yer vermiştir.

Yasanın 3. maddesi, bilgi sistemlerine ve internet sitelerine önleyici yasal koruma sağlamaktadır. Yasa, sistemlere yasa dışı erişimin çeşitli siber suçların işlenmesi için bir ön koşul olduğunu ve çoğu suçların öncelikle bilgi sistemine erişmeden işlenemeyeceğini savunmaktadır. Söz konusu madde, bilgi sistemlerine yasa dışı erişimin suç sayılmasını 3 bantta düzenlemektedir:
"A- Bilgi ağına veya bilgi sistemine yetkisiz olarak veya yetkiye aykırı veya yetkiyi aşarak herhangi bir şekilde kasten giren kişi, bir haftadan az ve üç aydan fazla olmamak üzere hapis veya (100) yüz Ürdün dinarından az ve (200) iki yüz Ürdün dinarından fazla olmamak üzere para cezası veya her ikisi ile cezalandırılır. B- Bu maddenin (A) bendinde öngörülen yetkisiz erişim, veri veya bilgileri iptal etmek, silmek, eklemek, yok etmek, ifşa etmek, zarar vermek, alıkoymak, düzeltmek, değiştirmek, aktarmak veya kopyalamak veya bilgi sistemlerinin çalışmasını durdurmak veya kesintiye uğratmak ise fail, üç aydan az bir yıldan fazla olmamak üzere hapis ve (200) iki yüz Ürdün dinarından az ve (1.000) bin Ürdün dinarından fazla olmamak üzere para cezası ile cezalandırılır. C- Ayrıca bir internet sitesinin içeriğini değiştirmek, iptal etmek, yok etmek, düzeltmek, istismar etmek veya sitenin ya da sahibinin kimliğini çalmak amacıyla kasten giren kişi, üç aydan az bir yıldan fazla olmamak üzere hapis ve (200) iki yüz Ürdün dinarından az ve (1.000) bin Ürdün dinarından fazla olmamak üzere para cezası ile cezalandırılır".

3. Maddenin hükümlerini analiz ettiğimizde Ürdünlü yasa koyucunun, A bandında olduğu gibi sadece hackleme amacıyla yetkisiz erişim ile B bandında olduğu gibi belirli bir hedefe ulaşmak amacıyla erişim arasında ayrım yaptığına görebiliyoruz. Bazı hukuk uzmanları, suçu belirli bir amaca ulaşmakla ilişkilendirmenin kanıtlanmasının zor olduğunu ve cezaları ağırlaştırmak için sonuçların dikkate alınması gerektiğini savunmaktadır. Ayrıca bu maddede

Ürdünlü yasa koyucu, yasa dışı erişmeyi izinleri aşmayı suç sayarken erişimin meşru ve izinli olduğu sürenin sona ermesine rağmen kişinin sisteme girmeye devam ettiği durumlarda olan erişimin meşru olmayan devamlılığını ele almayarak suç haline getirmediğini görmek mümkündür.[221]

3. maddedeki suçun konusu, kişilerin bilişim sistemleri ve internet ağı üzerinden gönderilen verilerinin mahremiyetine ilişkin bilgi ve verileri ele almaktadır. Siber Suçlar Yasasının 2. Maddesi, veriyi "kendi başına bir anlamı olmayan sayılar, harfler, semboller, şekiller, sesler ve görüntüler olarak tanımlarken bilgiyi işlenmiş ve anlamı büyük olan veriler" olarak tanımlanmaktadır. Burada, Ürdünlü yasa koyucunun yazılı belgeler, görüntüler ve ses kayıtları dahil etmekle internet ağında iletilen bilgi ve veriler için cezai koruma kapsamını genişlettiğini fark ediyoruz.

Cezaya ilişkin olarak, failin kastına ilişkin bir şartın bulunduğu ve maddede belirtildiği gibi erişim hedefinin farka yaratan bir öneme sahip olduğunu görüyoruz. Yasa koyucu, hackleme veya yasa dışı erişim gibi suçlar için ağırlaştırıcı sebep teşkil eden amaçları genişleterek belirtmektedir. Bu anlamda ağırlaştırılmış ceza, üç aydan az bir yıldan fazla olmamak üzere hapis ve (200) iki yüz Ürdün dinarından az ve (1.000) bin Ürdün dinarından fazla olmamak üzere para cezası olacaktır. Ancak bazı hukukçular, bu cezanın ağırlaştırma felsefesine uymadığına ve ağırlaştırıcı duruma ulaşmak için asıl sorunun amaçların kanıtlanmasının zor olduğuna inanmaktadır. Bu nedenle yargı, A bandında yer alan bir haftadan az ve üç aydan fazla olmamak üzere hapis veya (100) yüz Ürdün dinarından az ve (200) iki yüz Ürdün dinarından fazla olmamak üzere para cezası hükmüne yönelmektedir. Bu ceza da yetersiz olmakla birlikte ağırlaştırma felsefesine uymamakta ve caydırıcı bir ceza teşkil etmemektedir.[222]

---

[221] Ahmed Al-Mana'sah ve Jalal Muhammad Al-Zoubi, *Crimes Relating To Information Electronic Systems And Technology*, Amman: Dar Al-Thaqafah For Publishing And Distribution, 2017, s.33.
[222] Wejdan Irtaimeh, "Criminal Protection Of Privacy In The Jordanian Cybercrime Law No.27 of 2015", *Asian Social Science*, 16/12 (2020), s.69.

3. Maddenin C bandına gelince, internetteki bir web sitesine yasa dışı erişim suçuna ilişkin olup bilgi ağlarına veya sistemlerine yönelik saldırıyı suç sayan B bendinde belirtilen suçtan farklı değerlendirilmektedir. Böylece C bandında saldırının konusu web siteleridir. Bilgi sistemlerine yönelik saldırıları ele alan önceki bantların aksine Ürdünlü yasa koyucu, C bendinde internet sitelerinin kamuya açık olması nedeniyle siteye erişimin izinsiz veya yetkiyi ihlal ederek yapıldığını belirtmemiştir. Ürdünlü yasa koyucu, internet sitelerini hackleme suçunda, sitesinin içeriğini değiştirmek, iptal etmek, yok etmek, düzeltmek, istismar etmek veya sitenin ya da sahibinin kimliğini çalmak gibi bir suç kastının bulunmasını şart koşmaktadır.[223]

Bir siteyi istismar etmek veya kimliğini çalmak, "bu sitenin kontrol edilmesi ve sitenin orijinal kimliğini kopyalayarak benzer bir tasarımı olan başka bir sitenin yapılması ve ziyaretçileri bu sitenin orijinal site olduğu konusunda yanıltılması ve böylece suçlunun bu bilgileri daha sonra kullanmak üzere ziyaretçilerin bu siteye girip doldurduğu sağlıkla ilgili, mesleki, sosyal ve benzeri kişisel ve gizli bilgilerin ele geçirmesi. Site sahibinin kimliğini çalmaya gelince, suçlunun davranışı, başkalarını sitenin sahibi olduğu konusunda aldatması" anlamına gelmektedir.[224]

Ayrıca yasanın 4. maddesi, virüs ve bilgisayar korsanlığı programları gibi kötü amaçlı yazılımların bilgi sistemlerine ve internet sitelerine yönelik saldırılarını suç saymıştır. Buna göre, "kasıtlı olarak bir programı internet aracılığıyla veya bir bilgi sistemini kullanarak iptal etmek, silmek, eklemek, yok etmek, ifşa etmek, zarar etmek, engellemek, değiştirmek, düzeltmek, aktarmak, kopyalamak, yakalamak veya başkalarını verileri görüntülemesini sağlamak amacıyla kullanan ya da bir bilgi sistemini engellemek, müdahale etmek,

[223] El-Bishtawy, a.g.m., s.126.
[224] Irtaimeh, a.g.m., s.72.

çalışmasını durdurmak veya devre dışı bırakmak hedefiyle davranan ya da bir web sitesini değiştirmek, iptal etmek, imha etmek, içeriğini değiştirmek, istismar etmek, sitenin veya sahibinin kimliğini izinsiz çalmak veya yetkiye aykırı davranmak suratıyla hareket eden herkesi bir aydan az ve bir yıldan fazla olmamak üzere hapis ve (200) iki yüz dinardan az ve (1.000) bin dinardan fazla olmamak üzere para cezası ile cezalandırılır".

4. Madde, maddenin içinde ve 3. Maddenin B bendinde belirtilen amaçlardan herhangi birine ulaşmak için bilgi sistemine erişimin gerektirmediği açısından 3. Maddeden farklıdır. Zira internet siteleri herkesin kullanımına açıktır ve suçlu, amacına ulaşmak için siteye yasa dışı veya izinsiz bir şekilde erişmeye ihtiyaç duymamaktadır. Aynı zamanda suçlu, E-posta yoluyla bir virüs göndermek, alıcının bilgi sisteminin diğer bilgilere saldırmasını sağlayan bir program yollamak veya bir web sitesine saldırmak için bir program kullanmak süratiyle verilere saldırmak için uzak bir program devriye sokması yeterlidir. Ayrıca 4. maddede belirtilen suç, suçlunun bilişim teknolojisine dayanması nedeniyle yöntem bakımından 3. maddede belirtilen diğer suçlardan farklılık göstermektedir.[225]

Ayrıca 5. Maddeye göre, "İnternet ağı veya herhangi bir bilgi sistemi aracılığıyla gönderilenleri kasıtlı olarak ele geçiren, engelleyen, gizlice dinleyen, değiştiren veya silen kişi, bir aydan az ve bir yıldan fazla olmamak üzere hapis ve (200) iki yüz dinardan az ve (1.000) bin dinardan fazla olmamak üzere para cezası ile cezalandırılır". Bununla birlikte 6. madde, "internet ağı aracılığıyla kasıtlı ve izinsiz bir şekilde kredi kartı bilgi sisteminden herhangi bir veri veya bilgiyi ya da finansal veya sanal bankacılık işlemlerinin yürütülmesinde kullanılan veri veya bilgileri elde eden kişileri" cezalandırmaktadır.

[225] Irtaimeh, a.g.m., s.72.

Bu yasanın 5. maddesinde belirtilen bu suç, iletişim ağları aracılığıyla bir mesajın içeriğini ele geçiren, engelleyen, değiştiren veya silen ya da başkalarını bu eylemi gerçekleştirmeye teşvik eden kişilerin bir aydan az ve altı aydan fazla olmamak üzere hapis cezası veya 220 Ürdün dinarını geçmemek üzere para cezası veya her ikisi ile cezalandıran İletişim Yasası'nın 76. maddesinde öngörülen suça benzemektedir. Siber Suçlar Yasası'nın açıklama Metni, Ürdünlü yasa koyucunun kamu ile özel iletişim ve internet arasında farklılık bulunduğu görüşünde olduğundan söz konusu suç, bu yasada da ele alındığını göstermektedir. Kamu ve özel iletişim şebekeleri, her iki şebekenin ancak iletişim yasasına uygun olarak ruhsat alarak kurulduğu veya bağlandığı nedeniyle bu yasa (iletişim yasası) ile düzenlenmiştir. Ancak internet şebekesi, kamu iletişim şebekesini kullanması gerekse bile böyle bir ruhsat ihtiyacı bulunmamaktadır. Zira internet şebekesi, ruhsat ihtiyacı olmayan ve Ürdün yasalarının geçerli olmadığı ülke sınırları dışında başka bir iletişim ağına bağlı olmaktadır.[226]

Yazışmaya saldırma suçu, 5. Maddede belirtildiği şekliyle suç niyetiyle kasıtlı bir suç sayılmaktadır. Başka bir deyişle Ürdünlü yasa koyucu, 5. Maddede suçun suç kastı ile mahremiyete yönelik bir saldırının olması gerektiğini öngörmüş ve (kasıtlı yapan ... cezalandırılacaktır) şeklinde düzenlemiştir. Bu suç için öngörülen cezaya gelince yasa koyucu, internet veya bilgi sistemi aracılığıyla gönderilen her şey için 5. Maddede yer alan tüm mahremiyet ihlallerine yönelik tek bir ceza vermiştir. Aynı zamanda yasa koyucu, hâkime takdir yetkisini vererek hapis ve para cezaları arasında seçmesini isterken ikisini birlikte uygulaması yasaklamıştır.[227] Siber Suçlar Yasası'nın 8. maddesine göre, 3. maddeden 6. maddeye kadar yer olan suçlara ilişkin cezalar, bir kişi tarafından görevi nedeniyle işlenmesi halinde bir kat artırılmaktadır. Zira bu madde, " 3. ile 6. maddeler arasındaki suçlara ilişkin cezalar, görevi veya işi ya da bunlardan herhangi birini istismar etmesi nedeniyle daha artmaktadır".

[226] Almudhakira Alayadahia Liqanun Jarayim 'Anzimat Almaelumat (TR: Siber Suçlar Yasası'nın Açıklama Metni), erişim 09 Ağustos, 2021, https://2u.pw/16BlG.
[227] Irtaimeh, a.g.m., s.67.

Siber Suçlar Yasası, mahremiyeti ihlal etme teşebbüsü için bir ceza öngörmemiştir. Zira (3, 4 ve 5) maddelerde belirtilen mahremiyetin ihlal biçimleri, hafif hapis veya para cezalarıyla cezalandırılan durumlar şeklinde algılanmıştır. Bu nedenle Ceza Yasası'na göre (71. Madde), yasada açıkça belirtilen durumlar dışında, kabahatler olarak görülen suçlara teşebbüs edilmesi cezalandırılmamaktadır. Siber Suçlar Yasası hükümlerini inceleyerek Ürdünlü yasa koyucu, 3-5 Maddelerde yer alan mahremiyetin ihlal biçimleri de dahil olmak üzere, yukarıda belirtilen suçlardan herhangi birine teşebbüs için bir ceza vermediği sonucuna varıyoruz.

1.2.2 Siber Suçlar Yasası'ndaki Yasal Boşluklar

Daha önce de belirttiğimiz gibi, Siber Suçlar Yasası, dijital mahremiyet hakkını güvence altına alan yasal maddeler öngörmemiş ve sadece (3-5) arasındaki maddelerde yer alan bilgi sistemleri aracılığıyla gerçekleşen bazı dijital mahremiyet ihlal biçimlerine yer vermiştir. Zira Ürdünlü yasa koyucu, yasa dışı veri toplama ve depolama, güvenlik tedbirleri sağlamadan izinsiz bilgi işleme, nominal verilerin yasadışı ifşası, meta verilere erişip kullanma, veri ve bilgilerin işleme hedefinden sapma gibi bireylerin dijital mahremiyeti ile ilgili yeni siber suç biçimlerini görmezden gelmiştir. Mevcut Ürdün siber Suçlar Yasası, çeşitli yasal eksikliklere sahiptir. Hakaret, iftira ve aşağılama suçlarına ilişkin madde (11. Madde) nedeniyle sert eleştirilere maruz kalan yasa, aynı zamanda dijital mahremiyet hakkına yeterli cezai koruma sağlamamıştır. Zira yasa, dijital mahremiyet hakkını ve kişisel verileri cezai olarak açıkça korumamıştır. Aynı şekilde 3., 4. ve 5. maddelerdeki cezalar caydırıcı görülmemektedir.

Ayrıca yasanın 13. Maddesi, yetkili başsavcıdan veya yetkili mahkemeden izin aldıktan sonra adli kolluk görevlilerine delillerin bu yasada öngörülen suçlardan herhangi birinin işlenmesinde kullanıldığını düşünülen herhangi bir yere girmelerine izin vermektedir. Ayrıca

bu görevliler, söz konusu suçlardan herhangi birini işlemek için kullanılan cihazları, araçları, gereçleri, programları, işletim sistemlerini ve internet ağını arama yetkisine sahiptir. Bu madde, iletişim gözetimiyle ilgili insan hakları standartlarının uygulanmasına ilişkin uluslararası ilkelere açıkça aykırıdır. Zira bu standartlar, girme, arama veya izleme emrinin sivil bir mahkeme hâkimi tarafından verilmesinin yanında hâkimin mümkün olduğu kadar eylemin zaman kapsamı ve ele geçirilecek verinin boyutu belirtmesini şart koşmuştur. Ancak Ürdün'de uluslararası kabul görmemiş bir mahkeme olan Ürdün Devlet Güvenlik Mahkemesinin savcısı, kararları yargı tarafından verildiği için giriş ve denetim yetkisine sahiptir.[228]

Bahsettiğimiz gibi Siber Suçlar Yasası, geniş yasal itiraz ve eleştirilerle karşılaşmıştır. Zira söz konusu suçlar, daha hafif cezalarla Ceza Yasası'nda yer almasına rağmen bu yasada yüksek cezalarla yer almıştır. Bu durum, ancak hükümetin internet ve dijital alan kullanıcılarına otosansür uygulamayı amaçlamasıyla açıklanması mümkündür. Siber Suçlar Yasası'ndaki en belirgin yasal boşluk, 11. Maddede yer alam hakaret, aşağılama ve ifade suçları ile ilgili hükümlerdir. 2015 tarihli 27 Sayılı Siber Suçlar Yasası'nın yasal boşluklar ışığında dijital mahremiyetle ilgili sorunlar, Ürdün mevzuatında kişisel verileri korumaya yönelik özel bir yasanın olmamasından kaynaklanmaktadır. Zira Kişisel Verileri Koruma Yasası Tasarısı, yıllardır Mevzuat ve Görüş Kurulu'nda takılıp kalmış ve tartışılmak ve onaylanmak üzere Temsilciler Meclisi'ne iletilmeyi beklemektedir.

