HAKEMLİ Denetişim
Ortak Aklın Harmanı

Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 16, Sayı: 32, 189-203, 2025

Araştırma Makalesi

UYAP'IN HOLİSTİK GÜVENLİK DENETİMİ
(HOLISTIC SECURITY AUDIT OF UYAP)

Hakan YILDIRIM[1]

ÖZ
UYAP (Ulusal Yargı Ağı Bilişim Sistemi), Türkiye'nin adalet sisteminin dijitalleşmesi amacıyla oluşturulmuş büyük ve çok taraflı bir bilişim sistemidir. Bu geniş kapsamlı sistem, yargı süreçlerini daha hızlı, verimli ve şeffaf hale getirmeyi amaçlamaktadır. Ancak, bu büyüklükteki ve bu kadar tarafı olan bir sistemin yönetim karmaşası yaşaması çok normaldir ve sistemin Holistik olarak güvenliğinin sağlandığını söylemek mümkün değildir. Holistik yaklaşım, sistemin tüm bileşenlerinin ve güvenlik unsurlarının bir bütün olarak değerlendirilmesi gerektiğini ifade eder. Bir bilişim sisteminin güvenliğinin fiziksel, sanal, politika, veri, bilgi, mahremiyet, kişisel ve ulusal gibi pek çok boyutunun birlikte alınmasına 'Holistik Güvenlik' denmektedir. UYAP'ın güvenlik politikalarının tüm paydaşlarca belirlenmesi ve denetlenmesi büyük önem taşımaktadır, ancak mevcut durumda UYAP'ın güvenliğiyle ilgili olarak kimin ne ölçüde yetki ve sorumluluğu olduğuna dair belirsizlikler bulunmaktadır. Bu durum, UYAP'ın denetiminin bağımsız ve UYAP'ı kullanan tarafların geniş tabanlı temsilinden oluşan bir kurul tarafından yapılması gerektiğini ortaya koymaktadır. Bu kurul hem güvenlik hem de denetim politika ve standartlarını belirlemelidir. Bu makale, UYAP'ın etkili yönetim ve denetimi için politika belirleyici olarak oluşturulması gerekli bir kurulda temsil edilmesi gereken tarafları ve kurulun yetkileri hakkında bir öneri sunmuştur.

Anahtar Kelimeler: UYAP, Holistik Güvenlik, Paydaş Katılımı, Politika Kurulu, Denetim.

***JEL Kodu: K10**- Kamu Hukuku (General), **K39**- Diğer Hukuki Konular (Diğer), **L86**- Bilişim Hizmetleri; İnternet Teknolojileri ve Yazılımlar.*

ABSTRACT
UYAP (National Judiciary Informatics System) is a large and multifaceted information system created to digitize Turkey's justice system. This comprehensive system aims to make judicial processes faster, more efficient, and transparent. However, it is quite normal for a system of this magnitude and with so many stakeholders to experience management complexity, and it is not possible to say that the system's security is ensured holistically. A holistic approach means that all components and security elements of the system need to be evaluated as a whole. The security of an information system is referred to as 'holistic security' when the physical, virtual, policy, data, information, privacy, personal, and national dimensions are considered together. It is of great importance that UYAP's security policies are determined and supervised by all stakeholders. However, there are uncertainties regarding who has what degree of authority and responsibility for UYAP's security in the current situation. This situation indicates that UYAP's oversight should be carried out by an independent board consisting of broad-based representation of the parties using UYAP. This board should determine both the security and audit policies and standards. This article has proposed which parties should be represented and the authorities of the board necessary for policy determination for effective management and oversight of UYAP.

***Keywords**: UYAP, Holistic Security, Stakeholder Participation, Policy Board, Audit.*

***JEL Classification: K10** - General Public Law, **K39** - Other Substantive Areas of Law, **L86** - Information and Internet Services; Computer Software.*

[1] Dr. Öğretim Üyesi, Ankara Bilim Üniversitesi, ORCID: 0000-0002-5959-269, hakan.yildirim@ankarabilim.edu.tr

1. GİRİŞ

Türkiye'de adalet sisteminin dijital dönüşümünde önemli bir mihenk taşı olan UYAP (Ulusal Yargı Ağı Bilişim Sistemi), yargı süreçlerinin hızlandırılması, daha verimli hale getirilmesi ve şeffaflık sağlanması amacıyla geliştirilmiştir. UYAP, yargı makamlarından avukatlara, vatandaşlardan devlet kurumlarına kadar geniş bir kullanıcı kitlesine hizmet eden çok Paydaşlı bir bilişim sistemi olarak öne çıkmaktadır. Ancak böyle büyük çaplı ve karmaşık sistemlerin güvenliği, yalnızca teknik tedbirlerle sağlanamayacak kadar geniş bir perspektifi zorunlu kılar.

Holistik güvenlik yaklaşımı, UYAP'ın güvenliğinin fiziksel, sanal, etik ve yasal tüm boyutlarıyla bir arada ele alınmasını gerektirir (Demir, 2021). Bu bağlamda; bilgi güvenliği, kişisel verilerin korunması, mahremiyet, bilişim güvenliği ve ulusal güvenlik unsurlarının bir bütün olarak değerlendirilmesi kritik bir önem taşır. Ancak mevcut durumda UYAP'ın güvenlik politikalarının oluşturulması ve uygulanması sürecinde, yetki ve sorumlulukların paydaşlar arasında net bir şekilde tanımlanmamış olması önemli bir belirsizlik oluşturmaktadır. Bu durum, sistem güvenliğinin sağlanması için bağımsız bir kurulun oluşturulmasını kaçınılmaz hale getirmektedir.

Bu çalışmanın temel amacı, UYAP (Ulusal Yargı Ağı Bilişim Sistemi) güvenliğinin yalnızca teknik ve prosedürel önlemlerle sınırlı kalmaması gerektiğini vurgulamak, sistemin etik, yasal, fiziksel ve ulusal güvenlik boyutlarını kapsayan bütüncül (Holistik) bir güvenlik yaklaşımı ile ele alınmasını sağlamaktır. Özellikle kişisel verilerin korunması, mahremiyetin sağlanması, bilişim güvenliği ve ulusal güvenlik unsurlarının birlikte değerlendirilmesinin önemine dikkat çekilmektedir.

Çalışmanın yöntemi, açık kaynaklardan erişilen verilerin analiz edilmesi ve dünyadaki benzer büyük ölçekli bilişim sistemlerinin karşılaştırmalı olarak incelenmesine dayanmaktadır. Özellikle; ABD'deki CM/ECF, Almanya'daki EGVP, Estonya'daki e-Adalet Sistemi gibi uluslararası örnekler ele alınmış ve bu sistemlerin güvenlik politikaları karşılaştırmalı olarak analiz edilmiştir. Bu yöntem, UYAP için uygulanabilir güvenlik ve denetim politikalarının geliştirilmesine temel oluşturmuştur.

Bunun yanında, çalışmada etik kurallara tam anlamıyla uyulmuş; verilerin kullanımı, analiz süreci ve önerilen politikaların oluşturulması aşamalarında tarafsızlık ve güvenilirlik esas alınmıştır.

Bu makale, UYAP'ın güvenliğinin sağlanabilmesi için gerekli olan bütüncül güvenlik yaklaşımını detaylı bir şekilde ele almakta ve özellikle bağımsız bir kurulun oluşturulmasına yönelik kapsamlı bir öneri sunmaktadır. Makale, sistemin güvenlik politikalarını oluşturacak kurulun yapısını, bu yapıda yer alması gereken tarafları, kurulun yetkilerini ve sorumluluklarını tanımlayarak, UYAP'ın güvenli ve sürdürülebilir bir sistem haline getirilmesine katkıda bulunmayı hedeflemektedir.

2. AÇIKLAMA, TARTIŞMA VE DEĞERLENDİRMELER

2.1. Mevcut Durum Analizi

UYAP (Ulusal Yargı Ağı Bilişim Sistemi), Türkiye'nin yargı süreçlerini hızlandırmak ve şeffaflığı sağlamak amacıyla geliştirilmiş çok taraflı bir bilişim sistemidir. Ancak bu büyüklükte bir sistemde güvenliğin sağlanması yalnızca teknik önlemlerle sınırlı değildir. Mevcut durumda:

- Yetki ve sorumlulukların paydaşlar arasında net olarak tanımlanmamış olması, güvenliğin yönetiminde belirsizliklere yol açmaktadır.
- Denetim mekanizmalarının bağımsız olmaması, sistemin şeffaflığına ve güvenliğine yönelik soru işaretleri doğurmaktadır.
- Güvenlik politikalarının tüm paydaşlar tarafından ortak bir katılım ile belirlenmemesi, kullanıcı güvenini azaltmakta ve riskleri artırmaktadır.

Bu eksiklikler, UYAP'ın güvenliğini Holistik (bütüncül) bir yaklaşımla ele almayı zorunlu kılmaktadır. Güvenliğin teknik, yasal, etik ve denetim boyutlarının birlikte değerlendirilmesi gerektiği açıktır.

2.2. Ulusal ve Uluslararası Uygulamalar ve Standartlar

Uluslararası Uygulamalar:

Dünyadaki büyük ölçekli e-adalet sistemleri, güvenlik ve denetim politikalarının oluşturulmasında önemli bir referans noktasıdır. (Şahin & Yıldırım, 2020) Örneğin:

- **ABD- CM/ECF (Case Management/Electronic Case Files)**

Federal mahkemelerde kullanılan bu sistem, elektronik dava dosyalarını güvenli bir şekilde saklamakta ve erişim yetkilerini net bir şekilde tanımlamaktadır.

Güçlü erişim kontrol mekanizmaları ve şifreleme teknolojileri kullanılarak güvenlik sağlanmaktadır.

- **Almanya- EGVP (Elektronik Mahkeme ve İdari Posta Sistemi)**

Yargı kurumları ve avukatlar arasında güvenli dijital iletişim sağlanmaktadır.

Dijital imzalar ve kriptografik iletişim yöntemleri kullanılmaktadır.

