# Evrensel Parlamento’25

## Teknoloji Meclisi

### Çalışma Rehberi

**Akademik Ekip Üyesi:** Efe Pamir Çakır
**Meclis Başkanı:**Elif Rana İşbilir
**Meclis Başkan Yardımcısı:**Şevval Özgü Tan

**Kapsam:** Teknolojinin insanlığın kötülüğüne kullanılmasına engel olmak.

**Geçmiş:** Nükleer silah teknolojilerinin gelişimi ile İkinci Dünya Savaşında Japonya'ya karşı yapılan nükleer saldırı.

**Günümüz:** İnternet üzerinden yapılan veri hırsızlığına karşı alınabilecek önlemler.

**Gelecek:** 2085 yılında yapay zekanın gelişimi ile robotların günlük hayatta insanların yerine geçmesinin yaratabileceği sorunlar.

# İçerik tablosu

# A.Meclisin Kapsamının açıklanması

Teknoloji, insanlık tarihinin en önemli ve en hızlı gelişen alanlarından biridir. Temel olarak, teknoloji, insanın doğa ile olan ilişkisini geliştirmek, sorunları çözmek ve yaşam kalitesini artırmak amacıyla bilimsel bilgi ve becerilerin sistemli bir şekilde uygulanmasıdır. Teknoloji, sağlık, eğitim, iletişim, ulaşım gibi birçok alanda devrim yaratmış ve hayatı kolaylaştırmıştır. Bilgisayarlar, yapay zeka, robotlar ve genetik mühendislik gibi alanlarda kaydedilen ilerlemeler, insanlığın potansiyelini artırmış ve insan yaşamını daha verimli hale getirmiştir. Ancak, teknolojinin gelişimi sadece olumlu sonuçlar doğurmakla kalmamış, aynı zamanda insanlığın kötüye kullanabileceği bir güce de dönüşmüştür. Teknolojinin insanlığın kötülüğüne kullanılmasının sakıncaları, çoğu zaman doğrudan ve dolaylı etkilerle kendini gösterir. Teknolojinin yanlış ellerde veya kötü amaçlarla kullanılması, toplumsal yapıları sarsabilir, bireylerin haklarını ihlal edebilir ve çevresel felaketlere yol açabilir. Peki bunun gibi durumlar teknolojinin gelişimi kısıtlanmadan nasıl engellenebilir? Teknoloji meclisi, bu sorunları çözmek adına geçmiş, günümüz ve gelecek perspektiflerinden birer protokol yazacaktır.

# B. Kapsamla ilgili Genel Terimler

**Manhattan Projesi:** Manhattan Projesi, İkinci Dünya Savaşı sırasında ilk nükleer silahların üretimini gerçekleştirmek için yürütülmüş bir araştırma ve geliştirme projesidir.

**Cambridge Analytica:**Cambridge Analytica, siyasi kampanyalar için kişisel verileri analiz ederek hedeflenmiş reklamlar ve stratejiler geliştiren, 2018 yılında Facebook veri skandalıyla büyük tartışmalar yaratan bir İngiliz danışmanlık firmasıdır

**Büyük Veri:** Büyük veri, geleneksel veri işleme araçlarıyla işlenemeyecek kadar büyük, karmaşık ve hızlı büyüyen veri setlerini ifade eder. Bu veriler, analiz edilerek önemli içgörüler elde edilmesini ve kararlar alınmasını sağlar, genellikle iş dünyası, sağlık, finans ve teknoloji gibi alanlarda kullanılır.

**Veri İhlali:** Veri ihlalleri, bireylerin ya da kuruluşların gizli ya da hassas verilerine yetkisiz erişim sağlanması, bu verilerin çalınması ya da ifşa edilmesi durumudur.

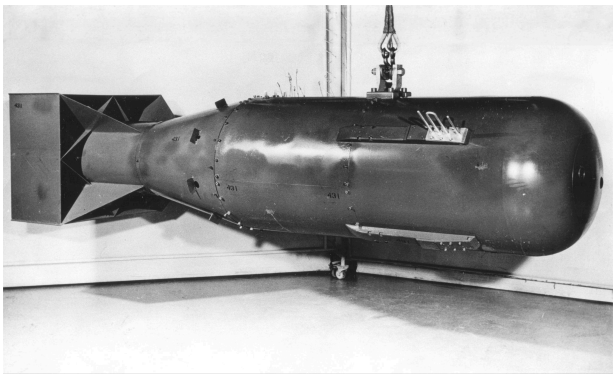
**Bilgisayar Korsanı:** Bilgisayar korsanı, bilgisayar sistemlerine veya ağlarına izinsiz erişim sağlayarak güvenlik açıklarından yararlanıp veri çalma, zarar verme ya da kötüye kullanma amacı güden kişidir. Bu tür kişiler genellikle yasa dışı faaliyetlerde bulunurlar ve bilgisayar güvenliği konusunda ciddi tehditler oluştururlar.