2. Dijital Mahremiyetle İlgili Yasaların Filistin Temel Yasası ve İlkelerine Uyumu

2.1 Dijital Mahremiyet Hakkının Filistin Mevzuatındaki (Yasal) Ele Alınışı

Filistin yargısı, İnternet ve bilgi teknolojisi yoluyla işlenen suçların ele almasında esas olarak 1996 tarihli Telsiz İletişim Yasası, 2013 tarihli Dijital İşlemler Yasası ve 1960 tarihli 16 Sayılı Ürdün Ceza Yasası'nın yorumlarına dayanmaktadır. Bu nedenle bahsi geçen

[228] Al-Masry, (2017), a.g.e.

yasalardaki dijital mahremiyet ile ilgili maddeleri ele almanın yanı sıra 2018 tarihli Filistin Siber Suçlar Yasası'nı daha detaylı bir inceleyeceğiz.

-İletişim Yasası: Bu yasanın 4. Maddesine göre, "Filistin topraklarındaki iletişimin mahremiyeti korunur ve yalnızca yasaların sınırları dahilinde kamu otoritesi tarafından ihlal edilebilir". Bu madde, iletişimin mahremiyetine yer vermesine rağmen izin verilen durumları veya yargı emirlerinin çerçevesini belirtmeksizin İstihbarat ve Önleyici Güvenlik Gücü gibi kamu otoritesi bilişenlerine görüntüleme, izleme ve ele geçirme yetkilerini tanıyarak bu hakkı kısıtlamakta ve böylece uluslararası ilke ve anlaşmaları açıkça ihlal etmektedir. Söz konusu madde, güvenlik güçlerine yargı emirleri ile sınırlı olması gereken gerçek kontrol prosedürleri olmadan kullanıcıları izleme yetkisi vermektedir.

Ayrıca 86. maddeye göre, "görevi gereği gördüğü veya hukuki dayanağı olmaksızın kaydettiği herhangi bir iletişimin içeriğini veya telefon mesajını bir iletişim ağı aracılığıyla paylaşan veya yayan kişi, bir yılı geçmeyen hapis veya 300 Ürdün dinarını geçmeyen para cezası veya her ikisi ile cezalandırılır". Buna ilaveten aynı maddenin ikinci bendi, istihbarat sırrı kendisine emanet edilen bir kimseyi bu sırrı ifşa ermeye tahrik edene, 100 dinardan az ve 300 dinardan fazla olmamak üzere para cezası ve bir aydan az ve bir yıldan fazla olmamak üzere bir hapis cezası veya her ikisi ile cezalandırılacağını belirtmiştir.

92. Madde, "İletişim ağları aracılığıyla bir mesajın içeriğini engelleyen, değiştiren veya silen veya başkalarını bu eylemi gerçekleştirmeye teşvik eden kişilerin bir aydan az ve altı aydan fazla olmamak üzere hapis cezası veya 50 Ürdün dinarından az ve 200 Ürdün dinarından fazla olmamak para cezası veya her ikisi ile cezalandırılır" hükmünü içermektedir. 93. madde, bir mesajı kopyalayan veya ifşa eden veya gizli telefon numaraları ve gönderilen ile teslim alınan mesajlar dahil olmak üzere bir aboneye ait özel bilgilere müdahale eden kişilerin altı ayı geçmeyen bir hapis cezası veya 1.000 Ürdün dinarı geçmeyen bir para cezası

veya her ikisi ile cezalandırılır" olduğunu öngörmektedir.[229] Bu bağlamda yasanın internet bağlantı mekanizmasını düzenlemediğini ve hükümlerinde doğrudan bilgi sistemleri ile ilgili konuların hiçbirini ele almadığını belirtmekte fayda var.

Filistin İletişim Yasası ile Ürdün İletişim Yasası arasında sağlanan yasal koruma ve cezalar bakımından büyük benzerlik olduğunu görüyoruz. Ürdün İletişim Yasasında yer alan hükümler, Filistin'deki yasadan farklı olarak azami ve asgari cezayı belirtirken, Filistinli yasa koyucu asgari bir ceza belirlememiştir. Ayrıca Ürdünlü yasa koyucu, telefon görüşmelerini ve özel iletişimi gizli meseleler olarak kabul edip genel olarak bunlara yönelik saldırıları yasaklarken Filistinli yasa koyucu, kamu makamlarının bunlara erişmesine ve yargı ve mahkeme emirleriyle sınırlandırmadan izlemesine izin vererek bu hakkı zayıflatmıştır. Bu anlayış, yargı emri olmadan devlet kurumlarının bireylerin iletişimini izlemesini yasaklayan anayasal ilkelere ve uluslararası sözleşmelerin standartlarına açık bir ihlal temsil etmektedir. Ürdün İletişim Yasası'nda olduğu gibi, Filistin İletişim Yasası, modern iletişim araçlarını ve bunlar aracılığıyla iletilen verilerin gizliliğini kapsamamakta ve yalnızca geleneksel anlamda telefon iletişimi için yasal koruma sağlamaktadır.

-Ceza Yasası: Batı Şeria bölgeleri, 1960 tarihli 16 sayılı Ürdün Ceza Yasası'nı kullanmaktadır. Filistin Ceza Yasası Tasarısının hazırlanmasına rağmen, 2006 yılından bu yana Filistin Yasama Meclisi'nin yokluğu ve tasarıyla ilgili birçok yorum ve eleştiri olduğu nedeniyle onaylanmamıştır. Ürdün Ceza Yasası, ikinci bölümde namus ve özgürlüklere karşı suçlar bağlamında özel hayata saldırı suçlarını ele alınmıştır. Mevcut yasada yer alan ve aslında 1960 tarihli 16 sayılı Ürdün Ceza Yasası'nda bulunan 347. Madde, konutun dokunulmazlığını ihlal eden ve izin alamdan bir konuta veya eklerine girenlerin altı ayı geçmemek üzere hapis cezası ile cezalandırılacağını belirtir. Aynı madde, saldırganın yalnızca zarar gören tarafın şikâyeti üzerine yargılandığını belirtmiştir. Madde metni:

[229] Qanun Bishan Alaitisalat Alsilkia Wallaasilkia (TR: Telli ve Telsiz İletişim İle İlgili 1996 Tarihli (3) Sayılı Yasa), erişim 14 Ağustos, 2021, https://2u.pw/WQj59.

“1. Sahibinin iradesi dışında bir konuta veya onun eklerine girenler veya bir konutta onları çıkartma hakkı olan sahibin izni olmadan ikamet edenler altı ayı geçmemek üzere hapis cezası ile cezalandırılır. 2. Konut ihlal fiili, şiddeti veya silahı kullanarak geceleyin ve birden fazla kişi tarafından meydana geldiğinde suçu işleyenler, bir aydan bir yıla kadar hapis cezası verilir. 3. Birinci bentte öngörülen durumda, zarar gören tarafın şikâyeti olmadan soruşturma yapılamaz.”

Yasanın 355. Maddesi ise, önceden de ele aldığımız gibi, görevi gereği resmi sırları elde edip ifşa edenler, gizli veya resmî belgeleri ele geçirip paylaşanlar ya da mesleği gereği bir sırrı bilip açıklayanlar için 3 yıla kadar hapis cezası öngörmüştür.

Ayrıca 356. madde, “Telefon İşleri Dairesi'nde işi ve konumu gereği ulaştığı bir telefon görüşmesini ifşa eden kişiye altı ay hapis cezası veya yirmi Ürdün dinarına kadar para cezası uygulanır” hükmünü içermektedir. Buna ilaveten yasanın 357. maddesi, “Kendisine gönderilmeyen bir mektubu veya telgrafı kasten imha eden veya açan kişi beş Ürdün dinarı geçmemek üzere para cezası ile cezalandırılır” hükmünü vermiştir. Eski bir yasa olan 1960 tarihli Ürdün Ceza Yasası’na dayanan Filistin Ceza Yasası, dijital mahremiyetin özel doğasını ve internet yoluyla özel hayatın ihlalini dikkate almadığını ve hiçbir hükmünde yeni iletişim araçlarına ve kişisel verilerin korunmasına yer vermediğini görüyoruz. Filistin Ceza Yasası, Ürdünlü yasa koyucunun 348. Madde metninde yaptığı küçük değişiklikler dışında Ürdün Ceza Yasası ile aynı maddeleri içermektedir. Böylece iki ülkedeki tüm değişiklikleriyle bu yasa, yalnızca bir mesajın veya telefon görüşmesinin ifşası ile sınırlı kalan geleneksel bir mahremiyet koruması sağlamıştır.

-Ceza Muhakemeleri Usulü Yasası: Bu yasa, 51. maddesinin ikinci bandında, telefon görüşmelerinin takip edilmesini yargı emirleri şartıyla sınırlandırılmasına ilişkin usuller belirlenmiştir. Bu maddeye göre, “1. Başsavcı veya yardımcılarından biri, cinayet ve onu işleyen kişi ile ilgili olan telgraf ve posta ofislerinde bulunan mektupları, gazeteleri, yayınları, telgrafları ve paketleri ele koyma yetkisine sahip. 2. Başsavcı veya yardımcılarından biri, bir

yıldan az olmayan bir süre için hapis cezası gerektiren bir suç veya kabahatte gerçeğin ortaya çıkarılmasında faydalı olacaksa sulh hakiminin iznine istinaden telli ve telsiz görüşmeleri gözetebilir ve özel bir yerde yapılan görüşmeleri kayıt altına alabilir. 3. Tutuklama emri, gözetim izni veya kayıt gerekçeli olma şartıyla bir sefer yenilenebilen on beş günü aşmayan bir süre içinde olabilir".[230] Bu anlamda bu madde, konuşmaları özel hayatın bir parçası değerlendirerek özel hayatın gizliliği hakkının ihlalini suç sayan Filistin Temel Yasası'na uyumlu olurken, diğer Filistin yasaları gibi mahremiyeti geleneksel anlamda ele alarak dijital mahremiyeti dâhil etmeden sadece fiziksel koruma sağlamaktadır.

-Medeni Yasa: Filistinli yasa koyucu, 59. Maddesinde kişilik haklarına yasa dışı saldırıları suç sayan 2012 tarihli Medeni Yasa'yı onaylamıştır. Aynı madde, Ürdün Medeni Yasası'nda yer almış ve özel hayatın gizliliği hakkını kişilik haklarından saymıştır. Ayrıca maddeye göre, "Kişilik haklarından birine hukuka aykırı bir saldırıya uğrayan herkes, bu saldırının durdurulmasını ve uğradığı zararın tazmin edilmesini isteyebilir." Bu madde, zarar gören herkes için tazminat hakkını teyit ettiği için Filistin Temel Yasası'ndaki anayasal ilkelerle uyumludur.

-Suçu Önleme Yasası: Batı Şeria'da yürürlükte olan 1954 tarihli 7 sayılı Suçu Önleme Yasası, Ürdün Suçu Önleme Yasası ile aynıdır. Daha önce de belirttiğimiz gibi bu yasa, valiye yazışma ve kişisel görüşmelerin hiçbirine erişme yetkisini doğrudan vermemesine rağmen yasanın 5. Maddesi, bu yetkiyi kendisine dolaylı bir şekilde vermiştir. Bu durum da anayasal hüküm ve ilkelere aykırıdır.

-Yolsuzlukla Mücadele Yasası: 2015 tarihli 1 Sayılı Yolsuzlukla Mücadele Yasası ve değişiklikleri, dijital izleme ile ilgili dahil olmak üzere bazı kusurlar içermektedir. Bu

[230] 2001 Tarihli (3) Sayılı Qanun Al'iijra'at Aljazayiya Alfilastini (TR: Filistin Ceza Muhakemeleri Usulü Yasası), erişim 11 Ağustos, 2021, https://2u.pw/Wz3rZ.

bağlamda 22. Maddesi, "İlgili yasada yer alan suçlara ilişkin delillerin toplanmasını kolaylaştırmak amacıyla, yetkili merciin izni ile kontrollü teslimata başvurulabileceği gibi uygun şekilde dijital izleme ve hackleme gibi özel bir soruşturma yolunu takip edilmesi de mümkündür. Bu yollarla ele geçirilen delillerin geçerliliği, mahkemenin takdirine tabi tutulmaktadır" hükümleri yer almaktadır. Bu madde, gereklilik ve orantılılık koşullarının sağlanması başta olmak üzere ifade özgürlüğü üzerindeki kontrollere ilişkin anayasal kriteri ihmal etmektedir. Bu bağlamda gereklilik kriteri, hacklama ve dijital takip gibi yöntemlerin meşru bir amaca ulaşmanın tek yol olduğu anlamına gelmektedir.

Böylece söz konusu amaca ulaşmanın başka bir yolu olduğu sürece hacklama ve dijital takip gibi yöntemler gerekliliğini kaybederek meşru sayılmamaktadır. Buna bağlı olarak 31 Sayılı Genel raporunda İnsan Hakları Yüksek Komiserliği, "hiçbir durumda hakların özüne zarar verecek şekilde kısıtlamalar getirilemez veya başvurulamaz" vurgusunu yapmıştır.[231] Orantılılık kriteri ise, suçun meydana geldiğine veya işlenmek üzere olduğuna dair açık delillerin bulunması ve daha az ihlal edici diğer soruşturma yöntemlerinin tüketilmiş olması durumunda uygulanmaktadır. Ancak bu durumda, yargı emirleri olması gerektiği gibi elde edilen bilgilerin soruşturma konusu olan suçla sınırlı kalması ve ek bilgilere el uzatılmaması şartı aranmaktadır.[232]

2019 yılında Filistin Bakanlar Kurulu, vatandaşların kişisel verileriyle ilgili 2019 tarihli 3 sayılı Kararını yayınlamıştır. Bu karar, Batı Şeria ve Gazze Şeridi'nde yürürlükte olan özel bir yasa olarak kabul edilmiştir. Bu yasa, iki madde içermiştir. 1. Madde: Ticari amaçla hizmet sağlayan şirket ve kuruluşlardan hizmet alan vatandaşların doğrudan veya dolaylı kişisel verilerinin önceden izin almaksızın kullanılması cezai yasal sorumluluk altında

[231] Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği Yıllık Raporu: Alhaqu Fi Alkhususia Fi Aleasr Alraqamii (TR: Dijital Çağda Mahremiyet Hakkı), Birleşmiş Milletler Genel Kurulu- İnsan Hakları Konseyi, Oturum (27). s.64.
[232] Esam Abdin, "Mulahazat Muasasat Alhaq Ealaa Mashru Alqarar Biqanun Almueadal Liqanun Mukafahat Alfasad" (TR: Al-Haq Kurumunun Yolsuzlukla Mücadele Yasasındaki Değişiklik Tasarısı Hakkındaki Yorumu), Al-Haq Kurumu, erişim 17 Mayıs, 2022, https://2u.pw/929ew.

yasaktır. Madde (2): Tüm yetkili merciler, bu kararın hükümlerini her biri kendi yetki alanında uygular. Bu karar, Resmî Gazetede yayımlanır ve yayım tarihinden itibaren yürürlüğe girer.[233]

2.2 Filistin Siber Suçlar Yasası

2.2.1 Filistin Siber Suçlar Yasası'nda Dijital Mahremiyet Hakkının Ele Alınışı

Filistin Yönetimi Başkanı Mahmud Abbas, 2017 tarihli 16 Sayılı Siber Suç Yasası'nı kabul etmiştir. Yasa, tam bir gizlilik içinde onaylanmış ve internette ifade özgürlüğünü ve mahremiyeti tehdit eden geniş hükümler içermesi nedeniyle Filistin insan hakları örgütleri tarafından çeşitli itirazlarla karşılanmıştır. Zira insan hakları örgütleri, bu yasanın insan hakları sistemini tehdit eden en tehlikeli mevzuatlardan biri olarak değerlendirmiştir. Yasa, dijital veri ve bilgilerin eklenmesine, silinmesine veya yayınlanmasına yol açan yasa dışı erişimi suç sayan 4. Madde ve ayrıca kişilerin özel yaşamına, aile işlerine veya onunla ilgili her türlü bilgileri keyfi veya yasa dışı bir şekilde müdahale edilmesini yasaklayan 22. Madde gibi bazı mahremiyet güvencelerini sağlamaktadır.