- **Estonya- e-Adalet Sistemi**

Estonya, blockchain teknolojisi ve çok faktörlü kimlik doğrulama yöntemleri ile sistem güvenliğini en üst düzeyde tutmaktadır.
Kullanıcıların mahkeme kayıtlarına güvenli erişimi sağlanmaktadır.

- **Ulusal Uygulamalar**

Türkiye'de UYAP ile birlikte çeşitli entegrasyonlar yapılmış ve büyük ölçüde dijitalleşme sağlanmıştır. Yetki karmaşası ve denetim eksikliği gibi sorunlar, sistemin güvenlik ve sürdürülebilirliğini riske atmaktadır. Kişisel verilerin korunması ve siber güvenlik önlemlerinin yetersizliği, uluslararası standartlara uyum konusunda eksiklikler yaratmaktadır.

- **Uluslararası Standartlar**
- ISO/IEC 27001- Bilgi Güvenliği Yönetim Sistemi:

Bilgi güvenliğinin yönetilmesinde uluslararası kabul görmüş bir standarttır.

- UYAP'ın güvenliği için bu standarda uyumlu denetim süreçleri oluşturulmalıdır.
- NIST Siber Güvenlik Çerçevesi (ABD):

Kritik altyapıların korunması için risk yönetimi temelli bir çerçeve sunmaktadır.

- GDPR (General Data Protection Regulation):

Kişisel verilerin korunmasına yönelik Avrupa Birliği düzenlemesidir. UYAP'ta kişisel veri mahremiyetinin sağlanması için bu düzenleme örnek alınmalıdır.

2.3. Mevcut Durumun Eksiklikleri ve Geliştirilmesi Gereken Yönler

- Mevcut durumda UYAP sisteminde tespit edilen başlıca eksiklikler şunlardır:
- Yetki Belirsizliği: Güvenlik ve denetim süreçlerinde kimin ne ölçüde yetkili olduğu net bir şekilde tanımlanmamıştır.
- Bağımsız Denetim Eksikliği: Sistemin güvenliği ve politikaları, bağımsız bir kurul tarafından denetlenmemektedir.
- Paydaşların Yetersiz Katılımı: Sistem güvenliği politikalarının oluşturulmasında kullanıcıların ve diğer paydaşların görüşleri yeterince temsil edilmemektedir.
- Kişisel Veri Güvenliği: Kişisel verilerin anonimleştirilmesi, şifrelenmesi ve sıkı erişim kontrolleri eksik kalmaktadır.

2.4. Taraflar

UYAP'ın taraflarını yeniden ele alırken, Cumhuriyet Savcılıkları, Adalet Bakanlığı'nın merkez ve taşra teşkilatları ve Adalet Komisyonları gibi önemli bileşenleri de dahil edelim. Aşağıda, bu yeni bileşenlerle birlikte UYAP tarafları daha geniş ve kapsamlı bir şekilde sunulmuştur:

Mahkemeler

Mahkemeler, UYAP (Ulusal Yargı Ağı Bilişim Sistemi) üzerinden birçok yargısal işlemi dijital ortamda gerçekleştiren en temel hizmet sunucularından biridir. Bu sistem, yargı süreçlerinin hızlanmasına, şeffaflık kazanmasına ve daha verimli bir şekilde yürütülmesine olanak tanır. Mahkemeler, dosya yönetimi, belge paylaşımı ve karar alma süreçlerinde UYAP'ı etkin bir şekilde kullanmaktadır.

Cumhuriyet Savcılıkları

Cumhuriyet Savcılıkları, ceza soruşturmalarını yürütmek ve kamu adına davalar açmakla sorumlu önemli bir yargı organıdır. UYAP üzerinden delil toplama, iddianame hazırlama ve dava dosyalarını yönetme gibi işlemleri dijital ortamda gerçekleştirirler.

Temel Özellikler

- Delil Toplama**:** Dijital ortamda delil toplama ve kaydetme.
- İddianame Hazırlama**:** UYAP üzerinden iddianame oluşturma ve ilgili mahkemeye gönderme.
- Dosya Yönetimi**:** Soruşturma dosyalarının elektronik olarak düzenlenmesi ve takip edilmesi.

Adalet Komisyonları

Adalet Komisyonları, yargı çalışanlarının atamaları, yer değiştirmeleri ve disiplin işlemlerini düzenleyen kurullardır. UYAP üzerinden personel işlemleri, performans değerlendirmeleri ve disiplin işlemlerini yönetirler.

Temel Özellikler

- Personel Yönetimi**:** Yargı personelinin atama ve yer değiştirme işlemlerinin elektronik olarak yapılması.
- Disiplin İşlemleri**:** Yargı çalışanlarının disiplin süreçlerinin dijital ortamda yürütülmesi.

- Performans Değerlendirme**:** Personelin performansının izlenmesi ve değerlendirilmesi.

Merkez ve Taşra Teşkilatları
Adalet Bakanlığı'nın merkez ve taşra teşkilatları, UYAP sisteminin yönetimi ve koordinasyonunda merkezi bir rol oynar. Merkez teşkilat, politika belirleme ve sistemin genel denetiminden sorumluyken, taşra teşkilatları yerel düzeyde sistemin işletilmesini ve bakımını sağlar.
Temel Özellikler
- Politika Belirleme**:** Merkez teşkilat, UYAP'ın işleyişi için gerekli politika ve prosedürleri belirler.
- Sistem Yönetimi**:** Taşra teşkilatları, UYAP'ın yerel düzeydeki işletim ve bakım faaliyetlerini yürütür.
- Denetim ve Raporlama**:** Sistem performansının ve güvenliğinin denetlenmesi, sonuçların raporlanması.

Avukatlar
Avukatlar, UYAP sayesinde dava açma, dilekçe verme, dosya inceleme ve duruşma takibi gibi işlemleri dijital ortamda gerçekleştirebilir. Bu, avukatların işlerini daha hızlı ve etkili bir şekilde yürütmelerine olanak tanır.
Temel Özellikler
- Dava Açma ve Takip**:** Avukatlar, dava dosyalarını UYAP üzerinden açabilir ve takip edebilir.
- Belge Yönetimi**:** Elektronik imza kullanarak belgeleri imzalama ve gönderme işlemlerini hızlandırır.
- Duruşma Takvimi**:** Duruşma tarihlerini ve saatlerini kolayca takip edebilirler.
- İnteraktif İşlemler**:** Avukatlar, mahkeme kararlarını ve dosya durumlarını anlık olarak öğrenebilir.

Vatandaşlar
Vatandaşlar, UYAP sayesinde birçok yargısal işlemi çevrimiçi olarak gerçekleştirebilirler. Dava sorgulama ve bilgi edinme işlemleri özellikle vatandaşlar için büyük kolaylık sağlar.
Temel Özellikler
- Dava Sorgulama**:** Kendi davalarını sorgulama ve dosya durumlarını öğrenme imkânı tanır.
- Belge ve Bilgi Erişimi**:** Mahkemeye sunulan belgeleri ve kararları UYAP üzerinden görüntüleyebilirler.
- E-Devlet Entegrasyonu**:** E-Devlet ile entegre olarak, vatandaşların tek bir platform üzerinden tüm adli işlemlerini yapmalarına olanak tanır.

Entegre Olan ve Bilgi Alışverişi Yapan Kurumlar
UYAP, sadece mahkemeler ve avukatlarla sınırlı kalmayıp, birçok kamu kurumu ve kuruluşu ile entegre bir şekilde çalışmaktadır. Bu entegrasyon, yargı süreçlerinin daha verimli ve etkili olmasını sağlar. Bunların başlıca olanları aşağıda sıralanmıştır.
Adalet Bakanlığı: Adalet Bakanlığı, UYAP sisteminin yönetimi ve denetimi konusunda merkezi bir role sahiptir. Bakanlık, sistemin sürekli olarak güncellenmesi ve güvenliğinin sağlanması için çalışır.
Emniyet Genel Müdürlüğü: UYAP, Emniyet Genel Müdürlüğü ile entegre çalışarak, adli vakaların hızlı bir şekilde değerlendirilmesini ve işlemlerin hızlandırılmasını sağlar.
Türkiye Barolar Birliği: Avukatların UYAP sistemine erişimini ve kullanımını kolaylaştırmak için Türkiye Barolar Birliği ile iş birliği yapılmaktadır.
Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü: Kimlik doğrulama ve vatandaşlık bilgileri konusunda UYAP ile entegre çalışan bu kurum, yargı süreçlerinin doğruluk ve güvenilirliğini artırır. (NVİ, 2024)
Maliye Bakanlığı: Vergi ve mali konularda, UYAP üzerinden bilgi alışverişi yapılmasını sağlayarak, mali işlemlerin hızlı ve güvenli bir şekilde yürütülmesine katkıda bulunur.
Ceza ve Tevkif evleri Genel Müdürlüğü: Mahkeme kararlarının hızlı bir şekilde uygulanması ve tutuklu/hükümlü bilgileri konusunda entegrasyon sağlanarak, ceza infaz süreçlerinin etkinliği artırılır.
Sosyal Güvenlik Kurumu (SGK): UYAP, SGK ile entegre çalışarak, sosyal güvenlik ile ilgili dava ve işlemlerin hızlı ve güvenilir bir şekilde gerçekleştirilmesini sağlar.
Ancak bunlarla sınırlı değildir. Adalet Bakanlığı tarafından hazırlanan kitapta 48 kurumdan 143 entegrasyon sıralanmaktadır. Bunlardan bir kısmının neden gerektiği anlaşılmaktadır. Ancak çoğu ise neden entegrasyon içinde sayılmış ve dahası bu veriler nasıl kullanılabilmekte bu durum anlaşılamamaktadır. Aşağıdaki tabloda Adalet Bakanlığının eğitim yayınlarından alınan verilere göre hazırlanmış ve UYAP'a entegre olan temel hizmetler ve işlevleri gösterilmiştir.