**Nükleer Silahların Yayılmasının Önlenmesi Antlaşması (NPT):** Nükleer Silahların Yayılmasının Önlenmesi Antlaşması, 1970'te yürürlüğe giren nükleer enerjinin barışçıl kullanımını amaçlayan antlaşmadır.

**Gelir uçurumu:** Gelir uçurumu, toplumdaki zengin ve yoksul kesimler arasındaki gelir farkının giderek daha belirgin hale gelmesidir. Bu durum, ekonomik kaynakların adaletsiz dağılımı nedeniyle sosyal sınıflar arasındaki uçurumu genişletir. Gelir uçurumu, genellikle eğitim, sağlık ve yaşam kalitesi gibi alanlarda eşitsizliklere yol açarak toplumsal sorunları derinleştirebilir. Uzun vadede, bu eşitsizlikler toplumsal huzursuzluklara ve ekonomik istikrarsızlıklara neden olabilir.

# C. Geçmiş konusu ve açıklaması:

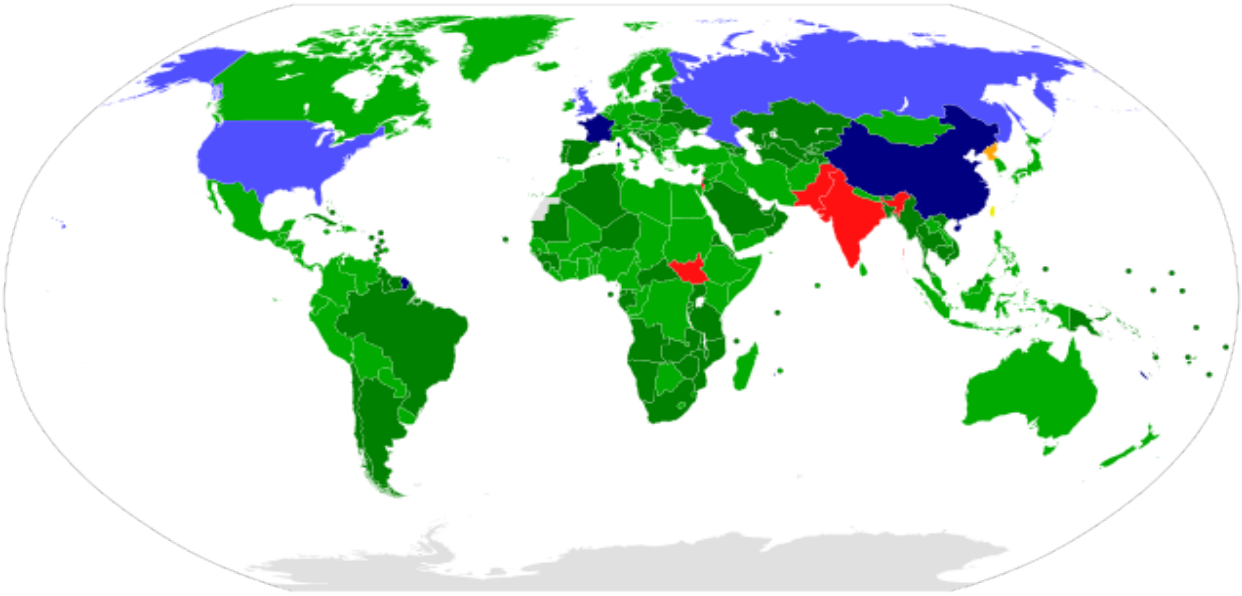
Teknoloji, insanlık tarihinin her döneminde hayatı geliştiren ve kolaylaştıran önemli bir olgu olmuştur. Ancak bu gelişmelerin bilinçsiz ve kötü amaçlarla kullanılmasının toplumu derinden etkilediği zamanlar da olmuştur. Teknolojinin olumsuz etkilerinden bahsedildiğinde, 1945 yılı 6 ve 9 Ağustos tarihlerinde Amerika Birleşik Devletleri tarafından Japonya'ya karşı gerçekleştirilen nükleer saldırılar akla gelir. Bu olay, teknolojinin kötü amaçla kullanımının trajik bir örneği olarak tarihe geçmiştir. Manhattan Projesi, II. Dünya Savaşı sırasında Amerika Birleşik Devletleri tarafından gerçekleştirilen gizli bir araştırma ve geliştirme programıdır. Proje, nükleer silahların geliştirilmesi amacıyla 1942 yılında başlamış ve dünyanın ilk atom bombasının üretimi için büyük bir çaba sarf edilmiştir. Projede Albert Einstein, J. Robert Oppenheimer ve Enrico Fermi gibi dönemin en ünlü bilim insanları görev almıştır. Proje kapsamında geliştirilen atom bombaları, savaşın seyrini değiştirecek kadar güçlü olmuştur.