Ancak bu yasa, Özel hayatın gizliliği hakkı, düşünce ve ifade özgürlüğü ve bilgi edinme hakkı ile ilgili ihlaller temsil eden çeşitli hükümler içermektedir. Zira yasa, kamu kurumlarına vatandaşların çevrimiçi faaliyetlerine ilişkin verileri izleme ve kolluk kuvvetlerinin talepleri doğrultusunda bilgilerini toplama, saklama ve aktarma konusunda geniş yetkiler vermiştir. Ayrıca yasa, hizmet sağlayıcıların kullanıcı verilerini ve özel bilgilerini en az üç yıl süreyle toplamasını ve güvenlik kurumlarıyla iş birliği içinde saklamasını zorunlu kılmaktadır. Filistin Yönetimi, özellikle söz konusu yasanın yürürlüğe girmesinden sonra gazetecileri tutuklamak ve çeşitli muhalif haber sitelerini engellemek amacıyla bir kampanya başlatmıştır. Bu nedenle farklı uluslararası kuruluşlar, Siber Suçlar

[233] Filistin Mahkemelerinin Yasaları ve Kararları Ansiklopedisi, Qarar Majlis Alwuzara' Bialbayanat Alshakhsia Alkhasa Bialmuatinin (2019) (TR: Vatandaşların Kişisel Verileriyle İlgili 2019 Tarihli (3) Bakanlar Kurulu Kararı), erişim 04 Aralık, 2021, https://2u.pw/EKcCt.

Yasası'nın uygulanmasını kınamış ve Birleşmiş Milletler, Filistin Yönetimi'nin onayladığı uluslararası standartlarla çeliştiğinden dolayı yasanın hükümlerinden endişelerini dile getirmiştir.[234]

Filistin Yönetimi'nin bu yasaya nedeniyle karşı karşıya kaldığı yerel ve uluslararası baskılar sonucunda ilgili makamlar yasada değişiklik yapmak zorunda kalmıştır. Filistin, 2018 tarihli 10 sayılı yasayı çıkarmıştır. Ancak bazı gazetecilerin tutuklanmasına esas teşkil eden 20. Maddenin iptal edilmesi, sert cezaların hafifletilmesi ve "milli birlik" ve "kamu düzeni" gibi açıkça tanımlanmayan kavramlarla ilgili suçları ilga edilmesi gibi bazı değişikliklerin yapılmasına rağmen yasa, kolluk güçlerine geniş yetkiler verilmesi ve web sitelerinin engellenmesi gibi itiraz nedeni olan çeşitli maddeleri çıkartmamıştır. Bundan sonra söz konusu yasanın mahremiyete yasal koruma sağlayan maddelerini ele alacağız. Aynı zamanda Filistin Yönetimi tarafından onaylanan uluslararası anlaşma ve sözleşmeleri, Filistin Temel Yasası'nı ve onun anayasal ilkelerini ihlal eden yasadaki yasal boşluklar inceleyeceğiz.
İlk olarak yasanın 4. maddesi, bilgi sistemleri, sanal siteleri ve internet için önleyici koruma sağlamıştır. Zira bu madde, bilgisayarlara ve dijital ağlara yasadışı erişimi suç saymış ve 4 bent içermiştir:

1. web sitesine, bilgi sistemine, internete veya bilgi teknolojisinin herhangi bir aracına ya da bunların bir kısmına herhangi bir surette kasten ve haksız bir şekilde erişen veya izin verilen erişimin süresini aşan ya da bundan haberdar olduktan sonra orada kalmaya devam eden kişiler, hapis cezası veya iki yüz Ürdün dinarından az ve bin Ürdün dinarından fazla olmamak üzere ya da dolaşımdaki yasal para birimindeki eşdeğeri ile para cezası veya her ikisi ile cezalandırılır.

[234] Nader Mamoun, *Dirasat Tahadiyat Alhuquq Alraqamia Fi Filastin (TR: Filistin'de Dijital Hakların Zorlukları Üzerine Bir Araştırma)*, 1.b., Ramallah: Filistin Kalkınma ve Medya Özgürlükleri Merkezi, 2019, s.13.

2. Bu maddenin 1. Bendinde belirtilen fiil, devlet verilerine karşı işlenirse, altı aydan az olmamak üzere hapis veya beş yüz Ürdün dinarından az ve iki bin Ürdün dinarından fazla olmamak üzere ya da dolaşımdaki yasal para birimindeki eşdeğeri ile para cezası veya her ikisi ile cezalandırılır.

3. Erişim sonucunda bilgi sisteminde saklanan verilerin veya dijital bilgilerin iptal edilmesi, silinmesi, eklenmesi, ifşa edilmesi, yok edilmesi, değiştirilmesi, aktarılması, ele geçirilmesi, kopyalanması, yayınlanması veya yeniden yayımlanması, kullanıcılara veya yararlanıcılara zarar verilmesi ya da bir internet sitesinin değiştirilmesi, iptal edilmesi veya içeriğinin değiştirilmesi, unvanını, tasarımlarını veya kullanım şeklini istismar edilmesi veya sahibinin ya da onu işletenin kimliğinin çalınması gibi durumlarda bir yıldan az olmamak üzere hapis veya bin Ürdün dinarından az ve 3 bin Ürdün dinarından fazla olmamak üzere ya da dolaşımdaki yasal para birimindeki eşdeğeri ile para cezası veya her ikisi ile cezalandırılır.

4. Bu maddenin 3. bendinde belirtilen fiil, devlet verilerine karşı işlenirse, beş yıldan fazla olmamak üzere hapis ve üç bin Ürdün dinarından az ve beş bin Ürdün dinarından fazla olmamak üzere ya da dolaşımdaki yasal para birimindeki eşdeğeri ile para cezası ile cezalandırılır.”

4. Madde hükümlerini ele aldığımızda, Filistinli yasa koyucunun 1. Bentte olduğu gibi bilgi sistemlerine, web sitelerine ve internete yasadışı erişimle sınırlı kalan suçun basit hali ile 3. Bentte olduğu gibi veri ve bilgilerin iptal edilmesi, silinmesi veya eklenmesi gibi sonuçlara yol açan erişim suçunun ağır hali arasında ayrım yaptığını görmek mümkündür. Ayrıca Filistinli Yasa koyucu, 1. Bentte hapis cezasının süresini açık ve net bir şekilde belirtmediği ve yargı kararına bıraktığı fark edilmiştir. Bu bağlamda Siber Suçlar Yasası’nın 1. maddesi hapis cezasını bir haftadan üç yıla kadar olarak ele almıştır. Bu maddeye göre, “hapis cezası:

mahkeme kararıyla hüküm giyen kişinin bir haftadan üç yıla kadar değişen sürelerle devlet hapishanelerinde hapsedilmesi" olarak tanımlamaktadır. Bu tanım, daha fazla detaylandırılması gereken geniş bir hüküm olarak kabul edilmektedir.

Filistinli yasa koyucu, yasadışı erişimin cezasını genel olarak ve özellikle suçlunun kastına göre ağırlaştırmıştır. Zira bu suçun basit hali için hapis cezası veya iki yüz Ürdün dinarından az ve bin Ürdün dinarından fazla olmamak üzere para cezası belirlemiştir. Ancak söz konusu suçun ağır hali için bir yıldan az olmamak üzere hapis veya bin Ürdün dinarından az ve 3 bin Ürdün dinarından fazla olmamak üzere para cezası koymuştur. Filistinli yasa koyucu, basit haliyle yasa dışı erişim suçunun devlet verilerine yönelik işlendiğinde cezayı ağırlaştırmıştır. Ayrıca bu yasa dışı erişim nedeniyle devlet verilerinin silinmesi, kopyalanması, değiştirilmesi veya yayınlanması gibi sonuçlar meydana geldiği durumunda cezanın daha ağır hale getirmiştir. Bunun aksine Filistinli yasa koyucu, kişisel verilerin ihlal edilmesine yönelik cezaları ağırlaştırmamıştır. Ancak beş yıla hapis ve 5 bin Ürdün dinarına para cezalarına varan devlet verileri ile ilgili cezalarda olduğu gibi kişisel veri ve bilgilerin özellikle silinme ve ifşa edilme durumlarında korumasını daha ağır cezalarla sıkılaştırılması gerekliydi.[235]

Ürdünlü yasa koyucunun aksine Filistinli yasa koyucu, yasadışı erişimin bilgisayar korsanlığı veya kötü amaçlı programlar yoluyla olup olmadığı konusunda ayrım yapmamıştır. Ancak yasanın 26. Maddesine göre, "Kullanım amacıyla bir cihaza, programa veya herhangi bir hazır dijital veriyi, şifreyi veya erişim kodlarını ele geçiren ya da yasada öngörülen suçların birini işlemek amacıyla bunları sağlayan, üreten, dağıtan, paylaşan, yayınlayan veya tanıtan herkes, beş yıla kadar hapis cezası ve üç bin Ürdün dinarından az ve beş bin Ürdün dinarından fazla olmamak üzere ya da dolaşımdaki yasal para birimindeki eşdeğeri ile para cezası ile

[235] Abuallah Mahmud, "Jarimat Aldukhul Ghayr Almashrue Wfqaan Lilqarar Biqanun Raqm (10) Lieam 2018 Bishan Aljarayim Al'iiliktrunia Alfilastinii" (TR: Siber Suçlara İlişkin 2018 Tarihli 10 Sayılı Filistin Yasası Uyarınca Yasadışı Erişim Suçu), *Al-Quds Açık Üniversitesi İnsan ve Sosyal Araştırmalar Dergisi*, 1/48 (2019), ss.4-7.

cezalandırılır.” Filistinli yasa koyucu, kullanılıp kullanılmadığına bakılmaksızın, kötü amaçlı bir programa sahip olmak gibi suça hazırlayıcı bazı fiilleri suç saydığı bu tür programların elde bulundurulmasının cezasının yasa dışı erişim cezasından daha ağır olduğu görülmektedir.[236]

Aynı şekilde Filistinli yasa koyucu, eylemde suç kastı olması gerekliliğini şart koşmamış ve failin niyetini, kastını veya yanlışlıkla yapıp yapmadığı konusunu tespit etmekle uğraşmaksızın verilerin yok edilmesi, imha edilmesi, paylaşılması gibi unsurların failin cezasını artırmak için ağırlaştırıcı sebepler olduğuna kanaat getirmiştir. Böylece Filistinli yasa koyucu, yasa dışı erişim eylemini kasta bağlayan ve suçun verileri silme veya iptal etme kastıyla olması durumunda kastın önceden belirlendiğinden dolayı eylemin silme veya iptal etme amacını geçekleştirilip gerçekleştirilmediğine bakılmaksızın ağır suç olduğuna karar veren Ürdünlü yasa koyucundan farklı bakmıştır.

Ayrıca yasanın 5. Maddesine göre, “İnternet ağı veya herhangi bir bilgi sistemi aracılığıyla gönderilenleri kasıtlı olarak ele geçiren, engelleyen, gizlice dinleyen, değiştiren veya silen kişi, bir aydan az ve bir yıldan fazla olmamak üzere hapis ve (200) iki yüz dinardan az ve (1.000) bin dinardan fazla olmamak üzere para cezası ile cezalandırılır”. Aynı zamanda 6. madde, “internet ağı aracılığıyla kasıtlı ve izinsiz bir şekilde kredi kartı bilgi sisteminden herhangi bir veri veya bilgiyi ya da finansal veya sanal bankacılık işlemlerinin yürütülmesinde kullanılan veri veya bilgileri elde eden kişileri” cezalandırmaktadır.

Buna ilaveten yasanın 7. Maddesi, internet veya herhangi bir bilgi teknolojisi aracı ile yapılan her türlü iletişim saldırısını suç saymıştır. Buna göre madde, "İnternet veya bilgi teknolojisi vasıtasıyla gönderileni ele geçiren, kaydeden, müdahale eden veya kasten ve haksız bir

[236] Mahmud, a.g.m., s.9.

şekilde dinleyen herkes bir yıldan az olmamak üzere hapis veya bin Ürdün dinarından az ve üç bin Ürdün dinarından fazla olmamak üzere ya da dolaşımdaki yasal para birimindeki eşdeğeri ile para cezası veya her ikisi ile cezalandırılır". Dolayısıyla iletişime saldırma suçu kasıtlı bir suç olarak kabul edilmiştir. Başka bir deyişle Filistinli yasa koyucu, 7. Maddede belirttiği gibi söz konusu suçun kast unsuruna sahip olması gerektiğini ve özel hayatın gizliliği hakkına yönelik saldırıların "kasten ve haksız bir şekilde" olması şartını koştuğunu açıklamıştır. Ürdünlü yasa koyucunun yaptığı gibi Filistinli yasa koyucu, bu maddeyi İletişim Yasası'nın 92. maddesi ile benzer düzenlemiş ve aynı şekilde İletişim Yasası'ndaki ceza miktarını 200 Ürdün dinardan fazla olmayacak şekilde açıklarken Siber Suçlar Yasası'ndaki ceza, 1000 Ürdün dinarından fazla olmayacak şekilde koymuştur.

Siber Suçlar Yasası'nın 22. Maddesine göre: "1. Herhangi bir kişinin özel yaşamına, ailesine, evine veya iletişimine keyfi veya yasa dışı müdahaleler yasaktır. 2. Bir web sitesi, uygulama veya dijital hesap oluşturan veya internet ya da bilgi teknolojisinin herhangi bir aracını kullanan ve doğru dahi olsa bile başkaların özel veya aile hayatını yasa dışı bir müdahale temsil eden doğrudan veya kayıtlı olarak haber, resim, ses veya video kayıtlarını paylaşmak niyetiyle bilgi yayınlayan herkes, bir yıldan az olmamak üzere hapis veya bin Ürdün dinarından az ve 3 bin Ürdün dinarından fazla olmamak üzere ya da dolaşımdaki yasal para birimindeki eşdeğeri ile para cezası veya her ikisi ile cezalandırılır".

22. maddenin birinci bendi, bireyin özel yaşamına, ailesine, evine veya iletişimine keyfi veya yasa dışı müdahaleleri yasaklamasına Filistinli yasa koyucu, özellikle keyfi müdahaleleri gerçekleştirenlerin çoğu resmi devlet kurumları olduğundan dolayı meydana gelen müdahaleler ve mahremiyet ihlallerine bir ceza vermemiştir. Bu müdahalelerin cezasının belirtilmesi ve davanın zamanaşımına uğramadığının vurgulanması, bireyin kişisel özgürlüklerine ve özel hayatının gizliliğine yönelik her türlü saldırıdan kaynaklanan cezai veya medeni dava, zamanaşımı ile düşmeyen bir suç sayan Filistin Temel Yasası'nın 32. Maddesiyle tutarlı olması açısından önemlidir. İkinci bende gelince ise, Filistinli yasa

koyucunun zarar görme şartını zorunlu kılmadan suç kapsamını genişlettiğini görüyoruz. Zira yasa dışı müdahale ile ilgili bir sitenin veya uygulamanın oluşturulması, hiçbir zarar olmasa bile ceza için yeterli bir sebep saymıştır.[237]

Madde, bir kamu hakkıyla değil, bir kişilik hakkıyla bağlantılı olmasına rağmen, soruşturmayı mağdurun şikayetine bağlamamış ve tüzel ile özel kişiler arasında da ayrım yapmamıştır. Bağımsız İnsan Hakları Komisyonu gibi çeşitli insan hakları örgütleri tarafından yapılan gözlemlerde, bu bendin yeniden yazılıp tehdit suçu olarak değil, zarar suçu olacak şekilde değiştirilmesi gerektiği savunulmuş ve cezai kovuşturmanın zarar gören tarafın şikayetine bağlanması istenmiştir. Aynı zamanda bu gözlemlerde, tüzel ile özel kişilerin özel hayatları arasında ayrım yapılmasını talep edilmiştir. Bu da yasanın tüzel kişiliği tanımlayan bir hükümle yeniden yazılmasını gerektirmektedir.[238]

Yasanın 27. maddesine göre ceza, fail çalışan ise üçte bir ve hizmet sunan bir çalışan ise üçte iki oranında ağırlaştırılacaktır. Buna göre, “bu yasada belirtilen suçlardan herhangi birini, işini yaparken yetkilerini ve otoritesini kötüye kullanarak işleyen veya işi nedeniyle suçu başkaları için kolaylaştıran her çalışanın cezası üçte bir oranında artırılır.” Ayrıca çalışan hizmet sunan bir çalışan olunca madde, "bu yasada belirtilen suçlardan herhangi birini, işini yaparken yetkilerini ve otoritesini kötüye kullanarak işleyen veya işi nedeniyle suçu başkaları için kolaylaştıran her hizmet sunan çalışanın cezası üçte iki oranında artırılır". Maddede belirtildiği gibi, çalışan terimi, kamu veya özel sektör, özel kuruluşlar, yerel ve sivil kurumlar, dernek veya devletin katkı sağladığı özel şirketler gibi yerlerde çalışan herkesi kapsamaktadır. Hizmet sunan çalışan ise, “bilgi teknolojisi aracılığıyla kullanıcılara

[237] Mahmud, a.g.m., s.13.
[238] “Alhayyat Turahib Bisudur Alqarar Biqanun Raqm (10) Lisanat 2018 Bishan Aljarayim Al'iiliktrunia Watuqadim Majmuea Min Almulahazat Waltahafuzat” (TR: Komisyon, Siber Suçlarla İlgili 2018 Tarihli 10 Sayılı Yasanın Yayınlanmasını Memnuniyetle Karşılamakta ve Bir Dizi Gözlem ve Çekince Sunmaktadır), Bağımsız İnsan Hakları Komisyonu-Şikâyet Kurulu, erişim 03 Aralık, 2021, https://2u.pw/SCthWj.

bağlanma hizmetini sunan veya herhangi bir elektronik hizmet ya da bu hizmetin kullanıcıları adına bilgisayar verilerini işleyen, depolayan veya barındıran herhangi bir kişi".