Tablo 1: UYAP'a Entegre Olan Kurumlar ve İşlevleri

Nr.	Entegrasyonun Adı	İşlevi
1	Adli Sicil Kaydı Sorgulama Entegrasyonu	Adli sicil kayıtlarının sorgulanması
2	Adli Sicil ve Arşiv Kaydı Sorgulama	Adli sicil ve arşiv kayıtlarının sorgulanması
3	MERNİS Sorgulama Entegrasyonu	MERNİS sistemi üzerinden kimlik bilgilerinin sorgulanması
4	SMS Geri Bildirim Entegrasyonu	Adli Sicil Genel Müdürlüğü'ne yapılan başvurularda başvuru sahibine SMS ile geri bildirim yapılması
5	Duruşma Bilgileri Sorgulama Entegrasyonu	Afyonkarahisar, Ankara ve Antalya barolarına anlık duruşma bilgileri ve haftalık duruşma listesinin verilmesi
6	Kadına Şiddet Tedbir Entegrasyonu	Aile Bakanlığı ile kadına şiddet tedbir kararlarının entegrasyonu
7	Çocuk Koruma Tedbir Kararları Entegrasyonu	Aile Bakanlığı ile çocuk koruma tedbir kararlarının entegrasyonu
8	Gazetede Yayınlanacak İlanların Verilmesi	Basın İlan Kurumuna gazetede yayınlanacak ilanların verilmesi
9	Gazete Künye Bilgilerinin Sorgulanması	Gazete künye bilgilerinin sorgulanması
10	TAKBİS Entegrasyonu	Tüzel ve gerçek kişilere ait mal varlığı sorgulaması
11	Tapu e-Haciz Entegrasyonu	Taşınmazlar üzerine ihtiyati haciz konulması işlemleri
12	Veraset İlamı ve Mirasçı Bilgileri Sorgulama	Tapu Kadastro Genel Müdürlüğünce veraset ilamı ve mirasçı bilgilerinin sorgulanması
13	Yurt Dışı İkamet Bilgileri Sorgulama	Dışişleri Bakanlığı ile yurtdışı ikamet bilgileri sorgulaması
14	e-Devlet Vasiyetname Sorgulama Entegrasyonu	Açılan vasiyetnameler ile iptal kararlarının sorgulanması
15	e-Devlet Veraset İlamı Sorgulama Entegrasyonu	Veraset ilamları ve veraset ilamı iptal kararlarının sorgulanması
16	4060 SMS Bilgi Sistemi Entegrasyonu	SMS bilgi sistemi başvuru, görüntüleme ve iptal işlemleri
17	Gümrük Bakanlığı Entegrasyonları	Kaçakçılık davalarına ilişkin bilgiler, iflas bilgileri, sicil sorgulama ve çek yasaklılık entegrasyonları
18	Emniyet Araç Entegrasyonu	Emniyet araçlarına ilişkin entegrasyon işlemleri
19	GöçNET Entegrasyonu	Göç İdaresi Genel Müdürlüğü ile yabancıların dava ve yakalama bilgilerinin verilmesi
20	İSKİ Adres Entegrasyonu	İstanbul Büyükşehir Belediyesi ile İSKİ abonelerine ait adres bilgilerine ulaşılması
21	Kamu Denetçiliği Dosya Sorgu Entegrasyonu	Kamu Denetçiliği Kurumu ile dosya kapak bilgileri ve belgelerin görüntülenmesi
22	TEHAKSİS Entegrasyonu	Kültür ve Turizm Bakanlığı ile telif hakları sorgulaması
23	Vakıfbank Banka Entegrasyonu	UYAP Vatandaş ve Avukat Portali üzerinden ödemelerin çevrimiçi olarak yapılması
24	Vakıfbank CTE Entegrasyonu	Hükümlülerin emanet para bakiyelerinin kart üzerinden kullanılması
25	Vakıfbank Hesap Hareketleri Entegrasyonu	Hesap hareketlerinin izlenmesi
26	Vakıfbank TÖS Entegrasyonu	Toplu ödeme sistemi üzerinden ödeme yapılması
27	Vakıfbank Vergi Entegrasyonu	Banka üzerinden vergi ödeme işlemleri
28	Yargıtay Dosya Sorgulama Entegrasyonu	e-Devlet üzerinden Yargıtay dosya kapak bilgilerinin ulaşılması
29	Yargıtay Mobil Entegrasyonu	Yargıtay çalışanlarına ilişkin bilgilerin verilmesi
30	Siyasi Partiler Entegrasyonu	Siyasi parti üye kayıtlarına ilişkin işlemler
31	YSK Entegrasyonu	Yüksek Seçim Kurulu entegrasyonları
32	Türkiye İş Kurumu Entegrasyonu	İşsizlik ödeneği alanların T.C. kimlik numarası ile ceza infaz kurumlarındaki durumunun sorgulanması
33	TNB Entegrasyonları	Türkiye Noterler Birliği ile noterlerin özlük işleri, vesayet ve velayet kararları, mühür talepleri
34	PTT Entegrasyonları	KEP e-Tebligat, KEP e-Yazışma, KEP hesap bilgileri, e-tebligat gönderim bilgileri
35	MASAK Entegrasyonu	Mali Suçları Araştırma Kurulu ile iflas erteleme ve derdest iflas erteleme kararlarının paylaşılması
36	Merkez Bankası Entegrasyonları	Veraset ilamı ve mirasçı bilgilerinin sorgulanması, faiz oran bilgilerine erişim
37	MKK Entegrasyonu	Merkezi Kayıt Kuruluşunda kayıtlı bulunan menkul kıymetlerin sorgulama işlemi
38	MSB Entegrasyonu	Milli Savunma Bakanlığı ile dosya kapak bilgilerinin (Silah Ruhsatı İçin) sorgulanması

39	ÖSYM Sorgu Entegrasyonu	Sınav sonuçlarının veri ve belge olarak alınması
40	TBB Entegrasyonu	Avukat Disiplin İşlemleri, Avukat Ruhsat İşlemleri, Baro kart Entegrasyonu
41	e-Devlet entegrasyonları	e-Devlet üzerinden vasiyetname, veraset ilamı sorgulama, 4060 SMS bilgi sistemi işlemleri, sınav başvuruları
42	Gümrük ve Ticaret Bakanlığı Entegrasyonları	Çek yasaklılık, kaçakçılık davaları, iflas bilgileri, sicil sorgulama
43	Adres ve Tanıma Tenfiz Entegrasyonları	Yurtdışı ikamet bilgileri sorgulama, dava ve karar bilgileri paylaşımı
44	BTK Entegrasyonları	İletişim tespiti talepleri, telefon açma-kapama ve IMEI bilgileri
45	Erişim Sağlayıcıları Birliği Entegrasyonu	Mahkeme kararlarına ilişkin erişimin engellenmesi
46	KAYSİS Entegrasyonu	Kurum ve kuruluşların resmi yazı ve iletişim bilgilerinin tutulduğu sistem
47	BAHUM Entegrasyonu	Kurum avukatlarının yetki belgesi ile tanımlanması ve evrak süreçlerinin işlenmesi
48	Sarı Basın Kartı Entegrasyonu	Sarı basın kartı sahiplerinin bilgileri
49	Tapu ve Kadastro Genel Müdürlüğü Parsel Sorgulama Entegrasyonu	Ada-parsel ve konum bilgisi alınması
50	Vergi Usul Kanunu Entegrasyonu	Vergi suçlarına ilişkin dosya kapak bilgilerinin elektronik ortamda görüntülenmesi

Kaynak: Adalet Bakanlığı, 2021

2.5. İşlem Hacmi

Bu tablo, Türkiye'deki adalet sistemi ile ilgili çeşitli istatistikleri sunmaktadır. Veriler, Ceza Mahkemeleri, Hukuk Mahkemeleri, İdari Yargı, Cumhuriyet Başsavcılığı ve İcra Daireleri'ndeki dosya sayıları ve süreçleri hakkında bilgi sağlamaktadır.

Ceza Mahkemeleri'nde günlük 10.927 dosya gelirken, günlük 5.363 karar alınmıştır. Yıl boyunca 2.567.345 dosya gelirken, 2.387.445 karar verilmiş ve 2.042.491 dosya derdest (karar bekleyen) durumdadır. Hukuk Mahkemeleri'nde ise günlük 10.150 dosya gelirken, 4.338 karar alınmıştır. Yıl boyunca 1.675.081 dosya gelirken, 1.738.516 karar verilmiş ve 2.531.592 dosya derdest durumdadır. İdari Yargı'da ise günlük 2.136 dosya gelirken, 830 karar alınmış; yıl boyunca 478.616 dosya gelirken, 448.042 karar verilmiş ve 376.270 dosya derdest durumdadır.

Cumhuriyet Başsavcılığı ise günlük gelen 1.272 ihbarın 651'i hakkında karar vermiştir. Yıl boyunca gelen 164.213 ihbardan 160.495'i karara bağlanmış, 43.944 ihbar ise hala işlem beklemektedir. Cumhuriyet Başsavcılığı soruşturma sayılarında ise günlük 21.059 soruşturma başlatılmış ve 16.158 soruşturma karara bağlanmıştır. Yıl boyunca gelen 3.297.407 soruşturmadan 3.182.405'i karara bağlanmış olup, 6.044.103 dosya hala derdest durumdadır.

Son olarak, İcra Daireleri'nde günlük gelen 49.036 dosyadan 40.557'si işlem görmüş, yıl boyunca gelen 5.673.083 dosyadan 4.434.866'sı sonuçlandırılmış olup, 22.546.095 dosya hala işlem beklemektedir. Denetimli serbestlik kapsamında ise günlük 2.165 kişi, yıllık toplamda 430.036 kişi ile ilgilenilmiş ve toplamda 227.567 kişi denetimli serbestlik sürecinde bulunmaktadır.

Bu istatistikler, adalet sisteminin yoğunluğunu ve çeşitli mahkemelerdeki iş yükünü gözler önüne sermektedir.