Amerikalı bilim insanları, nükleer patlamaların potansiyelini fark ettikten sonra Japonya'ya karşı kullanılmak üzere bir strateji oluşturmuşlardır. Araştırmalar sonucunda, Japon halkının en çok dışarıda bulunduğu saatlerin sabah 08.15 ve 10.58 olduğu belirlenmiştir. Bu bilgilere dayanarak, Hiroşima'ya sabah 08.15'te "Little Boy" (Küçük Oğlan) bombası, Nagasaki'ye ise 10.58'de "Fat Man" (Şişman Adam) bombası atılmıştır. Sonuç olarak, bu saldırılarda yaklaşık 220.000 insan hayatını kaybetmiş, çok sayıda kişi ise patlama sonrası oluşan radyasyon nedeniyle ciddi sağlık sorunları yaşamıştır. Evsiz kalanların sayısı ise bir hayli fazla olmuştur (yaklaşık 500.000 kişi). Bu korkunç olayın ardından, 1970 yılında nükleer silahsızlanmayı amaçlayan Nükleer Silahların Yayılmasının Önlenmesi Antlaşması (NPT) çeşitli ülkelerde yürürlüğe girmiştir. Bu antlaşma, yanlızca beş ülkenin nükleer silah bulundurma hakkında sahip olması gerektiğini savunmuştur (ABD, Rusya, Çin, Birleşik Krallık ve Fransa). Hindistan, Pakistan, İsrail ve Kuzey Kore gibi bazı devletler bu antlaşmayı imzalamamıştır. Bu antlaşma, nükleer silahların yayılmasının engellenmesi ve barışçıl amaçlarla kullanılmasının sağlanması amacıyla uluslararası bir çerçeve oluşturmuştur. Bugün bile, nükleer silahların gücü ve potansiyeli, insanlık için ciddi bir tehdit

oluşturmayı sürdürmektedir. Geçmiş meclisi, bu dönemin koşullarını göz önünde bulundurarak bir protokol yazacaktır.

## Nükleer Silahların Yayılmasının Önlenmesi Antlaşması



Tanınmış nükleer silah sahibi devletler (onaylayanlar)
Tanınmış nükleer silah sahibi devletler (katılanlar)
Diğer onaylayanlar
Diğer katılanlar veya yerine geçenler
Çekildiğini açıklayan katılımcı (Kuzey Kore)
Taraf olmayanlar (Hindistan, İsrail, Pakistan, Güney Sudan)
Kısmen tanınan devlet (onaylayan) (Tayvan)

## D. Geçmiş alt başlıkları

**1. Patlama sonucu oluşan radyasyondan ve diğer etkenlerden dolayı sağlık sorunları çeken insanlara nasıl yardım edilmelidir?**

**2. Bu tür bombaların kullanımına veya üretimine kısıtlamalar getirilmeli midir?**

**3. Saldırı sonucu bölgede oluşan evsizlik problemi ile nasıl başa çıkılabilir?**

**4. Saldırı sonrası Japonya'nın hasar gören altyapısı nasıl onarılabilir?**

**5.Nükleer Silahların Yayılmasının Önlenmesi Antlaşması'nı imzalamayan ülkeler nasıl nükleer silah gelişimlerini kısıtlamaya teşvik edilebilir?**

**6. Gelecekte meydana gelebilecek olası nükleer savaşlara karşı ne gibi önlemler alınabilir?**

**7. ABD, Rusya, Çin, Birleşik Krallık ve Fransa ülkelerinin nükleer silahlarını barındırmaya devam etmesi ne gibi sonuçlar doğurabilir?**