Ayrıca yasanın 28. maddesine göre, yasada öngörülen suçlardan herhangi birinin işlenmesine teşvik veya yardım eden herkes, asıl fail için öngörülen cezalarla cezalandırılır. Buna göre, "Bu yasada belirtilen suçlardan birini, herhangi bir dijital araçla ve herhangi bir şekilde işlemeye teşvik eden, yardım eden veya bunu başkasıyla işlemeye anlaşan herkes, bu teşvik, yardım veya anlaşma sonucunda suç işlenirse, asıl fail için öngörülen cezalarla cezalandırılır."

2.2.2 Siber Suçlar Yasası'ndaki Yasal Boşluklar

Siber Suçlar Yasası, mahremiyeti doğrudan kapsamamış ve sağladığı bazı güvencelere rağmen, birçok maddede anayasal ilkeleri ihlal etmiş ve Filistin Ceza Muhakemeleri Usulü Yasası'nda iletişimin izlenmesine ilişkin güvenceleri devre dışı bırakmıştır.

İlk olarak yasanın 3. maddesi, askeri güçler dahil olmak üzere tüm güvenlik kurumlarına siber suçların takibinde adli kontrol yetkisini geniş bir kapsamla vermiştir. Bu maddeye göre, "1. Siber Suçlar Birimi adı altında polis ve güvenlik güçlerindeki adli kontrol görevlilerinden oluşan özel bir ihtisas birimi kurulur ve bu birim, Savcılık tarafından kendi yetki alanı içinde yargısal denetime tabi tutulur. 2. Asliye mahkemeleri ve başsavcılığı, yetkilerine göre suç davalarını inceler". Keyfi gözaltı olasılığını artıran ve güvenlik güçlerine özgürlükler üzerinde daha fazla kontrol sağlayan bu yasa, ortaya koyduğu hükümleri uygulama sürecinde yetki ve görev açısından çeşitli güvenlik güçleri arasında karışıklık yaşanmasına yol açmaktadır. Ayrıca bu yasa, Filistin'in onayladığı Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme'nin 9. Maddesinin hükümlerini ihlal etmektedir.[239]

[239] Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'nin 9. Maddesine Göre, "Herkesin Kişi Özgürlüğü ve Güvenliği Hakkı Vardır. Hiç Kimse Keyfi Olarak Tutuklanamaz veya Gözaltına Alınamaz. Yasada Belirtilen

Gevşek dil, siber suç hukukundaki en belirgin yasal boşluklardan biridir. Zira olması gereken şey, ceza hükümlerinin açık ve net olması ve dolayısıyla yargı ve güvenlik güçlerinin görevi sadece suçları araştırıp soruşturmakla sınırlı kalmasıdır. Bununla birlikte yasanın bazı maddeleri, genel ahlak, ırkçı nefret, milli güvenlik, iç barış, kamu düzeni ve benzeri ifade ve terimlere yer vermiştir. 2018 yılında yapılan değişiklikler bu terimlerin bir kısmını kaldırsa da birçoğu hala yasanın metinlerinde yer almaktadır. Düşünce ve ifade özgürlüğü hakkının geliştirilmesi ve korunmasına ilişkin Özel Raportör'ün raporuna göre, "ulusal güvenlik" gibi geniş ve muğlak terimlerin kullanılması, devletlerin genellikle insan hakları savunucularını, gazetecileri ve aktivistleri hedef alan eylemleri meşrulaştırması için bir araçtır.[240]

Bununla birlikte yasa, internet servis sağlayıcılarının abonelere ait veri ve bilgileri 3 yıldan az olmamak üzere saklamasını ve Başsavcının talimatıyla yetkili makamlara vermesini gerekli kılmıştır. Zira yasanın 31. Maddesine göre, "İnternet servis sağlayıcısı, yerleşik yasal prosedürlere uygun olarak şunları yapmakla yükümlüdür: 1. Yetkili makamlara, savcılığın veya yetkili mahkemenin talebi üzerine, gerçeğin ortaya çıkmasına yardımcı olacak abone bilgilerini sağlamak. 2. Bu yasanın 39. maddesinde yer alan usulleri dikkate almak şartıyla yargı makamlarının kendisine verdiği talimata istinaden internette bir bağlantı, içerik veya uygulamanın engellemek. 3. Abone bilgilerini bu maddenin 1. bendinde belirtilen amaçlar doğrultusunda en az üç yıl süreyle saklamak. 4. Yetkili mahkeme hakiminin kararına dayanarak dijital bilgi ve verilerin toplanması, kaydedilmesi ve bunların geçici olarak saklanması konusunda ilgili makamlara yardım edip iş birliği yapmak".

Sebepler ve Belirlenen Usule Uygun Olmadıkça Hiç Kimse Özgürlüğünden Yoksun Bırakılamaz", erişim 13 Aralık, 2021, https://2u.pw/Jllqm.

[240] Düşünce ve İfade Özgürlüğü Hakkının Geliştirilmesi ve Korunmasına İlişkin Özel Raportör'ün Raporu. s.61, erişim 17 Şubat, 2022, https://2u.pw/6P7UT.

Aynı zamanda 33, 34 ve 36. Maddelerde olduğu gibi Siber Suçlar Yasası, çeşitli hükümlerde yargıdan izin alma şartını belirtmeden başsavcıya kullanıcıların mahremiyetini ihlal etme yetkisini geniş bir kapsamla vermiştir. Bu durum, herhangi bir giriş, arama veya takip emrinin bir sivil mahkeme hâkimi tarafından verilmesi gerektiğini vurgulayan iletişimin izlenmesinde insan hakları standartlarının uygulanmasına ilişkin uluslararası ilkelerle çelişmektedir. Zira 34. Maddenin 2. Bendi, başsavcıya veya yardımcılarından birine iletişim hareketleri izleme yetkisi vermiştir.

Bu bende göre, "başsavcı veya yardımcılarından biri, iletişim hareketleri, dijital bilgiler, geçiş verileri veya abone bilgileri de dahil olmak üzere soruşturmaların menfaati için gerekli gördüğü her türlü verinin birinci fıkrada belirtilen amaçlar doğrultusunda uygun teknik araçları kullanarak ve gerektiğinde sundukları hizmetin türüne göre servis sağlayıcılarından yardım isteyerek derhal toplanmasını ve sağlanmasını emredebilir". Söz konusu bent, yargının onayına yer vermeyerek başsavcının veya yardımcılarından birinin iletişim hareketlerini izleme emri ile yetinmiştir. Bu durum, iletişim ve telefon görüşmelerinin takip edilmesi konusunda sulh hakiminden başsavcıya veya yardımcılarından birine izin vermesini öngören aynı maddenin birinci bendi ile ters düşmektedir. Bu bende yapılan itiraz, aslında savcılığın yargının karar vereceği ceza davasında karşı taraf olduğu gerçeğinden kaynaklanmaktadır.[241]

Aynı şekilde yasanın 34. Maddesi, izleme yetkisinin verilmesinin yalnızca mahkeme kararıyla sınırlı olduğunu öngören uluslararası sözleşmeleri ve standartları ihlal etmektedir.[242] Ayrıca düşünce ve ifade özgürlüğü hakkının geliştirilmesi ve korunmasına ilişkin Özel Raportör'ün İnsan Hakları Konseyi'ne sunduğu raporuna göre, "Devletler, iletişim ve bilgi teknolojisinin gözetimini, ifade özgürlüğü ve mahremiyet haklarını ihlal

[241] Esam Abdin, "Mulahazat Muasasat Alhaqi Ealaa Mashrue Alqarar Biqanun Almueadal Liljarayim Al'iiliktrunia" (TR: Al-Haq Kurumunun Siber Suçlar Yasası Hakkındaki Yorumu), Al-Haq Kurumu, erişim 17 Mayıs, 2022, https://2u.pw/L37Zk.

[242] "Alhayyat Turahib Bisudur Alqarar Biqanun Raqm (10) Lisanat 2018 Bishan Aljarayim Al'iiliktrunia Watuqadim Majmuea Min Almulahazat Waltahafuzat" (TR: Komisyon, Siber Suçlarla İlgili 2018 Tarihli 10 Sayılı Yasanın Yayınlanmasını Memnuniyetle Karşılamakta ve Bir Dizi Gözlem ve Çekince Sunmaktadır), Bağımsız İnsan Hakları Komisyonu-Şikâyet Kurulu, erişim 03 Aralık, 2021, https://2u.pw/SCthWj.

edebilecek ve demokratik bir toplumun temellerini sarsabilecek son derece müdahaleci bir eylem olarak görmelidir. Bu anlamda mevzuat, devletin çok istisnai durumlar dışında gözetim yapmamasını ve bunun münhasıran bağımsız bir yargı merciinin gözetiminde olmasını şart koşmalı.[243] Ayrıca yasalar, olası tedbirlerin niteliği, kapsamı, süresi, kullanma dayanağı ve ulusal mevzuatta yer alan çözüm mekanizmeleri hakkında açık güvenceler içermelidir."[244]

Değiştirilen yasa maddelerinin arama emrinin süresini belirtmesine ve sanığın veya elinde delillerin bulunduğu kişinin bulunmasını şart koşmasına ve arama tutanağına imza etmesini gerekli kılmasına rağmen bu maddeler, Filistin Temel Yasası'na aykırı olduğu söylemek mümkündür. Filistin Temel Yasası'nın 11/2. maddesinde yasa hükümlerine uygun olan yargı kararı olmadıkça hiç kimsenin tutuklanamayacağı, aranamayacağı, hapsedilemeyeceği, herhangi bir şekilde özgürlüğünü kısıtlanamayacağı veya hareketine engel olunamayacağı belirtilmiştir. Aynı şekilde bu maddeler, Ceza Muhakemeleri Usulü Yasası'nın iletişimin izlenmesine ilişkin 51. maddesinin ikinci bendinde yer alan güvenceleri ihlal etmektedir.

C. Güncel Uygulamalar

Daha önce bahsi geçen bazı yasal metinlerin mahremiyet hakkına ilişkin anayasal ve yasal güvenceler sağladığını görünse de söz konusu güvenceler, diğer Ürdün ve Filistin yasaları ve iki ülkenin vatandaşlarının yaşadığı mahremiyet ihlali vakaları ışığında değerlendirildiğinde geniş genel kurallar olduğunu görmek mümkündür. Aynı zamanda yeterli anayasal korumanın bulunmaması ve yasal düzenleme çerçevelerin olmaması gibi durumlar, yalnızca dijital mahremiyet hakkının ihlaline yol açmamakta ve aynı zamanda siyasi haklar ve fikir beyan etme hakkı başta olmak üzere çeşitli temel ve anayasal hakkın ihlaline uzanmaktadır. Bu nedenle aşağıda anayasal koruma ve yeterli yasal düzenleme gibi faktörlerin yokluğuna

[243] Abdin, a.g.e.
[244] Düşünce ve İfade Özgürlüğü Hakkının Geliştirilmesi ve Korunmasına İlişkin Özel Raportör'ün Raporu- İnsan Hakları Konseyi 2013, erişim 22 Aralık 2021, https://2u.pw/aUdDR.

açıkça gösteren Covid-19 pandemisinin dijital mahremiyet hakkının ihlalleri üzerindeki etkisini ele alıyoruz:

1. Covid-19 Pandemisinin Ürdün'de Dijital Mahremiyet Üzerindeki Etkisi

2020 yılının başlarında Covid-19 pandemisinin başlamasıyla birlikte, dünyanın her yanındaki hükümetler salgınla mücadele etmek ve onu kontrol etmeye çalışmak için dijital teknolojileri kullanmıştır. Bu çabalar, akıllı telefon uygulamaları, takip bileklikleri, termal kameralar ve benzeri gelişmiş teknolojilere dayanmıştır. Bu teknolojilerin en önemlisi, hasta kişilerin bulunduğu yerleri takip etme, kendisine yakın olan kişileri belirleme ve onlara hasta bir kişiyle temaslı olup hastalanma riskine maruz olduklarını bildirme tekniklerine dayanarak virüsü kontrol altına almaya yardımcı olmak için kişileri izlemeyi amaçlayan akıllı telefon uygulamalarıydı. Bu tür uygulamalar, hasta kişilerin bulunduğu yerleri belirlemekte olan güçlü imkanlarıyla virüsün yayılmasını sınırlamayı ve yayılma hızına ayak uydurmayı amaçlamıştır. Ancak diğer dijital teknolojiler gibi söz konusu uygulamalar, özellikle etkinlik ve mahremiyet ihlalleri gibi konularla ile ilgili sorunlarla karşı karşıyadır. Bu bağlamda insan hakları kuruluşları, bireyleri izleme ve takip etme uygulamalarının kullanıcı verilerini koruması için çeşitli standartlar geliştirmiştir. Aynı zamanda uygulamaların mahremiyet hakkını ihlal etmesini önlemek için güncel bir yasal çerçeveye duyulan ihtiyacı vurgulamıştır.[245]

Bu bağlamda Ürdün, Sağlık Bakanlığı ile ortaklaşa bir grup uzman gönüllü tarafından geliştirilen ve temaslıları takip etmek ile virüsün yayılmasını sınırlamak için bir sosyal girişim olarak sunulan (Aman) uygulamasını Mayıs 2020 tarihinde başlatmıştır. İlk aşamalarda Ürdün, vatandaşların uygulamayı indirmesini şart koşmamış ancak daha sonra birçok kamu hizmetini uygulamayı indirme şartına bağlayarak indirmesi zorunlu hale

[245] Reem Al-Masry, "Tatbiq 'Aman Litatabue Almukhalitin: 'Asyilat Al'aman Walkhususia" (TR: Temaslı Kişileri Takip Etme Uygulaması "Aman": Güvenlik Ve Gizlilik Soruları), Hiber Magazine, erişim 19 Ocak 2022, https://2u.pw/Fs6iv.

gelmiştir. Aynı zamanda restoranlar ve spor kulüpleri gibi çeşitli tesislerin yeniden açılmasına ilişkin genelgeler, söz konusu uygulamanın indirilmesini şart koşmuştur. Bununla birlikte Ürdün'e ve Ürdün'den seyahat eden yolcular ve devlet dairelerini ile kamu kurumlarını müracaat eden veya ziyaret eden kişiler uygulamayı indirmek zorunda kalmıştır.[246]

Uygulamanın tasarlayanlar, Bluetooth teknolojisi aracılığıyla konum belirleme koordinatlarına dayanmıştır. Bu teknoloji, kişinin yaya, araba veya başka bir ulaşım aracıyla gezindiğini belirlemek ve belirli bir konumda harcadığı zamanı hesaplamak için hareket verilerinin çalışmasını gerektirmektedir. Bundan sonra uygulama, hareket verilerini kullanıcının cihazında 14 gün boyunca saklı tutarak hasta kişinin verilerini içeren bir dosya olarak Sağlık Bakanlığı'na göndermektedir. Ayrıca o dönemde Sağlık Bakanlığı, kullanıcı cihazının mahremiyetini ve gizliliğini korumak için gerekli talimatları yayınlamıştır.[247]
Ancak o dönemde birçok Ürdünlü hukukçu, Ürdün hükümetinin vatandaşların mahremiyetine sızarak ihlal etmesinden duydukları korkuyu dile getirmiştir. Ürdün Açık Kaynak Derneği, Ürdün'e temaslı kişileri takip etme uygulamalarıyla ilgili Dünya Sağlık Örgütü tarafından belirlenen hususlara ve standartlara uyulması ve kişisel Verileri koruma yasalarının olmadığında vatandaşların mahremiyetini korumak için yasal garantiler sağlanması için çağrıda bulunmuştur. Zira söz konusu uygulamanın açık kaynak protokollerini kullanmaması, uygulamanın nasıl çalıştığının ve mahremiyet hakkını ile bilgi güvenliğini korumaya bağlılığının anlaşılmasını engellemektedir.[248] Ancak Ürdün Başbakanlığı, Nisan 2021 tarihinde (Aman) uygulamasının indirilmesinin zorunluğunu kaldıran bir genelge yayınlamıştır.[249]

---

[246] Al-Masry, a.g.e.
[247] Al-Masry, a.g.e.
[248] “Tatbiq "'Aman" Yukhalif Alaietibarat Al'akhlaqia Alati Wadaeatha Munazamat Alsiha Alealamia” (TR: Aman Uygulaması Dünya Sağlık Örgütü Tarafından Belirlenen Etik Hususları İhlal Ediyor), Ürdün Açık Kaynak Derneği, erişim 17 Ağustos, 2021, https://2u.pw/9kbIQ.
[249] Aljameia Al'urduniya Lilmasdar Almaftuh Turahib Biqarar Rayiys Alwuzara' Bi'iilgha' 'İilzamiat Tatbiq 'Aman” (TR: Josa Başbakanın Aman Uygulamasının (2021) Zorunluluğunu Kaldırma Kararını Memnuniyetle Karşılıyor), Ürdün Açık Kaynak Derneği, erişim 17 Ağustos, 2021, https://2u.pw/xwEEm.