Tablo 2: UYAP'ın Resmi İstatistik Verilerine Göre Örnek Alınan Bir Günlük İşlem Özeti

Ceza, Hukuk Mahkemeleri ve İdari Yargı Dosya Sayıları					
	Günlük GELEN	Günlük KARAR	Seçili Yıl GELEN	Seçili Yıl KARAR	Seçili Gün DERDEST
Ceza Mahkemeleri	10.927	5.363	2.567.345	2.387.445	2.042.491
Hukuk Mahkemeleri	10.150	4.338	1.675.081	1.738.516	2.531.592
İdari Yargı	2.136	830	478.616	448.042	376.270
Cumhuriyet Başsavcılığı Soruşturma / İhbar Sayıları					
DEGER	Günlük GELEN	Günlük KARAR	Seçili Yıl GELEN	Seçili Yıl KARAR	Seçili Gün DERDEST
Cumhuriyet Başsavcılığı İhbar Sayıları	1.272	651	164.213	160.495	43.944
Cumhuriyet Başsavcılığı Soruşturma Sayıları	21.059	16.158	3.297.407	3.182.405	6.044.103
Cumhuriyet Başsavcılığı Toplam Sayıları	22.331	16.809	3.461.620	3.342.900	6.088.047
İcra Dairelerindeki İcra (Esas) ve İflas Dosya Sayıları					

	Günlük GELEN	Günlük ÇIKAN	Seçili Yıl GELEN	Seçili Yıl ÇIKAN	Seçili Gün DERDEST
İcra Dairelerindeki İcra (Esas) ve İflas Dosya Sayıları	49.036	40.557	5.673.083	4.434.866	22.546.095
Denetim Serbestlik Sayıları					
	Günlük SAYI	Yıllık SAYI	TOPLAM		
Denetim Serbestlik	2.165	430.036	227.567		

Kaynak: 07.08.24 tarihinde https://istatistikler.uyap.gov.tr/ web sitesinden alınmıştır.

2.6. Holistik Güvenlik

Holistik güvenlik, bir sistemin güvenliğini bütüncül bir perspektif ile ele alarak fiziksel, sanal, yasal, etik ve yönetsel boyutların bir arada değerlendirilmesini ifade eder. Bu yaklaşım, UYAP gibi büyük ve karmaşık sistemlerde güvenlik açıklarının her açıdan analiz edilmesini ve tüm paydaşların güvenliğe katılımını sağlamayı amaçlar. Bu bölümde, Holistik güvenliğin çeşitli bileşenleri detaylandırılarak mevcut durumdaki eksiklikler ve geliştirilebilir yönler ele alınacaktır.

2.6.1. Sanal Güvenlik

Holistik güvenlik, bir sistemin güvenliğinin bütüncül bir yaklaşımla, tüm boyutlarıyla ele alınması gerektiğini ifade eder. UYAP gibi büyük ve karmaşık bir bilişim sisteminin güvenliği, tek bir alanın güvenliğini sağlamaktan çok daha fazlasını gerektirir. Böylesine geniş çaplı ve çok taraflı bir sistemde güvenliğin sağlanması, sadece teknik önlemlerle sınırlı kalamaz; aynı zamanda stratejik, idari, fiziksel ve yasal boyutların da entegre bir şekilde ele alınmasını zorunlu kılar.

Bu bağlamda, sanal güvenlik bilgi güvenliği temeline dayanırken fiziksel güvenlik ise sistemin altyapısını oluşturan fiziksel varlıkların korunmasını kapsar. Sanal güvenlik bileşenleri olarak sanal erişim yöntemleri düşünülürken fiziksel güvenlik olarak fiziksel erişim yöntemlerini göz önünde tutmak ve önlemleri de bu çerçevede ele almak daha önemlidir. Fiziksel güvenlikte binaların ve donanımların güvenliğinden, yetkisiz erişimlerin önlenmesine kadar geniş bir yelpazede güvenlik tedbirlerini içerir. Ancak sanal ve fiziksel güvenlik birlikte ele alındığında anlamlı ve yeterli olacaktır. (Whitman & Mattord, 2018)

UYAP (Ulusal Yargı Ağı Bilişim Sistemi), Türkiye'nin adalet sisteminin dijitalleşmesi amacıyla geliştirilen ve çeşitli güvenlik mekanizmalarıyla desteklenen kapsamlı bir bilişim sistemidir. UYAP'ın mevcut durumu, güvenlik ve kullanıcı destek sistemleri bağlamında aşağıdaki gibi özetlenebilir:

Bilgi Güvenliği

- Merkezi Yapı: UYAP, merkezi bir bilgi güvenliği yapısına sahiptir. Bilgiler, merkezi bir sistem üzerinden yönetilmekte ve tüm veriler tek bir veri tabanında saklanmaktadır. Bu, bilgi tekrarlarının önlenmesini ve veri bütünlüğünün korunmasını sağlar.
- Fiziki Güvenlik**:** Sistem, sadece yazılımsal değil, fiziki güvenlikle de desteklenmektedir. Fiziksel güvenlik, sistemin altyapısını oluşturan binaların ve donanımların korunmasını kapsar.
- Yazılımsal Güvenlik**:** UYAP, yazılımsal güvenlik katmanları ile korunmakta ve sistemin güvenliğine yönelik çeşitli önlemler alınmaktadır. Bu önlemler arasında yetkisiz erişimlerin önlenmesi ve verilerin şifrelenmesi gibi tedbirler bulunmaktadır.
- N-Katmanlı Erişim**:** Kullanıcıların sisteme erişimi, N-katmanlı güvenlik yapılarıyla kontrol edilmekte ve her kullanıcının görev tanımına uygun erişim seviyeleri belirlenmektedir. (Stallings, 2017)

UYAP İç ve Dış Güvenlik Sistemleri

- İç Güvenlik Sistemi**:** İç güvenlik sistemi, UYAP'ın iç operasyonlarının güvenliğini sağlamak için geliştirilmiştir. Bu sistem, kullanıcıların erişim kontrolünü sağlamak ve iç tehditlere karşı koruma sağlamak amacıyla tasarlanmıştır.
- Dış Güvenlik Sistemi**:** Dış tehditlere karşı UYAP'ın güvenliğini sağlamak için çeşitli önlemler alınmıştır. Bu sistem, dışarıdan gelebilecek saldırılara karşı sistemin korunmasını sağlar.

Bilgi Güvenliği Yönetim Sistemi (BGYS)

- ISO/IEC 27001 Uyumlu**:** UYAP, ISO/IEC 27001 bilgi güvenliği yönetim sistemi standardına uygundur. Bu uluslararası standart, bilgi güvenliğinin en üst düzeyde sağlanmasını ve sürekli iyileştirilmesini hedefler.
- Faydaları**:** ISO/IEC 27001 standardı sayesinde UYAP, bilgi güvenliği risklerini sistematik bir şekilde yönetebilmekte, uyumluluğu artırabilmekte ve güvenlik açıklarını minimize edebilmektedir. (ISO/IEC, 2013)

Yardım Masası

- Görevleri**:** Yardım Masası, UYAP kullanıcılarına teknik destek sağlar. Kullanıcıların karşılaştığı sorunları çözmek, talepleri değerlendirmek ve hızlı bir şekilde geri dönüş sağlamak Yardım Masası'nın temel görevleri arasındadır.
- Hedefler**:** Yardım Masası, kullanıcıların sistemle ilgili yaşadıkları sorunları en kısa sürede çözerek sistemin etkin kullanımını artırmayı hedefler.

- Kullanımı**:** Yeni hata talebi veya destek talebi, kullanıcıların Yardım Masası'na başvurmasıyla işleme alınır. Operatörler bu talepleri değerlendirir ve gerekli durumlarda sorunu çözmek için müdahale eder. (Anadolu University, 2018).

Siber güvenlik, dijital varlıkların korunması açısından kritik öneme sahiptir. Bu, sistemin siber saldırılara, veri sızıntılarına ve diğer dijital tehditlere karşı korunmasını içerir. Siber güvenlik önlemleri, yalnızca dış saldırılara değil, aynı zamanda iç tehditlere karşı da etkili olmalıdır. Bilgi sistemleri üzerinde gerçekleştirilen düzenli güvenlik denetimleri ve saldırı tespit sistemlerinin sürekli izlenmesi, siber güvenliğin temel taşları arasında yer alır.

Kişisel verilerin mahremiyeti de Holistik güvenlik anlayışının önemli bir parçasıdır. Kişisel verilerin korunması, bireylerin özel bilgilerinin güvenli bir şekilde işlenmesini ve saklanmasını sağlar. Bu, yalnızca yasal zorunluluklar nedeniyle değil, aynı zamanda kullanıcıların güvenini sağlamak için de hayati bir unsurdur. Mahremiyetin sağlanması, veri anonimleştirme, şifreleme ve sıkı erişim kontrolleri gibi yöntemlerle desteklenmelidir. (Schneier, 2015)

Ulusal güvenlik boyutu, bu tür geniş çaplı bilişim sistemlerinde göz ardı edilemeyecek bir unsurdur. Ulusal güvenlik, devletin ve vatandaşların güvenliğini sağlamak amacıyla, sistemin kritik verilerinin korunmasını ve bu verilere erişimin sıkı denetim altında tutulmasını gerektirir. Bu bağlamda, ulusal güvenlik stratejileri, UYAP gibi sistemlerin bütünsel güvenlik politikalarının bir parçası olmalıdır.

2.6.2. Fiziksel Güvenlik

UYAP'ın güvenliği sadece dijital önlemlerle sağlanamaz; aynı zamanda sistemin fiziksel altyapısının korunması da büyük önem taşır. Fiziksel güvenlik, binaların, sunucuların, veri merkezlerinin ve diğer kritik altyapıların güvenliğini sağlamak için alınan önlemleri kapsar. Bu bağlamda, insan gücüne dayalı güvenlik önlemleri, fiziksel güvenliğin en kritik unsurlarından biridir.