# E. Günümüz konusu ve açıklaması

Günümüzde internet, günlük yaşamın ayrılmaz bir parçası haline gelmiştir. Araştırma yapmaktan arkadaş edinmeye kadar pek çok farklı amaçla kullanılan internet, sınırsız erişim imkanı sunarken, beraberinde ciddi güvenlik tehditlerini de getirmektedir. İnternette yapılan her işlem, ziyaret edilen web siteleri ve kullanılan hesaplardan elde edilen veriler, zamanla büyük veriyi oluşturur. Bu veriler, kullanıcıların davranışlarını, tercihlerini ve kişisel bilgilerini içerdiği için, kötü niyetli kişilerin eline geçmesi durumunda ciddi sonuçlar doğurabilir. Bu verilerin çalınması, sadece bireyleri değil, aynı zamanda kurumları ve devletleri de tehdit altına sokmaktadır.


Bilgisayar korsanları, hedefledikleri kişilerin veya kurumların verilerini çalarak, bu bilgileri çeşitli kötü amaçlarla kullanabilir. Çalınan veriler, genellikle kimlik hırsızlığı yapmak, dolandırıcılık amacıyla kullanmak veya bu verileri kara pazar üzerinden satmak gibi çeşitli şekillerde değerlendirilebilir. Bu tür siber saldırılar, yalnızca bireylerin güvenliğini değil, aynı zamanda kurumların itibarını ve finansal durumlarını da ciddi şekilde tehdit eder. Özellikle büyük şirketler, **veri ihlallerini** önlemek için yüksek miktarda paralar harcayarak, gelişmiş güvenlik önlemleri almak zorunda kalmaktadır.

Veri ihlalleri, tarihteki en büyük siber güvenlik felaketlerinden bazılarına yol açmıştır. Örneğin, 2013 ve 2014 yıllarında Yahoo'ya yapılan saldırılar sonucunda, yaklaşık 3,5 milyar kişinin telefon numaraları, e-posta adresleri ve güvenlik soruları çalınmış, 2018 yılında ise Cambridge Analytica adlı şirket, 87 milyon Facebook kullanıcısının verilerini izinsiz bir şekilde elde ederek, bu bilgileri siyasi çıkarlar için kullanmıştır. Bu tür olaylar, teknolojiye dayalı ekonomilerin güvenlik tehditleriyle karşı karşıya olduğunu açıkça ortaya koymaktadır.

Veri güvenliğini sağlamak, sadece kişilerin değil, aynı zamanda kurumların ve devletlerin de sorumluluğundadır. Bu tehditlere karşı alınacak önlemler arasında, düzenleyici otoritelerle uyumlu politikaların geliştirilmesi ve kullanıcı farkındalığının artırılması önemli bir yer tutmaktadır. Veri güvenliği, sadece kişisel bilgilerin korunmasını değil, aynı zamanda

mahremiyetin ve güvenliğin sağlanmasını da gerektirmektedir. Bu nedenle, kullanıcılar ve kurumlar arasında güçlü bir işbirliği ve bilinçli yaklaşım, veri ihlallerinin önlenmesinde en etkili

stratejiler arasında sayılabilir. Günümüz meclisi, veri ihlallerini engellemeyi ve siber güvenliği güçlendirmeyi amaçlayan bir protokol yazacaktır.

# Veri hırsızlığı çeşitleri

**Oltalama Saldırıları (Phishing):** Oltalama, sahte e-postalar, mesajlar veya web siteleri aracılığıyla, kullanıcıları kandırarak kişisel bilgilerini (şifre, kredi kartı bilgisi) ele geçirme yöntemidir. Genellikle acil bir işlem yapmalarını isteyen mesajlar gönderilir. Kullanıcılar, gerçek gibi görünen bağlantılara tıklayarak bilgilerini verir.

**Malware (Zararlı Yazılım) Kullanımı:** Malware, bilgisayarlara veya mobil cihazlara bulaşan ve kullanıcı verilerini çalmayı, izlemeyi veya cihazı kontrol etmeyi amaçlayan yazılımlardır. Virüsler, trojanlar ve spyware gibi çeşitleri vardır. Bu yazılımlar, kullanıcıların farkında olmadan çalışabilir ve gizli bilgilere erişim sağlar.