2. Covid-19 Pandemisinin Filistin'de Dijital Mahremiyet Üzerindeki Etkisi

Covid-19 pandemisinin 2020 yılının mart ayında patlak vermesiyle birlikte Filistin Devlet Başkanı Mahmud Abbas, Covid-19 virüsü tehdidine karşı tüm Filistin topraklarında olağanüstü hali ilan eden bir başkanlık kararnamesi yayınlamıştır. Aynı ay içinde Abbas, olağanüstü halin amaçlarına ulaşmak için yetkili resmi makamlarca alınan karar, talimat ve usulleri ihlal edenleri bir yıla varan hapis cezası ve para cezası ile cezalandıran olağanüstü halle ilgili yasa hükmünde kararname çıkarmıştır. Olağanüstü hâl mevzuatı, çok genel ifadeler kullanarak dijital mahremiyet haklarını hedef almıştır. Söz konusu yasa hükmünde kararnamenin 3. maddesinin 3. fıkrasına göre: "Kanunen yetkisi olmayanların, olağanüstü hâle ilişkin her türlü yazılı, işitsel ve görüntülü tüm sosyal medya aracılığıyla herhangi bir açıklama veya beyanda bulunması veya bu duruma ilişkin resmi kaynaklara dayandırılmayan bir haber yayınlaması her ne şekilde olursa olsun yasaklanmıştır. Buna aykırı davrananlar, bir yılı geçmemek üzere hapis cezası ve iki bin Ürdün dinarından az ve beş bin Ürdün dinarından fazla olmamak üzere veya dolaşımdaki para birimindeki karşılığı kadar para cezası ile cezalandırılmaktadır". Bu madde, doğru veya gerçek olsa dahi resmi bir kaynak tarafından belirtilmeyen her türlü haber yayınlanmasını suç saymakta ve bu durum, dijital içeriklere, düşünce özgürlüğüne ve mahremiyet hakkına karşı bir kısıtlama çabası olarak değerlendirilebilmektedir.[250]

Olağanüstü hâl yasa hükmündeki kararnamesinin yanında Filistin Yönetimi, diğer ülkeler gibi, Covid-19 virüsünün bulaştığı doğrulanan hastaları ve temaslılarını takip etmek için bir dizi uygulama başlatmıştır. Filistin'de Covid-19 hastalarının hareketlerini ve karantina kurallarına uyumlarını takip etmek için tasarlanan ilk hasta takip uygulaması Filistin güvenlik güçleri tarafından geliştirilmiştir. Uygulamayı geliştiren Önleyici Güvenlik Gücü,

[250] Esam Abdin, "Alhuquq Alraqamia Fi Filastin Bayn Altawari Wajayihat Korona" (TR: Olağanüstü hâl ve Covid-19 Pandemisi Arasında Filistin'de Dijital Haklar), *Sosyal Medya Geliştirme Arap Merkezi*, 13/3 (2020), s.5.

uygulamanın uluslararası standartlara göre geliştirildiğini vurgulasa da uygulamanın kapalı kaynak teknolojileriyle geliştirilmiş olması sonucunda bilgilerin nasıl saklandığını bilmek mümkün olmadığından dolayı uygulama kimliğinin net olmaması konusunda gerçek yasal endişeler bulunmaktadır. Bununla birlikte 2020 yılının Ekim aynıda Sağlık Bakanlığı, "Amankom" adı altında hastaların temaslılarını takip etmek için yeni bir uygulamanın başlatıldığını duyurmuştur. Aynı zamanda Sağlık Bakanlığı, yeni uygulamanın çıkartılmasından sonra "Manii" adı atındaki eski bir uygulamayı kapatmıştır. "Amankom" adlı uygulama, telefonda toplanan verilerin kaydedildiği Bluetooth teknolojisine dayanmaktadır. Sağlık Bakanlığı, uygulamanın Bluetooth tabanlı olduğunu açıklamış olsa da uygulamayı deneyenler, cihazın konumuna erişmesine izin verilmeden uygulamanın açılamayacağını belirtmiştir. Sağlık Bakanlığı, uygulamanın gizlilik politikasını web sitesinde yayınlamış ancak yayınlanan gizlilik politikası, uygulamanın topladığı bilgilerin türü, kimlerin erişebileceği ve kullanım süresi gibi bazı temel bilgileri açıklamamıştır.[251]

D. Ürdün ve Filistin'deki Mevzuatın İki Ülkenin Anayasalarıyla Uyumluluğunun Karşılaştırılması

Aşağıdaki noktalarda hem Ürdün hem de Filistin'deki mevzuatın iki ülkenin anayasalarıyla ne kadar uyumlu olduğunu özetliyoruz ve ardından bu iki ülkenin mevzuatını Avrupa Birliği yasalarıyla karşılaştırmaya başlıyoruz:

1. Ürdün'deki Mevzuat

-Ceza Yasası: Ürdün Ceza Yasası'ndaki dijital mahremiyet hakkına ilişkin maddeleri incelediğimizde, özel hayatın korunması ve yazışmaların gizliliği ile ilgili anayasal maddelerle uyumlu olduğunu tespit ediyoruz. Ancak aynı zamanda bu maddelerin çağın ruhuna ve modern teknolojik araçların kullanımından kaynaklanan yeni hukuki sorunlara ayak uyduramaması dikkat çekmektedir.

[251] Fatafta ve Samaro, a.g.m., s.39.

-Suçu Önleme Yasası: Valiye yazışma ve kişisel görüşmelerin hiçbirine erişme yetkisini doğrudan vermemesine rağmen yasanın 5. Maddesi, bu yetkiyi kendisine dolaylı bir şekilde vermiştir. Bu durum da yargı kararları olmadan böyle bir yetkiyi yasaklayan anayasal hüküm ve ilkelere aykırıdır.

- İletişim Yasası: İletişim Yasası'nın 56. maddesi, telefon görüşmelerinin ve iletişimlerin gizliliğini öngörmekte ve mahremiyetlerinin ihlalini yasaklamaktadır. Ayrıca aynı yasanın 71. maddesi, konumu gereği gördüğü gizli yazışmaları yayınlayanları da cezalandırmaktadır. Bununla birlikte 76. ve 77. maddeler, yazışmaların içeriğininim ele geçirilmesini, engellenmesini, düzeltilmesini, saklanmasını, taşınmasını veya ifşa edilmesini cezalandırmakla birlikte kişisel verilerin kötüye kullanılmasını yasaklamıştır. İletişim Yasası'nın bu maddeleri, Ürdün Anayasası'nın 18. Maddesi ile uyumludur. Ancak bu maddeler, modern iletişim araçlarından açıkça söz etmeyip niteliklerine uygun ve bunların kullanımından kaynaklanan davaları kapsayan ayrıntılı yasal hükümlere yer vermemesi gibi önemli eksiklikleri bulunmaktadır.

İletişim Yasası'nın 29. maddesinin G bendi ise, internet servis sağlayıcılarının iletişimi denetlemeye ilişkin adli ve idari talepleri yerine getirmek için gerekli kolaylıkları sağlaması ruhsat verme koşullarından bir tanesi olarak düzenlemiştir. Böylece kişisel verilere erişimi sadece yargı kararları yoluyla sınırlı kılan anayasal hükümlerle usul açısından çelişmektedir. Genel olarak, Anayasa'da yer alan yargı kararı veya talebi şartının yasal olarak detaylıca ele alınmadığını ve bu tür karar ve taleplerin hiçbir yasada düzenlenmediğini görüyoruz. Başka bir deyişle genel olarak veri izleme sürecini düzenleyen, vatandaşların mahremiyetini garanti altına alan ve kolluk kuvvetlerinin vatandaşların verilerine ve mahremiyetine nasıl erişip incelediğini ve bu konuda hangi yetkilere sahip olduğunu açıklayan bir yasal düzenleme bulunmamaktadır.

-Medeni Yasa: Medeni Yasa'nın 48. maddesi, Kişilik haklarına yönelik saldırılardan zararların teminat altına alınmasını zorunlu kılmıştır. Ayrıca bu madde, özel hayat dahil olmak üzere tüm kişisel haklara yönelik tüm saldırıları içerecek şekilde genel düzenlenmiş ve böylece Ürdün anayasasının sağladığı korumayla uyumlu olmuştur. Ayrıca yasa koyucu, herhangi bir saldırıya uğrayan herkese tazminat hakkı ilkesini öngörmüştür.

-Ceza Muhakemeleri Usulü Yasası: Ceza Muhakemeleri Usulü Yasası'nın 88. maddesi, yazışmaların ve iletişimlerin içeriğine erişmek dahil olmak üzere başsavcının yetkilerini ve hareket alanlarını tanımlamaktadır. Bu madde, Ürdün Anayasası'nın yazışma ve telefon görüşmelerinin mahremiyetini koruma altına alan ve yargı kararı olmadan ele geçirilmelerini yasaklayan 18. maddesi ile uyumludur.

2. Filistin'deki Mevzuat

-Ceza Muhakemeleri Usulü Yasası: Bu yasanın 51. Maddesi, telefon görüşmelerinin takip edilmesini ancak yargı emirleri çerçevesinde sınırlandıran usulleri belirlemiştir. Bu maddenin metni, yazışma ve konuşmayı içeren özel hayat hakkının ihlalini suç sayan Temel Yasa ile uyumludur. Ancak Filistin'deki diğer yasalar gibi kişisel verilerin ve dijital mahremiyet hakkının korunmasını ele almamış ve özel hayat hakkına sağladığı koruma geleneksel bir yasal koruma şeklinde kalmıştır.[252]

-Filistin Medeni Yasası: Kişilik haklarının ihlalinden kaynaklanan zararın tazmini ile ilgili 59. Madde, zarar gören herkes için tazminat hakkını vurguladığı için Temel Yasa'daki anayasal ilkelerle uyumlu.

[252] 2001 Tarihli (3) Sayılı Qanun Al'iijra'at Aljazayiya Alfilastini (TR: Filistin Ceza Muhakemeleri Usulü Yasası), erişim 09 Mayıs, 2022, https://2u.pw/Wz3rZ.

-Batı Şeria'da yürürlükte olan 1954 tarihli 7 Sayılı Suçu Önleme Yasası, Ürdün çu Önleme Yasası'nın aynısıdır. Daha önce de belirttiğimiz gibi, bu yasa, Valiye yazışma ve kişisel görüşmelerin hiçbirine erişme yetkisini doğrudan sağlamamış, ancak yasanın 5. Maddesi, bu yetkiyi kendisine dolaylı bir şekilde vermiştir. Bu durum da anayasal hüküm ve ilkelere aykırıdır.

Filistin Siber Suçlar Yasası: Filistin Siber Suçlar Yasası'nın 22. maddesinin ilk paragrafı, hiç kimsenin özel hayatına, ailesine, meskenine veya yazışmalarına keyfi veya hukuka aykırı bir şekilde müdahalelere maruz bırakılamaz olduğunu belirtmiştir. Ancak yasa koyucu bu eylem için ceza koymamış ve Temel Yasa'da olduğu gibi bu davaların zamanaşımına uğramadığını belirtmemiştir. Böylece bu yasanın söz konusu maddesi, özel hayatın mahremiyetine ve kişisel özgürlüklere yönelik her türlü saldırıdan kaynaklanan cezai veya medeni davanın zamanaşımı ile düşmeyen bir suç olduğunu kabul eden Filistin Temel Yasası'nın 32. maddesiyle uyumlu olmadığı görülmektedir.[253]

Ayrıca bu yasada yapılan değişikliklerle birlikte, arama emrinin süresini belirtmesine, sanığın veya elinde delillerin bulunduğu kişinin bulunmasını şart koşmasına ve arama tutanağına imza etmesini gerekli kılmasına rağmen Filistin Temel Yasası'na aykırıdır. Zira bu yasanın hükümleri, Filistin Temel Yasası'nın 11/2. maddesinde bulunan ve yasa hükümlerine uygun olan yargı kararı olmadıkça hiç kimsenin tutuklanamayacağı, aranamayacağı, hapsedilemeyeceği, herhangi bir şekilde özgürlüğünü kısıtlanamayacağı veya hareketine engel olunamayacağı belirten hükümlerle uyuşmamaktadır. Aynı şekilde bu yasanın hükümleri, Ceza Muhakemeleri Usulü Yasası'nın iletişimin izlenmesine ilişkin 51. maddesinin ikinci bendinde yer alan güvenceleri ihlal etmektedir.

---

[253] "Alhayyat Turahib Bisudur Alqarar Biqanun Raqm (10) Lisanat 2018 Bishan Aljarayim Al'iiliktrunia Watuqadim Majmuea Min Almulahazat Waltahafuzat" (TR: Komisyon, Siber Suçlarla İlgili 2018 Tarihli 10 Sayılı Yasanın Yayınlanmasını Memnuniyetle Karşılamakta ve Bir Dizi Gözlem ve Çekince Sunmaktadır), Bağımsız İnsan Hakları Komisyonu-Şikâyet Kurulu, erişim 03 Aralık, 2021, https://2u.pw/SCthWj.

3. Ürdün, Filistin ve Avrupa Birliği Mevzuatları Arasında Dijital Mahremiyet Hakkının (Yasal) Ele Alınışının Karşılaştırılması

Dijital mahremiyet hakkının mevzuatına gelince, şimdiye kadar hem Ürdün hem de Filistin'de dijital mahremiyet hakkı konusunu düzenlemek için tahsis edilmiş özel bir mevzuat bulunmamaktadır. Ayrıca dijital mahremiyet hakkını düzenleyip koruyan ya da bunların ihlal edilmesine yasal cezalar getiren yasa maddeleri, çeşitli yerlerde dağınık bir durumdadır. Bunun aksine Avrupa Birliği, AB veri koruma kuralları olarak bilinen ve aynı zamanda "Genel Veri Koruma Tüzüğü (GPDR)" adıyla meşhur olan dijital mahremiyet hakkı konusunu düzenleyen özel mevzuat hazırlamıştır. Bu nedenle, Genel Veri Koruma Tüzüğü (GPDR) ile ilgili genel bir çerçeve sunduktan sonra Avrupa Birliği tarafından çıkarılan bu tüzükte öngörülen en önemli noktaları özetleyeceğiz. Ardından bu noktaları, Ürdün ve Filistin'de dijital mahremiyet hakkını ele alan yasal metinlerle karşılaştıracağız.

Avrupa Birliği içindeki yasa koyucular, bireylerin mahremiyetinin ve kişisel verilerinin gizliliğinin korunmasına büyük önem vermektedir. Bu ilgi, mahremiyet hakkının korunmasının Avrupa ulusal güvenliğinin ve üye ülkelerin iç güvenliğinin ayrılmaz bir parçası olduğuna olan inançlarından kaynaklanmaktadır. Genel Veri Koruma Tüzüğü (GPDR-General Data Protection Regulation), Avrupa Birliği vatandaşlarının verilerini korumak için tasarlanmış çeşitli kural ve yasalardan oluşan ve AB üyeleri tarafından 14 Nisan 2016 tarihinde onaylanıp Mayıs 2018 itibarıyla yürürlüğe geren bir yasal belgedir.