Güvenlik Personelinin Rolü: Fiziksel güvenliğin sağlanmasında güvenlik personeli hayati bir rol oynar. Bu personel, veri merkezleri, sunucular ve diğer kritik alanların korunmasında doğrudan sorumludur. Güvenlik personeli, giriş-çıkış kontrollerini yönetir, şüpheli aktiviteleri izler ve acil durumlarda hızlı müdahalelerde bulunur. Etkili bir güvenlik politikası, bu personelin düzenli olarak eğitilmesini ve güncel güvenlik tehditlerine karşı hazırlıklı olmasını gerektirir. Örneğin, Amerika Birleşik Devletleri'nde yer alan Federal Veri Merkezleri, personel eğitimi ve acil durum yönetimi için katı standartlara sahiptir; bu da UYAP için bir model teşkil edebilir.

Erişim Kontrolleri: UYAP sisteminin fiziksel güvenliğinin sağlanmasında, yetkisiz kişilerin kritik alanlara erişimini engellemek için güvenlik personeli tarafından yönetilen erişim kontrol sistemleri kullanılır. Bu sistemler, biyometrik tarama, kimlik doğrulama kartları ve güvenlik kameraları gibi teknolojik araçlarla desteklenir. Güvenlik personeli, bu sistemlerin doğru bir şekilde çalışmasını sağlar ve herhangi bir ihlal durumunda gerekli önlemleri alır. Avrupa Birliği Veri Koruma Yönetmeliği (GDPR) kapsamında uygulanan veri merkezi erişim kontrol prosedürleri, UYAP için örnek teşkil edebilir. (European Union Agency for Cybersecurity [ENISA], 2017)

Acil Durum ve Müdahale Planları: Fiziksel güvenlik personeli, yangın, doğal afetler veya diğer acil durumlar için hazırlanmış müdahale planlarını uygulamakla yükümlüdür. Bu planlar, sistemin işleyişini kesintiye uğratabilecek durumlar için önceden belirlenmiş adımları içerir. Güvenlik personeli, bu planların uygulanmasında kritik bir rol oynar ve düzenli tatbikatlarla bu tür durumlara hazır hale getirilir. Japonya'daki veri merkezlerinde, deprem gibi doğal afetlere karşı özel hazırlıklar ve müdahale planları yapılmaktadır; bu da UYAP'ın acil durum planlarına entegre edilebilir. (ISO/IEC, 2019)

Gözetim ve İzleme: Fiziksel güvenlik kapsamında, güvenlik personeli, UYAP'a ait tesislerin 24/7 izlenmesini sağlar. Bu gözetim, olası güvenlik tehditlerinin erken tespiti ve önlenmesi için gereklidir. Güvenlik kameraları, alarm sistemleri ve diğer izleme araçları, güvenlik personeli tarafından sürekli olarak denetlenir ve yönetilir. Bu süreçler, Birleşik Krallıktaki hükümet binalarında uygulanan 24/7 izleme sistemlerine benzer şekilde, UYAP'ın güvenliğini sağlamak için kritik önem taşır. (Home Office, 2015; ICO, 2024)

İnsan Faktörünün Önemi: Fiziksel güvenlikte insan gücü, teknoloji ile desteklenen en önemli unsurdur. Güvenlik personelinin bilinçli, eğitimli ve dikkatli olması, fiziksel güvenlik politikalarının etkin bir şekilde uygulanmasını ve UYAP'ın fiziksel altyapısının korunmasını sağlar. Uluslararası Veri Koruma Otoriteleri, güvenlik personelinin eğitimi ve bilinçlendirilmesi konusunda sıkı standartlar uygulamaktadır; bu da UYAP için örnek teşkil edebilir. (European Union Agency for Cybersecurity [ENISA], 2019)

Bu unsurlar, UYAP'ın fiziksel güvenliğinin bütünsel bir güvenlik yaklaşımı içinde ele alınmasının önemini vurgular. Güvenlik personelinin rolü, yalnızca fiziksel tehditlere karşı değil, aynı zamanda sistemin genel güvenliğini artırmak için kritik öneme sahiptir. Bu nedenle, UYAP gibi büyük bir sistemde, fiziksel güvenlik politikalarının oluşturulmasında ve uygulanmasında insan gücü odaklı yaklaşımlar kaçınılmazdır.

Bu nedenle, UYAP'ın güvenliği, tüm bu unsurların bir arada ve uyum içinde ele alınmasını gerektiren karmaşık bir süreçtir. Her boyutun birbirini tamamladığı, çok katmanlı bir güvenlik yaklaşımı benimsenmeli ve bu yaklaşım, sürekli olarak gözden geçirilip güncellenmelidir. Bu tür bir yaklaşım, UYAP gibi büyük bir sistemin hem iç hem de dış tehditlere karşı etkin bir şekilde korunmasını sağlayacaktır.

Bu büyüklükte ve bu önemde bir bilgi sisteminin yönetimi, tüm paydaşların katıldığı bir kurul tarafından belirlenmelidir. Bu kurul, politika belirleyici bir kurul olup, güvenlik ve denetim politikalarını belirlemekle sorumludur. Ayrıca, bu politikaların işleyişi, sürekli olarak bu kurul tarafından kontrol edilmelidir.
Dünyada da benzer gereksinimlerle kurulmuş kurum ve kuruluşlar vardır. Bu kurumlar çalışmamıza ışık tutabilir. Bunlardan bazıları şöyledir:

2.7. Dünyadan Örnekler

Dünya genelinde büyük bilişim sistemlerinin yönetimi ve denetimi, birçok ulusal ve uluslararası kurum tarafından düzenlenmekte ve denetlenmektedir. Bu kurumlar, veri güvenliği, siber güvenlik ve kişisel verilerin korunması gibi kritik alanlarda standartlar belirlemekte ve bu standartların uygulanmasını sağlamaktadır. Aşağıda, UYAP gibi büyük bilişim sistemlerinin güvenlik ve denetim politikalarını oluştururken örnek alınabilecek bazı önemli uluslararası kuruluşlar ve düzenlemeler bulunmaktadır:
NIST (National Institute of Standards and Technology): ABD merkezli NIST, siber güvenlik ve veri gizliliği konusunda küresel ölçekte kabul gören standartları belirler. NIST'in geliştirdiği Siber Güvenlik Çerçevesi, uluslararası düzeyde benimsenmiş olup birçok ülke tarafından referans alınmaktadır. (National Institute of Standards and Technology [NIST], 2018)
ENISA (European Union Agency for Cybersecurity): ENISA, Avrupa Birliği'nin siber güvenlik ajansı olarak, AB genelinde siber güvenlik politikalarını koordine eder ve üye ülkeler arasında bilgi paylaşımını destekler. ENISA, Avrupa'da siber güvenlik stratejilerinin geliştirilmesi ve uygulanmasında kilit bir rol oynar. (European Union Agency for Cybersecurity [ENISA], 2020)
Budapeşte Sözleşmesi (Convention on Cybercrime): Avrupa Konseyi tarafından oluşturulan Budapeşte Sözleşmesi, siber suçlarla mücadelede uluslararası işbirliğini teşvik eden ilk uluslararası anlaşmadır. Bu sözleşme, siber suçlara karşı ülkeler arasında yasal düzenlemeler oluşturulmasını zorunlu kılar. (Council of Europe, 2001)
ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi: Bu uluslararası standart, bilgi güvenliği yönetim sistemleri için kabul görmüş bir çerçeve sunar. ISO/IEC 27001, kurumların bilgi güvenliği politikalarını tanımlamalarına ve uygulamalarına rehberlik eder. (ISO/IEC, 2013)
UNCTAD (United Nations Conference on Trade and Development): UNCTAD, dünya genelinde veri koruma ve gizliliği konusunda düzenlemeler yapan bir BM kuruluşudur. Özellikle gelişmekte olan ülkelerde veri güvenliği politikalarının geliştirilmesine yardımcı olur ve bu politikaların uluslararası standartlarla uyumlu hale getirilmesini sağlar. (United Nations Conference on Trade and Development [UNCTAD], 2016)
Bu kurullar ve standartlar, UYAP'ın güvenlik ve denetim politikalarını uluslararası normlarla uyumlu hale getirmek için kritik öneme sahiptir. UYAP'ın güvenliğinin sağlanmasında bu tür kurumların stratejilerinden ve uygulamalarından faydalanmak, sistemin uluslararası düzeyde kabul gören güvenlik standartlarına uygunluğunu artıracaktır.
Dünyadaki örnekler her ne kadar birbirinden oldukça farklı olsa bile bazı benzerlikler de mevcuttur. Aşağıda Tablo 3'de Türkiye, Amerika Birleşik Devletleri-ABD, Almanya ve Estonya'daki elektronik adalet uygulamalarının bir kıyaslaması gösterilmiştir.

Tablo 3: Türkiye, ABD, Almanya ve Estonya örneklerinin karşılaştırması

	Türkiye/UYAP	**ABD (CM/ECF)**	**Almanya (EGVP)**	**Estonya (e-Justice)**
Sistem Adı	**UYAP** (Ulusal Yargı Ağı Bilişim Sistemi)	Dava Yönetim/Elektronik Dava Dosyaları	Elektronik Mahkeme ve İdari Posta Sistemi	e-Adalet Sistemi
Ana İşlev	Yargı süreçlerinin dijitalleştirilmesi, güvenli belge yönetimi ve dava takibi	Federal mahkemeler için elektronik dava yönetimi ve dosya arşivleme	Mahkemeler, avukatlar ve otoriteler arasında güvenli dijital iletişim	Yargı süreçlerinin dijitalleştirilmesi, dava dosyalarına ve kayıtlara çevrimiçi erişim
Kullanılan Teknolojiler	Merkezi veri sistemi, e-İmza, Şifreleme, ISO/IEC 27001	Elektronik Dosyalama, e-İmza, Veri Yedekleme Sistemleri	Dijital Zaman Damgaları, Dijital İmzalar, Kriptografik İletişim	X-Road, Blockchain, Dijital İmza, e-Kimlik
Güvenlik Özellikleri	Çok katmanlı güvenlik, şifreleme, bağımsız denetim kurulu, GDPR uyumu	Çok katmanlı güvenlik, şifrelenmiş erişim, PACER entegrasyonu	Şifrelenmiş iletişim, e-İmzalar, GDPR uyumu	Blockchain ile sahtecilik önleme, çok faktörlü kimlik doğrulama, GDPR uyumu
Ulusal Sistemlerle Entegrasyon	Türk devlet kurumları ve hizmetleri ile entegrasyon (örneğin, emniyet, vergi dairesi)	PACER ile dava kayıtlarına kamusal erişim entegrasyonu	Belge transferi için çeşitli Alman federal sistemleriyle entegrasyon	Ulusal X-Road sistemi ile veri paylaşımı entegrasyonu

Kaynaklar: https://www.adalet.gov.tr, https://www.uscourts.gov/case-managementelectronic-case-files, https://www.egvp.de, https://www.just.ee/e-justice.