**Man-in-the-Middle (MITM) Saldırıları:** MITM saldırıları, iletişimdeki iki taraf arasına girilerek iletilen verilerin çalınması veya değiştirilmesi işlemidir. Genellikle açık Wi-Fi gibi güvenli olmayan ağlar üzerinden yapılır. Saldırgan, bu sayede kişisel bilgileri veya finansal verileri yakalayabilir.

**Fidye Yazılımı (Ransomware) Saldırıları:** Ransomware, kullanıcıların dosyalarını şifreleyerek erişimlerini engelleyen zararlı yazılımlardır. Saldırganlar, dosyaların çözülmesi için fidye talep eder. Kullanıcı, genellikle ödeme yapmadığı takdirde dosyalarına geri erişemez. Bu tür saldırılar ciddi finansal zararlara yol açabilir.

**Veritabanı Sızıntıları:** Veritabanı sızıntıları, zayıf güvenlik önlemleri veya yazılım açıkları kullanılarak, büyük miktarda kişisel verinin çalındığı saldırılardır. Bu tür saldırılar genellikle

kurumların veri tabanlarına yapılır. Çalınan veriler, kimlik hırsızlığı, dolandırıcılık ve diğer suçlar için kullanılabilir.

# Tarihin büyük veri ihlalleri

### Equifax Veri İhlali (2017)

2017 yılında, Amerika'nın en büyük kredi raporlama ajanslarından biri olan Equifax, büyük çaplı bir veri ihlali yaşadı. Bu saldırı sonucunda 147 milyon kişinin kişisel ve finansal bilgileri çalındı. Çalınan veriler arasında kredi kartı bilgileri, sosyal güvenlik numaraları ve doğum tarihleri gibi son derece hassas bilgiler yer alıyordu. Bu olay, milyonlarca Amerikalı için ciddi kimlik hırsızlığı ve güvenlik riskleri oluşturdu

### Target Veri İhlali (2013)

2013 yılında, büyük perakende zinciri Target, siber saldırıya uğrayarak yaklaşık 40 milyon müşterisinin kredi kartı ve banka kartı bilgilerini kaybetti. Saldırganlar, şirketin ödeme sistemlerine sızarak bu bilgileri ele geçirdi. Olay, perakende sektöründe dijital güvenliğin önemini bir kez daha gündeme taşıdı.

### Adobe Veri İhlali (2013)

Adobe, 2013 yılında gerçekleşen bir siber saldırı sonucunda 38 milyon kullanıcısına ait verilerin sızdırılmasıyla büyük bir güvenlik ihlali yaşadı. Saldırganlar, kullanıcı adları, şifreler ve kredi kartı bilgilerini içeren önemli verilere ulaştı. Bu olay, yazılım devlerinin de siber tehditlere karşı ne kadar savunmasız olabileceğini gösterdi.

## LinkedIn Veri İhlali (2012)

2012 yılında profesyonel sosyal ağ platformu LinkedIn, büyük bir veri ihlali ile karşı karşıya kaldı. Bu saldırı sonucunda 167 milyon kullanıcının hesap şifreleri ve e-posta adresleri gibi bilgileri çalındı. Çalınan veriler, daha sonra karanlık internet pazarlarında satışa sunularak milyonlarca kişinin hesap güvenliğini tehlikeye attı.

### Clearview AI Veri İhlali – 2020

Şubat ayında tartışmalı şirket, bir bilgisayar korsanının müşteri listesine "yetkisiz erişim sağladığını" bildirdi. Şirket müşterilerinin çoğu, bir şüphelinin fotoğraflarını çeken ve bunları şirketin 3 milyardan fazla görüntüden oluşan veri tabanıyla karşılaştıran kolluk kuvvetleri.

Şirketin siber ihlale tepkisi basitti: "Ne yazık ki, veri ihlalleri 21. yüzyılda hayatın bir parçası." Söz konusu firma, güvenlik açığını giderdiğini ve sunucularının güvende olduğunu iddia ediyor.

### Nintendo Veri İhlali – 2020

2020-Nisan ayında Nintendo, yaklaşık 160 bin hesap, e-posta ve şifre listesinin açığa çıktığını duyurdu. Sızan verilerin listesi ayrıca isimleri, doğum tarihlerini, cinsiyeti ve ülkeyi de içeriyor.