Genel Veri Koruma Tüzüğü'nden önce Avrupa, verilerin kontrol edilmesi ve korunması adına çeşitli girişimlere başvurmuştur. Bu girişimlerin en önemlilerinden Avrupa Konseyi tarafından 28 Ocak 1981 tarihinde imzaya açılan ve 1 Ekim 1985 tarihinde yürürlüğe giren Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'dir. Bu sözleşmeyi Türkiye hariç, Avrupa Konseyi'nin 47 üyesinin tamamı onaylamıştır. Ekim 1995 yılında ise Avrupa Veri Koruma Direktifi kabul edilmiş v 1998

yılında yürürlüğe girmiştir. Bu direktif, kişisel verilerin işlenmesin ancak direktifte belirtilen belirli temel ilkelerin sağlandığında mümkün olacağını belirtmiştir. Avrupa Veri Koruma Direktifi'nde belirtilen ilkeler, kişisel verilerin işlenmesi sürecinde temel hak ve özgürlükleri korumayı hedeflediği gibi Avrupa Birliği içinde kişisel verilerin işlenme sürecini ve veri aktarım özgürlüğünü düzenlemeyi amaç edinmiştir.

Ayrıca Avrupa Veri Koruma Direktifi, Avrupa Birliği'nin mahremiyet ve insan hakları yasalarının önemli bir bileşenini temsil etmektedir. Bu direktiften sonra, 2018 yılına kadar yirmi beş yıl boyunca düzenlenen çok sayıda konferans ve çalıştay aracılığıyla veri koruma sürecini reform etme ve güncelleme girişimleri sürmüştür. Sonuç olarak Genel Veri Koruma Tüzüğü (GPDR), Avrupa Birliği'ndeki 27 ulusal veri koruma rejimini birleştirmiş ve Avrupa Veri Koruma Kurulu'nun (EDPB) yerini almıştır. Aynı zamanda söz konusu tüzük, Avrupa Birliği'ndeki şirketlerin veri aktarım kurallarını iyileştirmiş ve kullanıcılara kişisel veriler üzerinde daha fazla kontrol vermiştir. [254] Ayrıca bu tüzük, Veri mahremiyeti ile ilgili bugüne kadar çıkarılmış en kapsamlı yasa olarak görülmektedir. Genel Veri Koruma Tüzüğü'nün yürürlüğe girmesi, iletişimlerin gizliliğini ve çerezlerin kullanımı düzenleyen E-Gizlilik Direktifi ve kişisel verileri işlerken AB kurumlarında uygulanan düzenlemeler gibi diğer AB düzenlemelerinin güncellenmesini gerektirmiştir.[255]

-Açık Onay: Tüzük, kullanıcının verileriyle ilgilenen kuruluşların kendisinden elde edilen herhangi bir veriyi işlemeden önce onun rızasını almakla yükümlü kılmıştır. Ayrıca tüzük, kullanıcının sessizliğini veya sadece reddetmemesini verilerini kullanmak için bir onay olarak sayan önceki uygulamanın aksine, bu kuruluşların kullanıcıdan açık bir onay almasını gerektirmiştir. Böylece tüzüğe göre kullanıcılar, verilerinin herhangi bir şekilde işlenebilmesi için önce onay vermesi lazımdır.

[254] "The History of the General Data Protection Regulation", European Data Protection Supervisor, erişim 05 Ocak, 2022, https://2u.pw/5Puvi.
[255] "A brief history of the General Data Protection Regulation (1981-2016)", International Association of Privacy Professionals, erişim 05 Ocak, 2022, https://2u.pw/yKtgn.

-Silme ve aktarma hakkı: Tüzükte öngörülen bu hak çerçevesinde Avrupa Birliği vatandaşları, verilerini elinde bulunduran herhangi bir tarafın bu verileri silmesini veya başka bir tarafa aktarmasını talep edebilir.
-Unutulma hakkı: Bu ilke, daha önce Avrupa Birliği mahkemelerinden bir tanesi tarafından onaylanmış ve tüzükte düzenlenmiştir. Bu hak, Avrupa Birliği'ndeki bireylerin internet ağında yayınlanan ve kendilerine ile isimlerine bağlı olan herhangi bir bağlantı veya verinin yetkili makamlardan silinmesini talep etmelerini sağlamaktadır. Bu durum, aynı zamanda veri denetleyicisi görevi üstlenen Google gibi arama motorları için de geçerlidir. Buna göre bireyler, bilgilerin yanlış, yetersiz, uygunsuz veya aşırı olması durumunda, adları da dahil olmak üzere web sayfalarının bağlantılarını arama motoru sonuçlarından kaldırılmasını talep edebilirler. Ayrıca şirketler, bireylerin kişisel verilerini çevrimiçi olarak kullanıma sunduğu ve bu bireyler söz konusu verilerin silinmesi talep ettiği durumlarda, verileri silmekle yetinmeyip bunların paylaşıldığı diğer web sitelerini de bilgilendirip silmelerini talep etmesi gerekmektedir.

-Kişisel verilerinize erişim: Bireyler, bir şirket veya kuruluşun sahip olduğu kendileriyle ilgili kişisel verilere erişim talebinde bulunabildiği gibi verilerinin bir kopyasını ücretsiz ve kolay bir şekilde alma hakkına sahiptir. Buna göre kuruluşlar, bireylere bir ay içinde yanıt vermeli ve kişisel verilerinin bir kopyasını ve bu verilerin nasıl kullanıldığına ilişkin tüm ilgili bilgileri sağlamalıdır.

-Kişisel verilerin düzeltilmesi: Bir şirket veya kuruluşun yanlış veya eksik kişisel veriler depoladığı durumda kişi, onlardan verilerin düzeltilmesini veya güncellenmesini isteyebilir.
-Para Cezaları: Tüzük hükümlerine aykırı davrananların şirketin piyasa değerinin %4'üne kadar veya doğrudan yirmi milyon avroya kadar para cezası ödemesi öngörülmektedir.
Ancak aynı zamanda tüzük, özellikle aşağıdaki noktalarla ilgili olarak birçok eleştiriye maruz kalmıştır:

-Tüzüğün uygulanması için tek bir mekanizmanın bulunmaması nedeniyle tüzüğün hükümlerini uygulama yöntemi farklı Avrupa ülkeleri arasında farklılık göstermesidir.
-Tüzükte belirtilen ve hükümlerini ihlal eden taraflara kesilen para cezalarının belirli miktarlarla belirlenmemesi ve bu cezaları tahsil eden taraf hakkında anlaşma sağlanmamasıdır.
-Tüzüğün uygulanması sonucunda sosyal medya siteleri başta olmak üzere kullanıcı sayısı azalan şirketlerin olumsuz etkilenmesidir.[256]

Genel Veri Koruma Tüzüğü (GPDR), verilerin özel kategorilerini "hassas" kişisel veriler olarak sınıflandırmış ve bu nedenle bu veriler özel koruma almıştır. Bu hassas veriler, ırk veya etnik kökenle ilgili verileri, siyasi görüşleri, dini veya felsefi inançları, sendika üyeliğini, Bir kişinin kimliğinin belirlenmesi amacıyla kullanılan genetik ve biyometrik verileri, Sağlık bilgilerini ve cinsel yaşam veya cinsel yönelim bilgilerini içermektedir. Genel bir kural olarak, yukarıdaki veri kategorilerinin işlenmesi yasaktır. Ancak, belirli istisnalar altında, bir şirket veya kuruluşun hassas kişisel verileri işlemesine izin verilebilir. Örneğin: genel sağlığı ve kamu yararını korumak için belirli bir hassas veri işleme eylemine izin veren yasalar bulunmaktadır. Bu durum, kamu sağlığı, istihdam ve sosyal koruma gibi farklı alanlarda hassas kişisel verilerin işlenmesini sağlayan ve yeterli güvenceleri içeren yasalar için geçerlidir.[257]

Ürdün ve Filistin'deki yasama sistemleri, dijital mahremiyet hakkını ele alıp düzenleyen özel bir yasadan yoksun olma konusunda örtüşmektedir. Buna göre bu tür özel yasaların bulunmaması sonucunda dijital mahremiyet hakkıyla ilgili yasal hükümler, çeşitli özel olmayan yasalar arasında dağınık kalacaktır. Dolayısıyla bu yasama sistemleri, dijital haklarla ilgili tüm yönleri kapsamaktan uzak kalacaktır. Bu durum, dijital mahremiyet

[256] "Data protection and online privacy", Your Europe, erişim 21 Ağustos, 2021, https://2u.pw/T4Wal.
[257] "How is data on my religious beliefs/sexual orientation/health/political views protected", European Commission, erişim 21 Ağustos, 2021, https://cutt.us/t6S4G

hakkının yasal korunmasını zayıflatmaktadır. Bunun sonucunda bireyleri, dijital dünyada paylaştıkları bilgilerden yararlanabilecek herhangi bir taraftan gelebilecek ihlallere karşı, özellikle bu bilgilerin günümüzdeki önemi göz önünde bulundurulduğunda, savunmasız bir hale getirmektedir.

Ürdün yasa koyucuları, bu gecikmeyi telafi etmeye çalışmış ve dijital mahremiyet hakkının korunmasına ilişkin bir yasa çıkarmak adına ilk adımlar 2014 yılında başlayıp meclise ulaşması sekiz yıl daha sürmüştür. Bu yasa tasarısı, şu anda meclisin bunu tartışmasını ve daha sonra onaylamaya sunmasını beklemektedir. Bireylerin verileri için genel koruma sağlamasına ve geç de olsa önemli bir gelişme olarak görülmesine rağmen bu yasa tasarısı, Ürdün'de verilerin korunmasını gözetmekten sorumlu bir makamın oluşturulmasını öngördüğü için bazı uzmanlar tarafından eleştirilmiştir.[258] Bu makam, yürütme gücüne tabi olan resmî kurumlardan oluşması nedeniyle özellikle kamu kurumlarının bu yasanın maddelerinin kapsamına giren herhangi bir ihtilaf veya ihlale taraf olması durumunda tarafsızlığından şüphe duyulmaktadır.[259]

İletişim Yasası: Hem Ürdün hem de Filistin'deki İletişim Yasaları, özellikle dijital mahremiyet hakkına ilişkin özel bir yasanın yokluğunda, dijital mahremiyetle ilgili sorunları ele almak için dayanılabilecek ana yasadır. İletişim Yasası'na dayanmak, Ürdün ve Filistin'deki yasama sistemlerinin çağın yasal ihtiyaçlarına ayak uydurmakta ve teknolojik devrimin sonucunda doğan yeni hakları ele almakta açıkça geciktiğini göstermektedir. Bu sonuç, özellikle de Ürdün İletişim Yasası'nın 1995 yılında ve Filistin İletişim Yasası'nın 1996 yılında çıkartıldığını bilince pekişmektedir.

[258] "Qanun Himayat Albayanat Alshakhsia Sayueaziz Haqa Al'urduniyiyn Fi Alkhususia Alraqamia" (TR: Kişisel Verileri Koruma Yasası, Ürdünlülerin dijital mahremiyet haklarını geliştirecek), Ürdün Açık Kaynak Derneği, erişim 09 Ağustos, 2021, https://2u.pw/kRrg8.
[259] Muswadat Qanun Himayat Albayanat Alshakhsia (TR: Kişisel Verileri Koruma Yasası Tasarısı), erişim 14 Aralık, 2021, https://2u.pw/UrcWK.

Yasal metin açısından bu iki yasa arasındaki en önemli fark, yasaların sınırları içinde olmasını gerekirse de Filistin yasasında iletişimin mahremiyetine ilişkin ve kamu kurumlarına iletişim ve yazışmalara erişme hakkını tanıyan bir istisnanın bulunmasıdır. Bununla birlikte iki yasa, yazışmaların ve çağrıların içeriğini yayınlama veya yayma ve çağrıları dinleme veya yazışmaları silme gibi belirli eylemleri suç saymak anlaşmıştır. Ancak yasa koyucuların cezaları belirlemekteki yaklaşımları farklılaşmıştır. Buna göre Filistin İletişim Yasası, cezanın en üst sınırını belirlemekle yetinirken Ürdün İletişim Yasası, cezanın hem alt hem de üst sınırlarını belirlemeye yönelmiştir.[260] [261]

Ceza Yasası: Ürdün Ceza Yasası, Filistin Ceza Yasası'nın tarihi kaynağı olduğundan dolayı iki yasa arasında köklü farklar yoktur. İki yasa arasındaki farklılıklar, Ürdün Ceza Yasası'nda yapılan bazı değişikliklerle sınırlı kalmıştır. Ancak bu farklılıklar, genel anlamda küçük kalmışken özel anlamda, Ürdün ve Filistin ceza yasalarının doğrudan ve ayrıntılı olarak bireylerin verileri üzerinde işlenebilecek ve mahremiyetleri için tehdit oluşturabilecek suçları ele almadığının gerçeğini değiştirmemiştir.

Ceza Muhakemeleri Usulü Yasası: Ceza Muhakemeleri Usulü Yasası'nın 51. maddesinin ikinci bandında, telefon görüşmelerinin takip edilmesini yargı emirleri şartıyla sınırlandırılmasına ilişkin usuller belirlenmiştir. Bu maddeye göre, "1. Başsavcı veya yardımcılarından biri, cinayet ve onu işleyen kişi ile ilgili olan telgraf ve posta ofislerinde bulunan mektupları, gazeteleri, yayınları, telgrafları ve paketleri ele koyma yetkisine sahiptir. 2. Başsavcı veya yardımcılarından biri, bir yıldan az olmayan bir süre için hapis cezası gerektiren bir suç veya kabahatte gerçeğin ortaya çıkarılmasında faydalı olacaksa sulh hakiminin iznine istinaden telli ve telsiz görüşmeleri gözetebilir ve özel bir yerde yapılan görüşmeleri kayıt altına alabilir. 3. Tutuklama emri ve gözetim veya kayıt izni, gerekçeli

[260] 1995 Tarihli ve 13 Sayılı Qanun Alaitisalat Al'urduni (TR: Ürdün İletişim Yasası ve Değişiklikleri), erişim 04 Mayıs, 2022, https://2u.pw/ru11b.
[261] Qanun Bishan Alaitisalat Alsilkia Wallaasilkia (TR: Telli ve Telsiz İletişim İle İlgili 1996 Tarihli (3) Sayılı Yasa), erişim 13 Nisan, 2022, https://2u.pw/WQj59.

olma şartıyla bir sefer yenilenebilen on beş günü aşmayan bir süre içinde olabilir".[262] Bu madde, özel konuşmalar gibi çeşitli unsurlardan oluşan özel hayat hakkının ihlalini suç sayan Temel Yasa ile uyumludur. Ancak Filistin'deki diğer yasalar gibi bu yasa, dijital haklara yer vermeden mahremiyete geleneksel şekliyle koruma sağlamıştır.

Medeni Yasa: Ürdün ve Filistin'deki medeni yasalar, zarara neden olan taradın zararın (tazminatın) garantisi gerektiren aynı maddeyi içermektedir.
Suçu Önleme Yasası: 1957 yılında çıkarılan suçların önlenmesine ilişkin aynı yasa, Ürdün ve Filistin'de yürürlüktedir. Bazen valiye yazışma ve kişisel görüşmelere erişme yetkisini verdiği şeklinde yorumlanan bu yasanın 5. maddesi, anayasal haklara aykırıdır.

Siber Suçlar Yasası: Siber Suçlar Yasası, 2015 yılında Ürdün'de ve ardından 2017 yılında Filistin'de yürürlüğe girmiştir. Öncelikle, iki yasanın neredeyse benzer koşullarda çıkarıldığını belirtmek lazımdır. Zira bu yasa, Ürdün'de çıkarıldığı sırada meclisin feshedilmiş olmasından dolayı geçici bir yasa şeklinde çıkarılmış ve benzer bir şekilde Filistin'de tam bir gizlilik içinde yürürlüğe girmiştir.

Bu İki yasanın paylaştığı temel özellik, web sitelerinin ve sosyal medya platformlarının bireylere fikirlerini ifade etmeleri için verdiği alanları daraltmayı hedeflemeleridir. Bu iki yasaya yönelik yoğun eleştirilere rağmen iki ülkenin kamu otoriteleri, internet ağındaki faaliyetleri nedeniyle bireyleri yasal tedbirlerle taciz etmeye ve cezai hükümleri kullanmaya devam etmiştir. Bununla birlikte bu iki yasa, kamu otoritelerinin bireyleri izleme çabalarını kolaylaştırmıştır. Zira bu yasa, başsavcıdan izin aldıktan sonra adli kolluk görevlilerine delillerin bu yasada öngörülen suçlardan herhangi birinin işlenmesinde kullanıldığını düşünülen herhangi bir yere girmelerine izin vermektedir. Ayrıca bu görevliler, söz konusu

[262] 2001 Tarihli (3) Sayılı Qanun Al'iijra'at Aljazayiya Alfilastini (TR: Filistin Ceza Muhakemeleri Usulü Yasası), erişim 16 Nisan, 2022, https://2u.pw/Wz3rZ.

suçlardan herhangi birini işlemek için kullanılan cihazları, araçları, gereçleri, programları, işletim sistemlerini ve internet ağının arama yetkisine sahiptir.