Bunların dışında da dünyada çeşitli örnekler mevcuttur. Dünyadaki diğer örneklere de kısaca değinmek gerekirse:

Birleşik Krallık
Sistem Adı: CE-File (Case Electronic File)
İşlev: İngiltere ve Galler'de kullanılan bu sistem, yüksek mahkemelerdeki dava işlemlerinin dijital olarak yönetilmesini sağlar. Avukatlar, davalarını elektronik olarak açabilir, dava belgelerine erişebilir ve yargı sürecini çevrimiçi takip edebilirler.
Kullanılan Teknolojiler: Elektronik Dosyalama, Dijital İmza, Erişim Denetimi.
Güvenlik: Sistem, güvenli erişim ve elektronik imza gibi güvenlik önlemleri ile korunur.
Ulusal Sistemlerle Entegrasyon: İngiltere'nin diğer devlet kurumları ile entegre olup, CE-File sistemi üzerinden bilgi alışverişi yapılabilir. (Gov.uk)

Hindistan
Sistem Adı: eCourts Projesi
İşlev: Hindistan'daki mahkemeleri dijitalleştirme girişimidir. Mahkeme işlemleri, dava takibi ve yargı belgeleri bu sistem aracılığıyla dijital olarak yönetilir. Vatandaşlar ve avukatlar davalarını çevrimiçi takip edebilir.
Kullanılan Teknolojiler: Elektronik Dosya Yönetimi, Mobil Uygulama Entegrasyonu, Elektronik Dava Takip Sistemi.
Güvenlik: Veri şifreleme, çok katmanlı güvenlik mimarisi ve erişim denetimleri kullanılır.
Ulusal Sistemlerle Entegrasyon: Hindistan genelindeki tüm yargı sistemlerini birbirine bağlayarak entegre bir yargı sistemi oluşturur. (Ecourts.gov.in)

Avustralya
Sistem Adı: Commonwealth Courts Portal
İşlev: Avustralya'da kullanılan bu portal, yüksek ve federal mahkemelerde dava açmak, dosya yönetmek ve mahkeme işlemlerini izlemek için kullanılır. Avukatlar ve taraflar, sistem üzerinden tüm dava işlemlerini yönetebilirler.
Kullanılan Teknolojiler: Elektronik Dosyalama, Dava Yönetimi, Çevrimiçi Takip.
Güvenlik: Kullanıcı kimlik doğrulama, şifreleme ve düzenli güvenlik denetimleriyle korunur.
Ulusal Sistemlerle Entegrasyon: Avustralya'nın diğer federal kurumlarıyla entegrasyon sağlar. (Fedcourt.gov.au)

Singapur
Sistem Adı: eLitigation
İşlev: Singapur'un yargı süreçlerini dijitalleştiren sistemdir. Davaların elektronik ortamda açılması, belgelerin dijital olarak sunulması ve takip edilmesi bu sistemle yapılır.
Kullanılan Teknolojiler: Elektronik Dosya Yönetimi, Dijital İmza, Zaman Damgalama.
Güvenlik: Kullanıcı doğrulama ve veri şifreleme.
Ulusal Sistemlerle Entegrasyon: Singapur'un çeşitli devlet kurumları ile veri paylaşımını mümkün kılan entegre bir platform. (Www.judiciary.gov.sg)

Brezilya
Sistem Adı: Processo Judicial Eletrônico-PJe (Elektronik Yargı Süreci)
İşlev: Brezilya'nın dijital adalet sistemidir. Mahkemelerdeki tüm işlemler dijital platformda yapılır. Dava açma, takip ve dosya yönetimi bu sistem üzerinden yürütülür.
Kullanılan Teknolojiler: Elektronik Dosyalama, Dijital İmza, Şifreleme.
Güvenlik: Erişim kontrolü, çok faktörlü kimlik doğrulama ve veri güvenliği önlemleri uygulanır.
Ulusal Sistemlerle Entegrasyon: Brezilya'nın adalet sistemine entegre olup, tüm mahkeme işlemleri dijital platformdan yönetilir. (Cnj.jus.br)

Kanada
Sistem Adı: Mahkeme Bilgi Sistemi (Court Information System -CIS)
İşlev: Kanada'daki mahkemelerin dijital olarak yönetilmesini sağlar. Avukatlar ve taraflar, dava dosyalarına çevrimiçi erişebilir ve işlemleri dijital olarak gerçekleştirebilirler.
Kullanılan Teknolojiler: Elektronik Dava Dosyası, Dijital İmza, Çevrimiçi Dava Yönetimi.
Güvenlik: Gelişmiş veri şifreleme ve güvenlik önlemleri mevcuttur.
Ulusal Sistemlerle Entegrasyon: Kanada'daki diğer adli sistemlerle entegre bir yapı sunar. (Justice.gc.ca)

2.8. Denetimler
Denetimler, güvenlik politikalarının uygulanıp uygulanmadığını kontrol etmek için düzenli olarak yapılmalıdır. Denetim Kurulu, bağımsız bir yapıdan oluşmalı ve şu şekilde organize edilmelidir:

- Denetim Standartları: ISO 27001 gibi uluslararası standartlara uygunluk sağlanmalıdır.
- Denetim Prosedürleri: Denetim süreçlerinin nasıl yürütüleceği ve hangi yöntemlerin kullanılacağı belirlenmelidir.
- Raporlama ve İzleme: Denetim sonuçlarının düzenli olarak raporlanması sağlanmalıdır.
- İhlal Yönetimi: Güvenlik ihlalleri durumunda alınacak önlemler belirlenmelidir.

Güvenlik politikaları, bir kurumun bilgi varlıklarını ve operasyonlarını çeşitli tehditlerden korumak amacıyla belirlediği kurallar, prosedürler ve uygulamaların toplamıdır. Bu politikalar, kurumun güvenlik hedeflerini, stratejilerini ve sorumluluklarını tanımlar. Güvenlik politikalarının önemi, kurumun güvenlik yönetimini düzenli ve etkili bir şekilde yürütmesini sağlamaktan kaynaklanır. (Whitman & Mattord, 2018)

Büyük Bilişim Sistemlerinde Denetimin Önemi: Büyük bilişim sistemleri, karmaşık yapıları ve çok sayıda paydaşı nedeniyle sürekli olarak denetim altında tutulması gereken yapılardır. Bu tür sistemlerde güvenlik, sadece teknolojik önlemlerle sağlanamaz; sistemin bütünsel olarak denetlenmesi, güvenlik politikalarının etkinliğini artırmak için hayati bir rol oynar. Denetim, sistemin belirlenen güvenlik standartlarına uygun çalışıp çalışmadığını kontrol etmek, olası zafiyetleri tespit etmek ve gerekli iyileştirmeleri yapmak amacıyla gerçekleştirilir. (Institute of Internal Auditors [IIA], 2012)

Denetim süreçlerinin bir diğer kritik işlevi, hesap verebilirliği artırmaktır. Büyük bilişim sistemleri, genellikle birçok farklı kurum ve kullanıcının etkileşimde bulunduğu ortamlardır. Bu nedenle, sistemin nasıl kullanıldığı, hangi verilerin kimler tarafından erişildiği ve bu süreçlerin ne kadar güvenli olduğu sürekli olarak izlenmelidir. Denetimler, sistemin şeffaf bir şekilde işletilmesini sağlar ve olası ihlallerin erken aşamada tespit edilmesine olanak tanır. Böylece, kullanıcıların ve paydaşların sisteme olan güveni artar ve sistemin genel verimliliği yükselir.

Ayrıca, denetimler, uyum süreçlerinin etkin bir şekilde yürütülmesi için de gereklidir. Büyük bilişim sistemleri, genellikle çeşitli yasal düzenlemeler ve uluslararası standartlar çerçevesinde faaliyet gösterir. Denetim, bu düzenlemelere uyumun sağlandığını ve sürdürüldüğünü teyit eder. Uyum denetimleri hem yasal riskleri minimize eder hem de sistemin operasyonel risklerini yönetilebilir seviyede tutar. Bu nedenle, düzenli denetimlerin yapılması, bilişim sistemlerinin uzun vadede sürdürülebilir ve güvenilir olmasını sağlar.

Denetim mekanizmaları, bir kurumun veya sistemin güvenliğini sağlamak ve sürekliliğini garantilemek için gerekli kontrollerin ve denetimlerin yapılmasını sağlayan süreçlerdir. Etkili bir denetim mekanizması, güvenlik politikalarının uygulanmasını izler, riskleri değerlendirir ve güvenlik açıklarını tespit ederek gerekli önlemlerin alınmasını sağlar. Bu kapsamda, Adalet Bakanlığı, Kişisel Verileri Koruma Kurumu (KVKK), adli merciler ve diğer paydaşların iş birliği içinde olması gerekmektedir. Kurulun geniş tabanlı temsilcilerden oluşan bağımsız bir denetim organı olarak faaliyet göstermesi, UYAP'ın güvenliğinin sağlanmasında kritik bir rol oynar. Bu sayede, kurumlar güvenli ve sürdürülebilir bir şekilde faaliyet gösterebilir.