Şirket, kullanıcılarını hesaplarının güvenliğini artırmak için iki faktörlü kimlik doğrulama kullanmaya çağırdı. İyi tarafı, hiçbir kredi kartı bilgisi sızdırılmadığı için kullanıcıların paraları güvende kaldı.

### Tetrad Veri İhlali – 2020

Şubat ayında Tetrad, milyonlarca Amerikan hanesi ve işletmesi hakkındaki bilgileri açığa çıkaran büyük bir veri ihlalinin kurbanı oldu.

Şirket, bir Amazon S3 kovasını yanlış yapılandırarak verilere web tarayıcısı olan herkesin erişebilmesini sağladı. Bilgiler toplam 747 GB'lık üç dosyada bulunuyordu. Neyse ki, sızıntının keşfedilmesinden bir hafta sonra şirket, ilgili güvenlik açığını giderdi.

**Virgin Media Veri İhlali – 2020**

Mayıs ayında Virgin Media, 10 ay boyunca erişilebilir ve güvenli olmayan yaklaşık 900.000 kullanıcıya ait kişisel veri olduğunu kabul etti.

Nedeni? Elbette yanlış yapılandırılmış bir veritabanı! Yetkisiz bir kullanıcı tarafından en az bir kez erişildi. İşin iyi tarafı, sızdırılan bilgiler herhangi bir finansal bilgi içermiyordu.

**Yahoo Veri İhlali (2013 - 2016)**

Bir zamanlar internetin devlerinden biri olan Yahoo, 2013 yılında tarihin en büyük veri ihlallerinden birine sahne oldu. Kimliği o dönemde bilinmeyen bir saldırgan, şirketin veritabanına sızarak tam 3 milyar kullanıcı hesabına erişim sağladı. Bu devasa saldırı, ancak 2016 yılında ortaya çıkarılabildi. Olayın büyüklüğü ve gecikmeli tespiti, Yahoo'nun güvenlik konusundaki zafiyetlerini gözler önüne serdi.

Veri ihlali, Yahoo'nun telekomünikasyon devi Verizon ile yürüttüğü satın alma görüşmelerinin tam ortasında patlak verdi. Sonuç olarak, anlaşma bedeli 350 milyon dolar düşürüldü ve Yahoo, 4,48 milyar dolara satıldı. Ancak bu maddi kayıp, şirketin itibarındaki sarsıntının yalnızca küçük bir kısmını temsil ediyordu.

Saldırı sırasında çalınan bilgiler arasında kullanıcıların tam adları, doğum tarihleri, e-posta adresleri, şifreler ve güvenlik soruları ile yanıtları bulunuyordu. Yahoo, bu siber saldırının arkasında devlet destekli bir grubun olduğunu iddia etti. Sonrasında ortaya çıkan bilgiler, ABD

Adalet Bakanlığı'nın bu saldırının Rusya Federal Güvenlik Servisi (FSB) ile bağlantılı olduğunu düşündüğünü gösterdi.

Bu olay, sadece Yahoo'nun değil, tüm teknoloji devlerinin dijital güvenlik konusunda nasıl büyük tehditlerle karşı karşıya olduğunu tüm dünyaya gösterdi.