Filistin Siber Suçlar Yasası ise, kamu kurumlarına vatandaşların çevrimiçi faaliyetlerine ilişkin verileri izleme ve kolluk kuvvetlerinin talepleri doğrultusunda bilgilerini toplama, saklama ve aktarma konusunda geniş yetkiler vermiştir. Ayrıca bu yasa, hizmet sağlayıcıların kullanıcı verilerini ve özel bilgilerini en az üç yıl süreyle toplamasını ve güvenlik kurumlarıyla iş birliği içinde saklamasını zorunlu kılmaktadır.[263] Bu madde, iletişim gözetimiyle ilgili insan hakları standartlarının uygulanmasına ilişkin uluslararası ilkelere açıkça aykırıdır. Zira bu standartlar, girme, arama veya izleme emrinin sivil bir mahkeme hâkimi tarafından verilmesinin yanında hâkimin mümkün olduğu kadar eylemin zaman kapsamı ve ele geçirilecek verinin boyutu belirtmesini şart koşmuştur.[264]

[263] Mamoun, a.g.e., s.23.
[264] Al-Masry, a.g.e.

Sonuç

Dijital mahremiyet hakkı, Ürdün ve Filistin anayasalarında açıkça düzenlenmemiştir. Ancak bu hak, özel hayatın gizliliği ilkesi kapsamıyla kesiştiği için bu duruma ilişkin genel yasalar; kısmi olarak bazı dijital mahremiyet hakkının yönlerini içerecek şekilde genişletilmiştir. Bu durum, tezin konusu olan yeni bir anayasal hak türü doğurmuş ve bu çalışmadan aşağıdaki sonuç ve öneriler çıkarılmıştır:

Sonuçlar

1. Dünya ülkeleri, genel olarak mahremiyet hakkının ve özel olarak dijital mahremiyetin anayasal anlamda el alma biçimleri farklılık göstermektedir. Ayrıca mahremiyet konusu, yeni ve güncel bir konu olması nedeniyle dünyada anayasa ve mevzuat açısından bu konuda ciddi bir farklılık bulunmaktadır. Zira, her ülke dijital dünyada mahremiyet hakkı ile ilgili konularda kendine has bir deneyime sahiptir. Bu durumla birlikte ülkelerin, yasal çerçevelerinin dışında başka sorunlarla karşılaşması durumunda yasalarını değiştirmek için dayandığı farklı anayasa ve yasama felsefeleri benimsemektedir.
2. İnternetin hızlı yayılması, kullanıcıların verilerini koruyan yasal çerçeveler geliştirme hızını aşmış ve hatta bireylerin dijital haklarını ihlal eden politikaların üretilmesine yol açmıştır. Bu bağlamda Filistin ve Ürdün'deki yönetimler, siber suçları önlemek için bir yasa çıkartmakta acele ederken, Kişisel Verileri Koruma Yasası gibi dijital mahremiyet hakkıyla ilgili yasalar henüz Filistin'de çıkartmamış ve Ürdün'de onaylamamıştır.
3. Özel hayat kavramı, Filistin ve Ürdün'deki anayasal belgelerde geleneksel şekliyle ele alınmış ve dijital mahremiyet, Ürdün Anayasasında ve anayasa hükmünde olan Filistin Temel Yasası'nda hiçbir maddesinde dahil edilmeyip açıklığa kavuşturulmamıştır. Böylece geleneksel şekliyle özel hayatın gizliliğine ve mahremiyete her türlü saldırı, zarar görenlerin tazmin edilmesini gerektiren bir anayasal suç sayılmıştır. Dolayısıyla dijital mahremiyet kavramını geleneksel anayasal kavramın üzerine temellendirmek mümkündür.

4. Ürdün ve Filistin'deki özel hayatın gizliliği hakkı ile ilgili anayasal güvenceler, özellikle kişisel verilerin korunması bağlamında yasalar ve benzeri yasal mevzuata kapsamlı bir şekilde yansıtılmamıştır. Hukuk sistemi, Ceza Yasası, Siber Suçlar Yasası ve İletişim Yasası gibi çeşitli farklı yasalarda dağılmış yasal düzenlemelerle kişisel verilere yalnızca kısmi koruma sağlamıştır. Ancak bu yasal koruma, yetersiz ve belirli durumlar için geçerlidir. Aynı zamanda söz konusu yasal koruma, birçok durumda bilişim alanındaki büyük gelişmelere ve internette bulunan devasa veri miktarlarına ayak uyduramayan geleneksel yasal düzenlemelere dayanmaktadır.
5. Hem Ürdün hem de Filistin siber suç yasaları, ciddi yasal boşluklar içermekte ve bazı maddeleriyle anayasal ilkeleri ve uluslararası anlaşmaları ihlal etmektedir. Ayrıca bu iki yasa, dijital mahremiyet hakkının ihlalini açıkça suç sayan özel hükümler düzenlemekle eleştirilirken bazı maddelerinde, özel bir koruma sağlamadan mahremiyet hakkını ve verileri hedef alan eylemler dahil olmak üzere başka genel suçlara yer vererek genel anlamda bilgi sistemlerinin korunmasına ilişkin hükümler düzenlemiştir. Ayrıca bu yasalar, Kişisel verileri sahiplerinin rızası olmasam dijital ortamda işlenmesi, nominal verileri hukuka aykırı bir şekilde ifşa edilmesi, kişisel verilerin yasa dışı bir şekilde toplanıp başka kurumlara satılması ve dijital verileri toplama ve işleme amacından sapma gibi dijital mahremiyet hakkıyla ilgili siber suçları ele almamışlardır.

Öneriler

Ürdün Anayasası, Filistin Temel Yasası, Ürdün Siber Suçlar Yasası ve Filistin Siber Suçlar Yasası başta olmak üzere çalışmada karşılaştırılan söz konusu mevzuatın dijital mahremiyet hakkına ilişkin açık bir düzenleme içermediğinden dolay Ürdünlü ve Filistinli yasa koyucuları, aşağıdaki önerileri dikkate alarak dijital mahremiyeti anayasal ilkeler kapsamında düzenlemesi gerekmektedir:

1. Dijital mahremiyet yasaları ve özellikle dijital mahremiyete yönelik anayasa değişiklikleri, mahremiyet hakkını internet, sosyal medya ve benzeri dijital platformlar ile olan ilişkisi açısından ele almalıdır. Ayrıca yasalar, tutarlı bir şekilde

hem ulusal güvenlik endişelerini hem de bireyin mahremiyet hakkını değerlendirmeli ve özellikle İnternet ve sosyal medya tarafından oluşturulan dijital ortamı incelemeli. Bahsi geçen durumlar dolayısıyla kişisel mahremiyet kavramı, internet ve sosyal medya ile birlikte değişmiştir.

2. Ürdün ve Filistin'de dijital mahremiyet ve kişisel verileri koruma yasaları düzenlemekte ve yasalar onaylamaktadır. Bu konu hakkında ciddi adımlar atılmaktadır. 2015 yılından bu yana, Ürdün'de kamuoyunda tartışılmak üzere kişisel verileri koruma yasasının birkaç tasarısı yayınlanmıştır. Tasarı, yakın zamanda tartışılmak ve onaylanmak üzere Temsilciler Meclisi'ne gönderilmiştir. Ancak son yasa tasarısı bile hala anayasa ilkelerini Avrupa Birliği tarafından geliştirilen Genel Veri Koruma Tüzüğü'nü (GDPR) ihlal eden birkaç temel sorunu içermektedir. Filistin'de ise mahremiyetin ve verilerin korunmasına yönelik henüz bir yasa tasarısı sunulmamıştır
3. Ürdün ve Filistin'deki siber suç yasasılarında, dijital mahremiyet hakkına yönelik her türlü saldırıyı suç sayan açık hükümler içerecek değişiklikler yapılmalıdır. Dijital mahremiyet hakkının ifade özgürlüğü dahil olmak üzere çeşitli hak ve özgürlüklerle iç içe olduğunu bir kez daha belirtmek önemlidir. Böylece özgürlük endekslerin iki ülkede gerilmesi nedeniyle mahremiyet ihlalleri konusunda endişelerin artması mantıklıdır. Bu nedenle Ürdün Siber Suçlar Yasası'nın hakaret, iftira ve aşağılama suçlarına ilişkin 11. Maddesi, tüzel ile özel kişiler arasında ayrım yapılarak yeniden düzenlenmelidir.
4. Ürdün ve Filistin mevzuatı, anayasa hükümleriyle ve mahremiyet hakkının genel ilkeleriyle çelişen hükümler içermesi nedeniyle gözden geçirilmelidir. Örneğin; dijital iletişimle ilgili olarak güvenlik güçlerinin ve istihbarat teşkilatlarının yetkilerini sınırlandıran bir yasa düzenlenmeli ve yasayı izleme yetkileri, mahremiyet hakkına ilişkin uluslararası anlaşmalara uygun olarak yasayla açıkça kısıtlanmalıdır. Ayrıca Ürdün ve Filistin, mevzuatlarındaki cezai hükümleri, onayladıkları uluslararası sözleşmelerden almalıdır. Bununla birlikte bu iki ülke, yasaları hazırlama veya değiştirme sürecinde hakkın içeriğinden boşaltılmaması, özün korunması ve

anayasaya uygun olması açısından mahremiyet hakkının anayasal ilkelerini dikkate alınmalıdır.

5. Ürdün ve Filistin'de kamu ve özel sektörleri kapsayan bir yasal çerçeve geliştirilmeli ve ulusal yasaları, öncelikle anayasaya ve Ürdün ile Filistin tarafından onaylanan ve ifade özgürlüğü dahil olmak üzere farklı özgürlüklerin korunmasını içeren uluslararası kural ve standartlara uyumlu hale getirilmelidir. Ayrıca yapılmış olan ihlallerin hesabını soracak mekanizmaların geliştirilmesi kuvvetler ayrılığı ve bağımsızlığı ilkesinin güçlendirilmesi yoluyla mahremiyetin korunmasını güvence altına alan yasalar uygulanıp etkinleştirilmelidir.

Kaynakça

Kitaplar

- Al-bahji, Essam. *Himayat Alhaqi Fi Alhayaat Alkhasa Fi Daw' Huquq Al'iinsan Walmasyuwliat Almadania (TR: İnsan Hakları ve Medeni Sorumluluk Işığında Özel Hayat Hakkının Korunması)*, İskenderiye: Al-Jamia Al-Jadida Yayınları Yayınevi, 2005.
- Al-Mana'sah, Ahmed ve Al-Zoubi, Jalal Muhammad. *Crimes Relating To Information Electronic Systems And Technology*, Amman: Dar Al-Thaqafah For Publishing And Distribution, 2017.
- Alahwani, Hussam. *Alhaqu Fi İhtiram Alhayaa Alkhassa Walhaqi Fi Alsumea (TR: Mahremiyete Saygı ve İtibar Hakları)*, 3.b., Kahire: Dar Al-Nahda Al-Arabiya, 2021.
- Bahr, Mamdooh. *Himayat Alhaya Alkhasa Ela Alintirnti: Dirasa Muqarana (TR: İnternette Özel Hayatın Korunması: Karşılaştırmalı Bir Çalışma)*, 1.b., Kahire: Dar Al-Nahda Al-Arabiya, 2020.
- Fadl, Suleyman. *Almawajiha Altashrieia Wal'amniat Liljarayim Alnaashiat An İstikhdam Shabakat Almaelumat Alduwalia (TR: Uluslararası Bilgi Ağının Kullanımından Kaynaklanan Suçlarla Yasama Ve Güvenlik Alanında Mücadele Edilmesi)*, 1.b., Kahire: Dar Al-Nahda Al-Arabiya, 2013.
- Hassan, Nihad ve Hijazi, Rami. *Digital Privacy and Security Using Windows: A Practical Guide*, 1.b., New York: Apress, 2017.
- İbrahim, Mahmoud. *Alhimaya Aljinayiya Lilkhususia Waltijara Al'iiliktirunia (TR: Mahremiyetin ve E-Ticaret Alanlarında Cezai Koruma)*, 1.b., İskenderiye: Al-Wafa Hukuk Yayınevi, 2014.
- Lami, Bariq. *Jarimat İntihak Alkhususia Eabr Alwasayil Al'iilikturunia Fi Altashrie Al'urduniyi: Dirasa Muqarana (TR: Ürdün Mevzuatında Dijital Araçlar Yoluyla Mahremiyetin İhlali Suçu: Karşılaştırmalı Bir Çalışma)*, Yüksek Lisans Tezi, Orta Doğu Üniversitesi, 2017.
- Mamoun, Nader. *Dirasat Tahadiyat Alhuquq Alraqamia Fi Filastin (TR: Filistin'de Dijital Hakların Zorlukları Üzerine Bir Araştırma)*, 1.b., Ramallah: Filistin Kalkınma ve Medya Özgürlükleri Merkezi, 2019.
- Mansur, Ahmed. *Damanat Alhaqi Fi Hurmat Alhayaa Alkhasa Fi Almawathiq Alduwlia Lihuquq Al'iinsan Walqawanin Alwatania (TR: Uluslararası İnsan Hakları Sözleşmelerinde*

Ve Ulusal Yasalarda Özel Hayatın Gizliliği Hakkına Sağlanan Güvenceler), 3.b., Kahire: Arap İdari Gelişim Kurumu, 2019.

- Miller, Arthur. *The Assault On Privacy: Computers, Data Banks, And Dossiers*, 1.b., Ann Arbor: University Of Michigan Press, 1971.
- Mugabgib, Naim. *Makhatir Almaelumatia Walantarnit (TR: Bilişim ve Internet Tehlikeleri)*, 2.b., Beyrut: Al-Halabi Hukuk Yayınları, 2008.
- Muhammad, Nasir. *Haqa Al'iinsan Fi Himayat Hayaatih Alkhasat Fi Alqanun Alduwali Waltashrieat Aldaakhilia (TR: Uluslararası hukukta ve iç mevzuatta insanın özel hayatını koruma hakkı)*, 2.b., Riyad: Hukuk ve Ekonomi Yayınevi Yayım ve Dağıtım, 2013.
- Qayed, Usama. *Alhimaya Aljinayiya Lilhayaa Wabanuk Almaelumat (TR: Özel Hayat ve Bilgi Bankaları İçin Cezai Koruma)*, Kahire: Dar Al-Nahda Al-Arabiya, 2.b., 1994.
- Qoutal, Yasen. *Haqu Alkhususia Al'iilikturunia Bayn Altaqyid Wal'iitlaq (TR: Kısıtlama ile Özgürlük Arasında Dijital Mahremiyet Hakkı)*, 1.b., İskenderiye: Al-Wafa Hukuk Yayınevi, 2017.
- Rayyes, Thoraya. *Digital Privacy İn Jordan: Perceptions And Implications Among Human Rights Actors*, 1.b., Amman: Information and Research Center, 2015.
- Salem, Hadi. *Aliaetida' Ela Alhayat Alkhasa Ean Tariq Al'iintirnti: Dirasa Muqarana (TR: İnternet Üzerinden Özel Hayata Yönelik Saldırılar: Karşılaştırmalı Bir Çalışma)*, Kahire: Dar Al-Nahda Al-Arabiya, 2018.
- Samida, Ahmed. *Altanzim Alqanuniu Lilhaqi Fi Alkhususia: Almaskan - Alaitisalat Alkhasa - Albayanat Alshakhsia (TR Mahremiyet Hakkının Yasal Düzenlemesi: Konut - Özel Iletişim - Kişisel Veriler)*, 1.b., Kahire: Dar Al-Nahda Al-Arabiya, 2021.
- Shath, Abdullah. *Hurmat Alhayaat Alkhasa Fi 'Atar Alkhususia Walhimaya Walhaqi Fi Almuraqaba (TR: Mahremiyet, Koruma Ve Kontrol Hakkı Çerçevesinde Özel Hayatın Gizliliği)*, İskenderiye: Al-Wafa Hukuk Yayınevi, 2017.
- Stewart, Daxton. Social Media and the Law, 2.b., Londra: Routledge, 2017.
- Sweis, Rana ve Baslan, Dina. *Mapping Digital Media: Jordan*, 1.b., Amman: Open Society Foundations, 2013.
- Westin, Alan. *Privacy And Freedom*, New York: Atheneum, 1967.
- Zahroudi, Hazem. *Tarihul Kanunul Madani (TR: Medeni Kanun Tarihi)*, 2.b., Beyrut: Arap Araştırmaları ve Yayınları Merkezi, 2017.