2.9. Kurul Önerisi

UYAP (Ulusal Yargı Ağı Bilişim Sistemi), Türkiye'nin adalet sisteminin dijitalleşmesi ve etkinleştirilmesi amacıyla geliştirilmiş kapsamlı bir bilgi işlem sistemidir. Bu sistemin güvenli ve verimli bir şekilde işletilebilmesi için, tüm bileşenlerini kapsayan güvenlik ve denetim politikalarının titizlikle oluşturulması gerekmektedir. Bu politikaların belirlenmesi, uygulanması ve denetlenmesi sürecinde çok Paydaşlı bir kurulun rolü hayati önem taşır. Bu kurul, yalnızca politika belirlemekle kalmayıp, aynı zamanda bu politikaların etkin bir şekilde yürütülmesi ve sürekli izlenmesi için gerekli denetim mekanizmalarını da oluşturmalıdır.

UYAP'ın güvenlik ve denetim politikalarının oluşturulması, sistemin güvenli ve verimli bir şekilde işletilebilmesi için hayati önem taşır. Bu süreç, çok Paydaşlı bir Politika Belirleyici Kurul tarafından yürütülmelidir. Kurul, sistemin güvenliği için gerekli politikaların belirlenmesi ve uygulanmasının yanı sıra, bu politikaların sürekli olarak izlenmesini ve güncellenmesini de sağlamakla yükümlüdür. Kurulun yapısı, hizmet sunucular, hizmet alıcılar ve güvenlik uzmanları dahil olmak üzere, çeşitli tarafların temsil edilmesini gerektirir. Bu bağlamda, kurulun aşağıdaki profillerden gelen üyelerden oluşması önerilmektedir:

- Hizmet Sunucular: Yüksek yargı temsilcileri, Adalet Komisyonu temsilcileri ve Bakanlık temsilcileri.
- Hizmet Alıcılar: Vatandaş temsilcileri ve baro temsilcileri.
- Güvenlik Uzmanları: Fiziksel güvenlik, ulusal güvenlik ve bilgi güvenliği profesyonelleri ile ulusal güvenlik uzmanları.
- Kişisel Veri Koruma Kurumu (KVKK) Temsilcileri
- Vatandaş Temsilcileri
- Bilgi Güvenliği Uzmanları
- Mahremiyet Uzmanları
- Avukatlar
- Ulusal Güvenlik Uzmanları

- Siber Güvenlik Uzmanları
- Hâkim ve Savcılar
- Üst Yargı Organları Temsilcileri

Bu kurulun oluşturulması, UYAP'ın güvenlik ve denetim süreçlerinin etkin bir şekilde yürütülmesini sağlamak için kritik öneme sahiptir. Sistematik bir yönetim ve denetim yapısı, UYAP'ın uzun vadeli başarısını güvence altına alacak ve Türkiye'nin dijital adalet sistemi üzerindeki güveni artıracaktır.

2.10. Güvenlik Politikaları

Erişim Kontrol Politikaları: Erişim kontrol politikaları, UYAP sistemine erişimin nasıl sağlanacağını ve yetkisiz erişimlerin nasıl önleneceğini belirleyen stratejik önlemler bütünüdür. Bu politikalar, kullanıcıların kimlik doğrulama süreçlerinden yetki seviyelerine kadar geniş bir yelpazede güvenlik tedbirlerini içerir. Bu bağlamda:

- Kimlik Doğrulama: Kullanıcıların UYAP'a giriş yaparken, iki faktörlü kimlik doğrulama gibi güçlü kimlik doğrulama yöntemleri kullanması zorunlu kılınmalıdır.
- Yetki Seviyeleri: Kullanıcılar, görev tanımları ve sorumlulukları doğrultusunda uygun yetki seviyeleriyle sınırlandırılmalıdır.
- Erişim Logları: UYAP'a yapılan tüm erişimler ayrıntılı olarak kaydedilmeli ve bu kayıtlar düzenli olarak denetlenmelidir.

Veri Güvenliği Politikaları: Veri güvenliği politikaları, UYAP sisteminde işlenen tüm verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini koruma amacı taşır. Bu politikalar, verilerin depolanması ve taşınması esnasında şifreleme, veri yedekleme ve veri erişim denetimleri gibi önlemleri kapsar:

- Şifreleme: Verilerin hem depolama süreçlerinde hem de aktarım sırasında güçlü şifreleme yöntemleriyle korunması sağlanmalıdır.
- Veri Yedekleme: Düzenli aralıklarla veri yedeklemeleri yapılmalı ve bu yedeklerin güvenli bir ortamda saklanması sağlanmalıdır.
- Veri Erişim Denetimleri: Verilere erişim yetkisi bulunan kullanıcıların denetimleri sıkı bir şekilde gerçekleştirilmelidir.

Siber Güvenlik Politikaları: Siber güvenlik politikaları, UYAP sisteminin siber saldırılara karşı korunmasını sağlar. Bu bağlamda, sistemlerin güvenlik duvarları ve güncel Anti Virüs Yazılımları ile korunması, siber saldırıların erken tespiti ve önlenmesi için gerekli sistemlerin kurulması büyük önem arz etmektedir:

- Güvenlik Duvarları ve Anti Virüs Yazılımları: Sistemler, güvenlik duvarları ve sürekli güncellenen anti virüs yazılımlarıyla korunmalıdır.
- Saldırı Tespit ve Önleme Sistemleri: Olası siber saldırıların erken tespiti ve önlenmesi amacıyla etkili tespit ve önleme sistemleri kurulmalıdır.
- Acil Durum Planları: Siber saldırı durumunda devreye girecek acil durum planları oluşturulmalı ve bu planlar düzenli olarak test edilmelidir.

Kişisel Veri ve Mahremiyet Politikaları: Kişisel veri ve mahremiyet politikaları, UYAP'ta işlenen kişisel verilerin korunmasını ve kullanıcı mahremiyetinin sağlanmasını hedefler (BfDI, 2024) Bu politikalar, verilerin yalnızca gerekli durumlarda ve yasal çerçevede toplanmasını, işlenmesini ve saklanmasını öngörür:

- Veri Toplama ve İşleme: Kişisel verilerin yalnızca zorunlu durumlarda ve yasal mevzuata uygun bir şekilde toplanması ve işlenmesi sağlanmalıdır.
- Anonimleştirme: Kişisel verilerin anonim hale getirilmesi ve yetkisiz erişimlere karşı korunması sağlanmalıdır.
- Kullanıcı Bilgilendirme: Kullanıcılar, verilerinin nasıl toplandığı, işlendiği ve korunduğu konusunda şeffaf bir şekilde bilgilendirilmelidir.

2.11. Denetim Politikaları

Denetim Standartları: Denetim standartları, UYAP'ın güvenlik politikalarının etkin bir şekilde uygulanıp uygulanmadığını değerlendirmek için oluşturulan kriter ve yöntemlerdir. Denetimlerin uluslararası kabul görmüş güvenlik standartlarına uygun olarak yapılması sağlanmalıdır:

- Uluslararası Standartlara Uyum: Denetimlerin ISO 27001 gibi uluslararası standartlara uygun olarak gerçekleştirilmesi sağlanmalıdır.
- Denetim Prosedürleri: Denetim süreçlerinin nasıl yürütüleceğini belirleyen prosedürler oluşturulmalıdır.
- Denetim Frekansı: Denetimlerin hangi sıklıkla yapılacağı ve bu denetimlerin kimler tarafından gerçekleştirileceği net bir şekilde belirlenmelidir.

Raporlama ve İzleme: Denetim süreçlerinin sonuçlarının düzenli olarak raporlanması ve izlenmesi gereklidir. Bu süreçlerin şeffaf ve hesap verebilir bir şekilde yürütülmesi, UYAP'ın güvenlik politikalarının etkinliğini artıracaktır:

- Denetim Raporları: Denetim sonuçları detaylı raporlar halinde hazırlanmalı ve ilgili paydaşlarla paylaşılmalıdır.

- Geri Bildirim Mekanizmaları: Denetim sonuçlarına yönelik geri bildirimler alınmalı ve bu geri bildirimler, politika geliştirme sürecine entegre edilmelidir.
- Sürekli İzleme: Güvenlik politikalarının ve denetim süreçlerinin sürekli olarak izlenmesi ve gerektiğinde güncellenmesi sağlanmalıdır.

İhlal Yönetimi: Güvenlik ihlalleri durumunda izlenecek adımlar ve alınacak önlemler, önceden belirlenmiş prosedürler çerçevesinde gerçekleştirilmeli; ihlal sonrası iyileştirme çalışmaları, sistemin gelecekteki güvenliğini temin etmelidir:

- İhlal Bildirim Prosedürleri: Güvenlik ihlalleri tespit edildiğinde izlenecek bildirim prosedürleri oluşturulmalı ve bu prosedürler tüm paydaşlar tarafından bilinmelidir.
- İhlal Müdahale Ekipleri: Güvenlik ihlallerine hızlı ve etkili bir şekilde müdahale edebilecek uzman ekiplerin oluşturulması sağlanmalıdır.
- İhlal Sonrası İyileştirme: Güvenlik ihlalleri sonrası yapılacak iyileştirme çalışmaları ve alınacak önlemler net bir şekilde belirlenmeli ve uygulanmalıdır.

2.12. İşleyiş

UYAP (Ulusal Yargı Ağı Bilişim Sistemi) için önerilen Politika Belirleyici Kurul, sistemin güvenlik ve denetim politikalarının etkin bir şekilde uygulanmasını sağlamak amacıyla oluşturulmuştur. Kurulun işleyişi, aşağıdaki adımları içerir:

Toplantı Frekansı ve Yönetimi:

Kurul, düzenli aralıklarla (örneğin, üç ayda bir) toplanır. Ayrıca, acil durumlar veya önemli güvenlik tehditleri durumunda olağanüstü toplantılar da yapılabilir. Toplantılara, tüm kurul üyelerinin katılımı zorunludur ve toplantılar, önceden belirlenmiş bir gündem çerçevesinde yürütülür. Toplantıların yönetimi, kurul başkanı tarafından koordine edilir ve alınan kararlar toplantı tutanaklarında kayıt altına alınır.