# F. Günümüz alt başlıkları

### 1.İnternet kullanıcıları veri ihlallerinden korunma konusunda nasıl bilinçlendirilebilir?

### 2. Devletin veri ihlallerini engellemedeki rolü nedir?

### 3. Veri ihlallerinin engellenmesi için ne gibi yasal düzenlemeler yapılabilir?

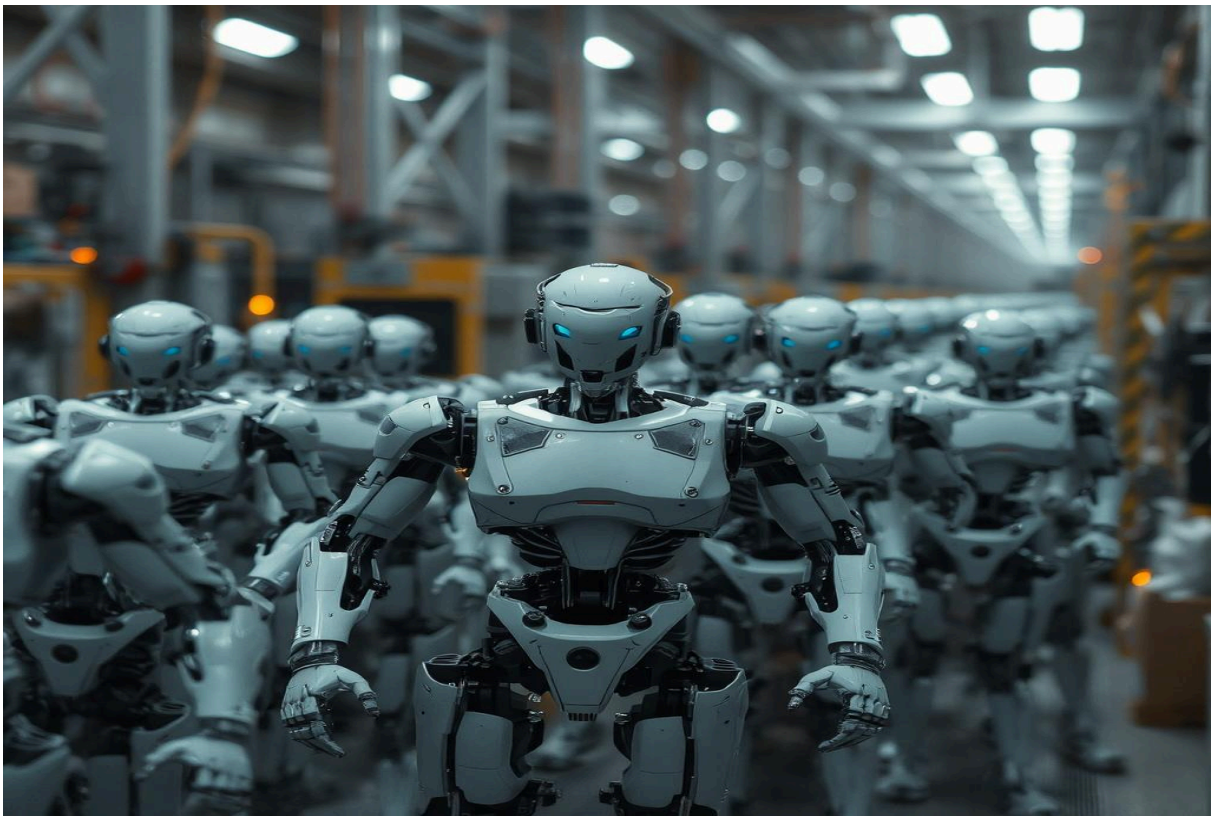
### 4. Kurumlar veri ihlallerinden korunmak için ne gibi önlemler almalıdır?

### 5. Bilgisayar korsanları siber saldırılardan önce nasıl tespit edilip etkisiz hale getirilebilir?

### 6. Veri ihlallerini önlemek için ne gibi teknolojik çözümler üretilebilir?

### 7. Sosyal medya platformlarının veri güvenliği konusundaki sorumlulukları nelerdir ve nasıl bu sorumlulukları üstlenmeye teşvik edilebilir?

## G. Gelecek konusu ve açıklaması



2085 yılı, yapay zeka teknolojilerinin zirveye ulaşarak günlük hayatta robot kullanımının yaygınlaştığı bir dönüm noktası haline gelmiştir. Teknolojik ilerlemeler, insanların rutin işlerini yorulmadan, karşılık beklemeden yapan makinelerin hayata girmesiyle hayatı teknik açıdan kolaylaştırmıştır. Bu değişim, birçok alanda devrim niteliğinde gelişmelere yol açmış, insanların fiziksel yükleri azalırken zaman ve iş gücü daha verimli kullanılmaya başlanmıştır. Ancak bu hızlı gelişim, sadece olumlu etkiler yaratmakla kalmamış, toplumsal yapıyı ve ekonomiyi derinden sarsan yeni sorunlar da ortaya çıkarmıştır. 2084 yılının Şubat ayında robotların seri üretimi başlamış ve hızla yaygınlaşan bu teknoloji, 2085 yılının başlarına gelindiğinde birçok sektörde iş gücünün yerini almıştır. İlk başlarda robotlar yalnızca fabrikalarda, tarımda ve ağır sanayide çalışmaya başlamışken, zamanla sağlık, eğitim, hizmet sektörü gibi daha karmaşık ve insana dayalı alanlarda da devreye girmiştir. Bu gelişmelerle birlikte insanlara olan iş talebi büyük oranda azalmıştır. İnsanlar, makinelerin daha hızlı ve verimli çalışabilmesi karşısında ekonomik olarak zayıf düşmüş, milyarlarca insan kendini işsiz ve değersiz bir pozisyonda bulmuştur.