- Zhuravlev, Malkova. *Philosophy Of Information Security*, 2.b., Tula: Proceedings Of The Tula State University, 2014.

Makaleler

- Abdin, Esam. "Alhuquq Alraqamia Fi Filastin Bayn Altawari Wajayihat Korona" (TR: Olağanüstü hâl ve Covid-19 Pandemisi Arasında Filistin'de Dijital Haklar). *Sosyal Medya Geliştirme Arap Merkezi*. 13/3 (2020): 1-14, https://2u.pw/Cnj5F (erişim 04.01.2022).
- Abdin, Esam. "Mulahazat Muasasat Alhaq Ealaa Mashru Alqarar Biqanun Almueadal Liqanun Mukafahat Alfasad" (TR: Al-Haq Kurumunun Yolsuzlukla Mücadele Yasasındaki Değişiklik Tasarısı Hakkındaki Yorumu). Al-Haq Kurumu. Erişim 17 Mayıs, 2022, https://2u.pw/929ew.
- Abushanab, Anan. "Israel's Control Of The Palestinian ICT Infrastructure And Its Impact On Digital Rights". *The Arab Center For Social Media Advancement.* (2018): 1-43, https://2u.pw/3W2ub (erişim 10.02.2022).
- Ahmed, Azam ve Perlroth, Nicole. "Using Texts As Lures, Government Spyware Targets Mexican Journalists And Their Families", New York Times. Erişim 21 Şubat, 2022, https://2u.pw/3ln4k.
- Al-Ajarma, Nofan. "Alhaqu Bihimayat Alkhususiat Fi Daw' Taedil Almada (23) Min Qanun Mukafahat Alfasad" (TR: Yolsuzlukla Mücadele Yasasının (23) Maddesinde Yapılan Değişiklik Işığında Mahremiyet Hakkının Korunması). Ammon Haber Ajansı, Erişim 02 Nisan, 2021, https://2u.pw/QPCUm.
- Al-Anaqrah, Mahmoud. "Mahatat Tarikhia: Aldustur Al'urduni" (TR: Tarihi İstasyonlar: Ürdün Anayasası), Al-Dustour Gazetesi. Erişim 20 Ağustos, 2021, https://2u.pw/c5ttr.
- Al-Kuda, Halid. "Eabir Lilhudud Bi'athar Rajei: Al'urduni Yadfae Biqanun Lihimayat Albayanat Alshakhsia" (TR: Sınırları Geçen ve Geriye Dönük Etkili Bir Yasa: Ürdün Kişisel Verileri Korumak İçin Bir Yasa Hazırlıyor). Al-Rai. Erişim 09 Mayıs, 2022, https://2u.pw/eQqUO.
- Al-Masry, Reem. "Qanun Aljarayim Al'iilikturunia: Alsaytart Ela 7 Milyun Mustakhdam Lilintirnit" (TR: Siber Suçlar Yasası: 7 Milyon İnternet Kullanıcısı Üzerinde Kontrol). Hiber Magazine. Erişim 06 Ağustos, 2021, https://2u.pw/5Ni8g.

- Al-Masry, Reem. “Tatbiq 'Aman Litatabue Almukhalitin: 'Asyilat Al'aman Walkhususia” (TR: Temaslı Kişileri Takip Etme Uygulaması “Aman”: Güvenlik Ve Gizlilik Soruları). Hiber Magazine. Erişim 19 Ocak 2022, https://2u.pw/Fs6iv.
- Al-Ustath, Suzan. “İntihak Hurmat Alhayat Alkhasa Eabr Al-İntarnit: Dirasa Muqarana” (TR: Özel Hayatın Gizliliği Hakkını Internet Üzerinden İhlali: Karşılaştırmalı Bir Çalışma). *Şam Üniversitesi İktisadi Ve Hukuki Bilimler Dergisi*. 29/03 (2013): 390-452.
- AlDahbi, Khadosh. “The Right to Privacy in The Face of Cyber Attack”. *The journal of Teacher Researcher of Legal and Political Studies*. 8/1 (2017): 140-157.
- Anton, Annie ve Mylopoulos, John. “Digital Privacy: Theory, Policies And Technologies”. *Requirements Engineering*. 16/1 (2011): 1-2.
- Ben Azza, Hamza. “Alnizam Alqanuniu Libayanat Aliatisal Bishabakat Alintirnit” (TR: İnternet Bağlantı Verilerinin Hukuk Sistemi). *Siyaset Bilimi Ve Hukuk Dergisi, Arap Demokratik Merkezi.* 4/23 (2020): 119-145.
- Ben-Hassine, Wafa. “Egyptian Parliament Approves Cybercrime Law Legalizing Blocking Of Websites And Full Surveillance Of Egyptians”, accessnow.org, Erişim 07 Şubat, 2022, https://2u.pw/I4SDM.
- Bettilyon, Tyler. “Why Good Digital Privacy Legislation Is So Hard to Get Right”, OneZero. Erişim 14 Şubat, 2022, https://2u.pw/z7orB.
- Bird Stephanie. “Security And Privacy: Why Privacy Matters”. *Science and Engineering Ethics*. 19/3 (2013): 669-671.
- Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği Yıllık Raporu: Alhaqu Fi Alkhususia Fi Aleasr Alraqamii (TR: Dijital Çağda Mahremiyet Hakkı). Birleşmiş Milletler Genel Kurulu- İnsan Hakları Konseyi, Oturum (27).
- Birleşmiş Milletler. “Information Received From The State Of Palestine On Follow-Up To The Concluding Observations On İts İnitial And Second Periodic Reports 2020”. Erişim 21 Ocak, 2022, https://2u.pw/LGjl6.
- Bojdin, Maria. “Min Alhaqi Fi Alhayaat Alkhasat 'İilaa Alhaqi Fi Alkhususiat Alraqamia” (TR: Özel Hayat Hakkından Dijital Mahremiyet Hakkına). *Anayasa Hukuku ve İdari Bilimler Dergisi: Berlin*. 2/3 (2019): 43-79.
- CNN. “Al'urdun: Taedilat Dusturia Jadida Tujib Salahiaa Lilmalik Minfirida” (TR: Ürdün: Krala Tek Taraflı Yetkiler Veren Yeni Anayasa Değişiklikleri”. erişim 28 Ağustos, 2021, https://2u.pw/ziexB

- Data Reportal. “Digital 2021: Jordan”. Erişim 13 Ocak, 2022, https://2u.pw/I2fwr.
- Data Reportal. “Digital 2021: Palestine”. Erişim 13 Ocak, 2022 https://2u.pw/4GBM3.
- Dijital Ekonomi ve Girişimcilik Bakanlığı. “Aliastiratijiat Al'urduniya Liltahawul Alraqmii 2020” (TR: Ürdün Dijital Dönüşüm Stratejisi 2020). Erişim 02 Haziran, 2021, https://2u.pw/VYLte.
- Dünya Bankası. “Tatwir Alkhadama Alraqamia Fi Aldifa Algharbia Waqitae Ghaza” (TR: Batı Şeria ve Gazze Şeridi’ndeki Dijital Hizmetleri Geliştirmek). Erişim 21 Ocak, 2022, https://2u.pw/j2cUu.
- El-Bishtawy, Saad. “Alhimaya Aldusturia Lilkhususia Almaelumatia” (TR: Dijital Mahremiyetin Anayasal Koruması). *Ürdün Kütüphaneler ve Bilgi Dergisi*. 52/2 (2017): 95-137.
- European Union. “Charter of Fundamental Rights of the European Union”. *Official Journal of the European Union.* 83/53 (2010).
- Fatafta, Marwa ve Samaro, Dima. “Exposed and Exploited: Data Protection In The Middle East and North Africa”. *Access now.org*. (2021): 3-45. https://2u.pw/gxmiq. (erişim 03.03.2022).
- Hamudi, Hamudi. “Almaswuwlia Altaqsiria Alnaajima Ean Antihak Alhaqi Fi Alkhususit Eabr Alintirnit” (TR: Dijital Mahremiyet Hakkının İhlalinden Kaynaklanan Haksız Fiil Sorumluluğu). *Hukuk ve Siyaset Bilimleri Dergisi*. 8/1 (2019): 306-335.
- Hartzog, Woodrow ve Richards, Neil. “Privacy's Constitutional Moment and the Limits of Data Protection”. *Boston College Law Review 1687*. 61/5 (2020): 1687-1761.
- Human Rights Watch. “A Threshold Crossed Israeli Authorities And The Crimes Of Apartheid And Persecution”. Erişim 25 Eylül, 2021, https://2u.pw/DqJ3T.
- Human Rights Watch. “Born Without Civil Rights Israel’s Use Of Draconian Military Orders To Repress Palestinians İn The West Bank”. Erişim 25 Ocak, 2022, https://2u.pw/1QBJo.
- Human Rights Watch. “Jordan ‘Fake News’ Amendments Need Revision”. Erişim 11 Ağustos, 2021, https://2u.pw/BsSY3.
- International Association of Privacy Professionals. “A brief history of the General Data Protection Regulation (1981-2016)”. Erişim 05 Ocak, 2022, https://2u.pw/yKtgn.
- Irtaimeh, Wejdan. “Criminal Protection Of Privacy In The Jordanian Cybercrime Law No.27 Of 2015”. *Asian Social Science*. 16/12 (2020): 64-79.

- Jordan Open Source Association. “Stakeholder Report Universal Periodic Review: The Right To Privacy İn Hashemite Kingdom Of Jordan”. Erişim 05 Nisan, 2021, https://2u.pw/Ab70I.
- Kaed, Aziz. “Qara'a Fi Mashrue Aldustur Alfilastinii Almuaqat” (TR: Geçici Filistin Anayasası Taslağı Üzerinde Bir İnceleme). *Filistin Bağımsız Vatandaş Hakları Komisyonu, Yasa Geliştirme Projesi Serisi.* 17/9 (2000): 53-81.
- Kapadia, Apu, Tristan Henderson, Jeffrey Fielding, David Kotz. “Virtual Walls: Protecting Digital Privacy In Pervasive Environments”. *Dartmouth Scholarship*. 5/3380 (2007): 146-169.
- Khalil, Asım. “Eamaliat Tahdir Aldustur Alfilastinii Watariqat Tabaniyh: Limadha Kayfi? Walimadha Alan?” (TR: Filistin anayasasını hazırlama ve kabul etme süreci: neden nasıl ve neden şimdi?). *Dirasat*. 36/2 (2009): 223-242.
- Khamis, Yasemin ve Khalil ,Asım. “Waqie Alnizam Aldusturii Watatawuruh: Murajaeat li'ahami Al'ahdath Walqararat Aldusturia Khilal Aleam 2018” (TR: Anayasal Sistemin Gerçekliği Ve Gelişimi: 2018 Yılındaki En Önemli Anayasal Olay Ve Kararların Gözden Geçirilmesi*). Birzeit Hukuk Çalışmaları Serisi*. 5/11 (2019): 1-16.
- Kokott, Juliane ve Sobotta, Christoph. “The Distinction Between Privacy And Data Protection In The Jurisprudence Of The CJEU And The Ecthr”. *International Data Privacy Law*. 3/4 (2013): s.222-228.
- Kramer, Irwin. “The Birth of Privacy Law: A Century Since Warren and Brandeis”. *Catholic University Law Review*. 93/3 (1990): 703-724.
- Kuznetsova, Olga ve Bondarenko, Natalia. “Private Life Safety Provision In Digital Age”. *The Journal Of Digital Forensics, Security And Law*. 12/3 (2017): 77-86.
- Mahmud, Abuallah. “Jarimat Aldukhul Ghayr Almashrue Wfqaan Lilqarar Biqanun Raqm (10) Lieam 2018 Bishan Aljarayim Al'iiliktrunia Alfilastinii” (TR: Siber Suçlara İlişkin 2018 Tarihli 10 Sayılı Filistin Yasası Uyarınca Yasadışı Erişim Suçu). *Al-Quds Açık Üniversitesi İnsan ve Sosyal Araştırmalar Dergisi*. 1/48 (2019): 4-31.
- Medanat, Nefis. Qimat Alhuquq Walhuriyaat Almuetaraf Biha Fi Aldustur Al'urduni (TR: Ürdün Anayasasında Tanınan Hak ve Özgürlüklerin Değeri). *Mu’tah Araştırma ve Çalışma Merkezi*. 11/1 (1996): 233-279.
- Mekovec, Renta. “Online Privacy: Overview and Preliminary Research”. *Journal Of Information And Organizational Sciences*. 34/2 (2010): 195-209.

- Mubarakiya, Moufida. “Alhimaya Alqanunia Lilhaqi Fi Alkhususia Alraqamia Fi Alqanun Aljazayirii” (TR: Cezayir Hukukunda Dijital Mahremiyet Hakkının Yasal Korunması), *Şeriat Ve Ekonomi Dergisi: Prens Abdul Qader İslami Bilimler Üniversitesi*. 7/13 (2018): 435-479.
- New York Times. “Edward Snowden, Whistle-Blower”. Erişim 13 Mayıs, 2022, https://2u.pw/R2dzx.
- Office of the United Nations High Commissioner for Human Rights. “Human Rights And Arrest, Pre-Trial Detentıon And Administrative Detention”. Erişim 13 Nisan, 2021, https://2u.pw/ttWBO.
- Salha, Nader. “Digital Rights Mapping In The MENA Region”. *The Arab Center For Social Media Advancement*. (2021):1-64. https://2u.pw/EcTlQ (erişim 17.09.2021).
- Salman, Oda. “Aljraym Almasa Bihimayat Alhya Alkhasa Alty Tqe Ebr Wasayl Tqnyt Almaelumat Alhdytha” (TR: Modern Bilgi Teknolojisi Vasıtasıyla İşlenen Özel Hayatın Korunmasına İlişkin Suçlar). *Al-Rafidain College*. 16/29 (2018): 79-102.
- Sharp, Tim. Right To Privacy: Constitutional Rights & Privacy Laws. Erişim 10 Ekim, 2021, https://2u.pw/37ndE.
- The Arab Center for Social Media Advancement. “Facebook And Palestinians: Biased Or Neutral Content Moderation Policies?”. Erişim 25 Eylül, 2021, https://2u.pw/gUNAP.
- Ürdün Açık Kaynak Derneği, Aljameia Al'urduniya Lilmasdar Almaftuh Turahib Biqarar Rayiys Alwuzara' Bi'iilgha' 'İilzamiat Tatbiq 'Aman” (TR: Josa Başbakanın Aman Uygulamasının (2021) Zorunluluğunu Kaldırma Kararını Memnuniyetle Karşılıyor). Erişim 17 Ağustos, 2021, https://2u.pw/xwEEm.
- Ürdün Açık Kaynak Derneği. “Taeliqat Wamulahazat Ela Aliastiratijiat Al'urduniya Liltahawul Alraqmii 2020” (TR: Ürdün Dijital Dönüşüm Stratejisi 2020 Üzerine Yorumlar Ve Notlar). Erişim 11 Haziran, 2021, https://2u.pw/CEzGo.
- Ürdün Stratejiler Forumu. “Alhukumat Al'iilikturuniat Fi Al'urdun: Nazrat Lisaniei Alsiyasat” (TR: Ürdün'de E-Devlet: Politika Yapıcılara Bir Bakış). Erişim 02 Haziran, 2021, https://2u.pw/deWax.
- Warren, Samuel ve Brandeis, Louis. “The Right To Privacy”. *Harvard Law Review*. 4/5 (1890):193-220.

İnternet Erişim Kaynakları

- Access Now (www.accessnow.org)
- European Commission (https://ec.europa.eu/)
- Filistin İnsan Hakları Merkezi (https://pchrgaza.org)
- Finlex Data Bank (https://finlex.fi/en/)
- Human Rights Library- University of Minnesota (http://hrlibrary.umn.edu/)
- Human Rights Watch (https://www.hrw.org/)
- International Association of Privacy Professionals (https://iapp.org/)
- Office of the United Nations High Commissioner for Human Rights (https://www.ohchr.org)
- Privacy International (http://privacyinternational.org/)
- Research Gate (https://www.researchgate.net/)
- Resmi Gazete (Filistin) (https://lab.pna.ps/ar)
- Resmi Gazete (Ürdün) (https://www.pm.gov.jo/ar/Pages/NewsPaper)
- The Arab Center For Social Media Advancement- 7amleh (https://7amleh.org)
- The Federal Register of Legislation (https://www.legislation.gov.au/)
- The Information and Research Center (https://irckhf.org/)
- The Internet Society (https://www.internetsociety.org/)
- The Jordan Open Source Association (https://jordanopensource.org/)
- United Nations (https://www.un.org/)