Karar Alma Süreci:

Kurul, UYAP'ın güvenlik ve denetim politikaları ile ilgili kararlarını çoğunluk oyu ile alır. Her üye, ilgili konular üzerinde görüş bildirme ve öneri sunma hakkına sahiptir. Karar alma sürecinde, uluslararası güvenlik standartları ve en iyi uygulamalar dikkate alınır. Ayrıca, kurulun her toplantısında, daha önce alınmış kararların uygulanma durumu gözden geçirilir ve gerekli görüldüğünde bu kararlar güncellenir.

Politika Geliştirme ve Onaylama:

Kurul, UYAP için gerekli güvenlik ve denetim politikalarını geliştirir. Bu politikalar, özellikle erişim kontrolü, veri güvenliği, siber güvenlik ve kişisel verilerin korunması gibi kritik alanları kapsar. Her yeni politika taslağı, kurul üyeleri tarafından incelenir ve onaylanır. Onaylanan politikalar, ilgili tüm taraflara duyurulur ve UYAP sistemine entegre edilir.

Denetim ve İzleme:

Kurul, UYAP'ın güvenlik politikalarının ve denetim süreçlerinin etkinliğini izlemek için düzenli olarak denetim raporları hazırlar. Denetim süreçleri, ISO 27001 gibi uluslararası standartlara uygun olarak gerçekleştirilir. Bu denetimler, sistemdeki olası güvenlik açıklarını tespit etmek ve bu açıkları gidermek için gerekli önlemleri almak amacıyla yapılır. Denetim sonuçları, kurulun bir sonraki toplantısında detaylı olarak değerlendirilir.

İhlal Yönetimi ve Müdahale:

UYAP sisteminde tespit edilen güvenlik ihlalleri, kurul tarafından belirlenmiş prosedürler doğrultusunda ele alınır. Herhangi bir ihlal durumunda, ilgili müdahale ekipleri hızlıca harekete geçer ve gerekli iyileştirme çalışmaları yapılır. Kurul, bu süreçlerin etkinliğini sürekli olarak izler ve gerektiğinde müdahale prosedürlerini günceller.

İletişim ve Koordinasyon:

Kurul, Adalet Bakanlığı, Kişisel Verileri Koruma Kurumu (KVKK), Emniyet Genel Müdürlüğü ve diğer ilgili paydaşlarla sürekli iletişim halinde olur. Bu iletişim, hem karar alma süreçlerinin şeffaflığını artırır hem de kurulun aldığı kararların etkili bir şekilde uygulanmasını sağlar. Ayrıca, kurul, ulusal ve uluslararası güvenlik otoriteleri ile de koordinasyon halinde çalışarak UYAP'ın güvenliğini en üst düzeyde tutmayı hedefler.

Sürekli Eğitim ve Bilgilendirme:

Kurul, UYAP'ın güvenlik ve denetim politikalarının etkinliğini artırmak amacıyla, güvenlik personeli ve sistem kullanıcıları için düzenli eğitim programları hazırlar. Bu eğitimler, yeni güvenlik tehditleri ve teknolojik gelişmeler hakkında bilgi vermek ve personelin güncel kalmasını sağlamak için tasarlanmıştır. Ayrıca, kullanıcıların güvenlik politikaları hakkında bilinçlendirilmesi için düzenli bilgilendirme çalışmaları yapılır.

3. SONUÇ

UYAP (Ulusal Yargı Ağı Bilişim Sistemi), Türkiye'nin adalet sisteminin dijital dönüşümünü sağlamak amacıyla oluşturulmuş, geniş kapsamlı ve çok taraflı bir bilişim sistemidir. Bu sistem, yargı süreçlerini hızlandırarak daha verimli ve şeffaf hale getirmektedir. Ancak UYAP'ın büyüklüğü ve karmaşıklığı, güvenlik yönetimi açısından çok boyutlu zorluklar doğurmaktadır. Bu zorlukların aşılabilmesi için Holistik Güvenlik Yaklaşımı'nın benimsenmesi kaçınılmazdır.

Holistik güvenlik, bir bilişim sisteminin tüm bileşenlerinin ve güvenlik unsurlarının bir bütün olarak ele alınmasını ifade eder. UYAP gibi büyük ölçekli ve karmaşık bir sistemde, güvenliğin sadece teknik önlemlerle sağlanması yetersiz kalacaktır. Sistemin fiziksel güvenlik, siber güvenlik, kişisel veri koruması, mahremiyet ve ulusal güvenlik gibi tüm boyutları entegre bir şekilde ele alınmalıdır. Bu bütünsel yaklaşım, sistemin güvenliğini sağlarken kullanıcıların ve paydaşların güvenini de artıracaktır (CISA, 2024)

Mevcut Durum ve İhtiyaç

Mevcut durumda UYAP'ın güvenliğiyle ilgili olarak kimin ne ölçüde yetki ve sorumluluğa sahip olduğu konusunda belirsizlikler bulunmaktadır. Bu durum, sistemin etkin yönetilmesini zorlaştırmakta ve güvenlik politikalarının oluşturulmasını aksatmaktadır. Bu belirsizliğin giderilmesi için;

Bağımsız Denetim ve Politika Kurulu oluşturulmalıdır: Kurulda Adalet Bakanlığı, avukatlar, hâkimler, Kişisel Verileri Koruma Kurumu (KVKK), bilgi güvenliği uzmanları ve vatandaş temsilcileri yer almalıdır.

Kurulun görevi; güvenlik ve denetim politikalarını oluşturmak, uygulamak ve uluslararası standartlara uygun olarak denetlemek olmalıdır.

Yetki ve Sorumlulukların Netleştirilmesi sağlanmalıdır: Tüm paydaşların görevleri ve sorumlulukları açık bir şekilde tanımlanmalıdır.

Kişisel Veri ve Mahremiyetin Korunması için, verilerin anonimleştirilmesi ve şifrelenmesi gibi güçlü koruma yöntemleri hayata geçirilmelidir.

Kullanıcılar, verilerinin nasıl toplandığı ve işlendiği hakkında şeffaf bir şekilde bilgilendirilmelidir.

Uluslararası Standartlara Uyum sağlanmalıdır; özellikle ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardına uygun güvenlik politikaları uygulanmalıdır.

Bu öneriler doğrultusunda oluşturulacak bağımsız ve geniş tabanlı bir kurul, UYAP'ın güvenlik yönetiminde şeffaflık, etkinlik ve hesap verebilirlik sağlayacaktır.

UYAP'ın güvenliği, yalnızca teknik ve prosedürel tedbirlerle değil, aynı zamanda etik, yasal, fiziksel ve siber güvenlik unsurlarının bütünsel bir şekilde değerlendirilmesiyle sağlanabilir. Bu makalede önerilen denetim kurulunun oluşturulması, sistem güvenliğini etkin bir şekilde sağlayacak ve Türkiye'nin dijital adalet sistemini daha güvenli, verimli ve şeffaf hale getirecektir. Adalet Bakanlığı başta olmak üzere ilgili kurumların iş birliği içinde çalışarak kapsamlı ve sürdürülebilir güvenlik politikalarını hayata geçirmesi hayati önem taşımaktadır.

Kaynakça

Adalet Bakanlığı Bilgi İşlem Genel Müdürlüğü. (2021). *UYAP Bilişim Sistemi*. Adalet Bakanlığı.

Anadolu University. (2018). *Ulusal Yargı Ağı Projesi-I*. Anadolu University.

Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. Council of Europe.

Demir, G. (2021). Ulusal Yargı Ağı Bilişim Sistemi'nin (UYAP) Güvenlik Politikaları. *Bilgi Güvenliği Dergisi, 15*(2), 45-61.

European Union Agency for Cybersecurity (ENISA). (2019). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. ENISA.

European Union Agency for Cybersecurity (ENISA). (2020). *ENISA Threat Landscape 2020: Cybersecurity Challenges for the EU*. ENISA.

European Union Agency for Cybersecurity (ENISA). (2017). *Guidelines on Data Protection Impact Assessment (DPIA) under Regulation (EU) 2016/679*. ENISA.

General Data Protection Regulation (GDPR). (2016). *Regulation (EU) 2016/679*.

Home Office, UK Government. (2015). *Security Guidance for Government Buildings*. Home Office.

Institute of Internal Auditors (IIA). (2012). *Global Technology Audit Guide (GTAG): Information Technology Controls*. IIA.

ISO/IEC. (2019). *ISO/IEC 22301: Business Continuity Management Systems – Requirements*. ISO.

ISO/IEC. (2013). *ISO/IEC 27001: Information Security Management Systems – Requirements*.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. NIST.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company.

Stallings, W. (2017). *Network Security Essentials: Applications and Standards*. Pearson.

Şahin, E., & Yıldırım, E. (2020). Türkiye'de Siber Güvenlik Politikaları: UYAP Örneği. *Güvenlik Stratejileri Dergisi, 16*(32), 79-102.

United Nations Conference on Trade and Development (UNCTAD). (2016). *Data Protection and Privacy Legislation Worldwide*. UNCTAD.

Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security*. Cengage Learning.

İnternet Kaynakları

Adalet Bakanlığı. (nd). UYAP İstatistikleri. Erişim tarihi: 01.05.2024. Erişim adresi: https://istatistikler.uyap.gov.tr/

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI). (nd). Erişim tarihi: 05.05.2024. Erişim adresi: https://www.bfdi.bund.de

Cybersecurity and Infrastructure Security Agency (CISA). (nd). Erişim tarihi: 10.05.2024. Erişim adresi: https://www.cisa.gov/

Information Commissioner's Office (ICO). (nd). Erişim tarihi: 12.05.2024. Erişim adresi: https://ico.org.uk/

Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü (NVİ). (nd). Erişim tarihi: 15.05.2024. Erişim adresi: https://www.nvi.gov.tr/

Sosyal Güvenlik Kurumu (SGK). (nd). Erişim tarihi: 20.05.2024. Erişim adresi: https://www.sgk.gov.tr/

Türkiye Barolar Birliği. (nd). Erişim tarihi: 25.05.2024. Erişim adresi: https://www.barobirlik.org.tr/