Bir işsizlik krizi başlamış, robotlar insanlar yerine her sektörde çalışarak üretkenliği artırmış olsa da, insana dayalı işler olağanüstü düzeyde azalmıştır. Eğitim sektöründe de çeşitli değişimler meydana gelmiştir. Yapay zeka mühendisliği, programlama ve diğer robot üretimi ve denetimi ile ilgilenen alanlara büyük bir yığılım olmuştur. Bazı insanlar kariyer seçeneklerinin azalması ile robotların yapamadığı işlere yönelme arayışıyla estetik ve ustalık gerektiren meslekleri tercih etmeye başlamıştır. Müzik, sanat, el yapımı ürünler gibi yaratıcı iş kolları, robotların hâlâ insan dokunuşuna ihtiyaç duyduğu alanlar olarak popülerlik kazanmıştır. Ancak bu alanlar, beceri ve yetenek gerektirir ve dolayısıyla sınırlı sayıda insanlar bu sektörlerden yararlanabilir. Ekonomik açıdan değerlendirildiğinde, robotların yaygınlaşması toplumda daha önce görülmemiş bir **gelir uçurumu** yaratmıştır.

Robotların sahipliği ve işletilmesi, robotlara erişimi olan varlıklı kesimlerin lehine bir avantaj sağlamıştır. Zengin insanlar, sahip oldukları robotları çalıştırarak büyük kazançlar elde etmişlerdir. Bu kişiler, robotların sağladığı yüksek verimlilik sayesinde daha da zenginleşmişlerdir. Öte yandan, robotlar insanı işgücü piyasasının dışına itmiş ve teknolojiye erişimi olmayan düşük gelirli insanlar giderek fakirleşmiştir. Bu eşitsizlik, toplumda derin bir sınıf ayrımına yol açmıştır. Zenginler daha fazla zenginleşirken, yoksullar daha da yoksullaşmıştır. Bu durumda, teknolojinin getirdiği eşitsizlik, sadece ekonomik değil, aynı zamanda sosyal huzursuzluklara da yol açmaktadır. Yoksul sınıflar, kendilerini toplumdan dışlanmış ve geleceksiz hissetmektedir. Çalışma imkânlarından yoksun kalan büyük nüfus, hayatta kalabilmek için farklı yöntemler aramaya başlamış, suç oranları artmış ve toplumda güvensizlik yaygınlaşmıştır. Bu sosyal gerilimler, toplumda huzursuzluk yaratmış, hükümetler ve

uluslararası kuruluşlar çözüm arayışlarına girmiştir. Gelecek oturumlarında bu sorunlara çözüm olacak bir protokol yazılacaktır.

## H. Gelecek alt başlıkları

**1. Robotların seri üretim sürecinde etik sorunlar var mıdır?**

**2. İş imkanlarının azalmasıyla oluşan işsizlik krizinin nasıl önüne geçilebilir?**

**3. Meydana gelen değişimlere göre eğitim sisteminde ne gibi düzenlemeler yapılmalıdır?**

**4. Robotların seri üretimi kısıtlanmalı mıdır?**

**5. Toplumda meydana gelebilecek sosyal huzursuzluklar ile nasıl başa çıkılabilir?**

**6. Robotların sağlık, eğitim gibi sektörlerde kullanılması olumsuz sonuçlar doğurabilir mi?**

**7. Kriz esnasında düşük gelirli sınıfların durumlarının kötüleşmesinin nasıl önüne geçilebilir?**

# I. Kaynakça


https://tr.wikipedia.org/wiki/Manhattan_Projesi

https://tr.wikipedia.org/wiki/N%C3%BCkleer_Silahlar%C4%B1n_Yay%C4%B1lmas%C4%B1n%C4%B1n_%C3%96nlenmesi_Antla%C5%9Fmas%C4%B1

https://dergipark.org.tr/en/download/article-file/3116868

https://tr.wikipedia.org/wiki/Cambridge_Analytica

https://tr.wikipedia.org/wiki/Facebook-Cambridge_Analytica_veri_skandal%C4%B1

https://tr.wikipedia.org/wiki/Hiro%C5%9Fima_ve_Nagasaki%27ye_atom_bombas%C4%B1_sald%C4%B1r%C4%B1s%C4%B1