

EJONS

International Journal on Mathematics, Engineering and Natural Sciences

(Uluslararası Fen, Mühendislik ve Doğa Bilimleri Dergisi)

<https://ejons.org/index.php/ejons>

e-ISSN: 2602 - 4136

Derleme Makalesi

Doi: <https://doi.org/10.5281/zenodo.14254063>

Dijital Çağda Önleme: Güvenli ve Sağlıklı Çalışma Hayatı için Çözümler

Serap TEPE^{1*}¹ Sağlık Bilimleri Üniversitesi, Hamidiye Sağlık Bilimleri Fakültesi, Sosyal Hizmet Bölümü, 34700, İstanbul, Üsküdar*Sorumlu Yazar e-mail: serap.tepe@sbu.edu.tr

Makale Tarihi

Geliş: 23.09.2024

Kabul: 12.11.2024

Anahtar Kelimeler

İş güvenliği,
İş sağlığı,
Önleme politikası,
Dijitalleşme

Öz: Çalışma hayatını sağlıklı ve güvenli bir ortamda oluşturma ve sürdürme adına alınan önlemler korunma politikalarının temelini oluşturmaktadır. Çünkü çalışma ortamlarında korunma ve güvenlik politikalarının etkili bir şekilde uygulanması, çalışanların sağlığını ve güvenliğini korumanın temelidir. Alınan bu önlemlerin dijital çağda çeşitlenmesi, içeriklerinin değişmesi, sınırlarının genişlemesi gibi faktörler nedeniyle bugün gelen noktada bu önlemlerin hem uygulanabilirlik açısından etkinlikleri hem uygulandığında oluşturabilecekleri etik meseleler hem de önleme politikaları kapsamında çalışma hayatında dikkat edilmesi gereken hususlar tartışılması gereken konulardandır. Tüm bu parametreler birlikte düşünüldüğünde önerilen yazıda öncelikle güvenlik ve sağlık kavramlarına değinilmiştir. Dijital çağda güvenlik ve sağlıkla ilgili çalışma ortamında var olan uygulamalar, karşılaşılan zorluklar ve konu ile ilgili çözümler ifade edilmiş, sonrasında etik ve yasal sorumluluklar ekseninde alınabilecek önlemler ve önlemenin gerekliliği tartışılmıştır. Sürdürülebilir bir çalışma ortamının inşa edilmesi, sağlıklı ve güvenli çalışma koşullarının oluşturulması, çalışanın fiziksel, ruhsal, sosyal iyi oluşunun sağlanması ve iş barışının korunması adına dijital çağın tüm nimetlerinden en etkin seviyede yararlanırken bu durumun yasal ve etik sınırlar içerisinde değerlendirilmesi gerektiği düşünülmektedir.

Atıf Künyesi: Tepe, S., (2024). Dijital Çağda Önleme: Güvenli ve Sağlıklı Çalışma Hayatı İçin Çözümler, EJONS International Journal on Mathematics, Engineering and Natural Sciences 8(4), 480-492. **How To Cite:** Tepe, S., (2024). Digital Age Prevention: Solutions for a Safe and Healthy Working Environment, EJONS International Journal on Mathematics, Engineering and Natural 8(4), 480-492.

Digital Age Prevention: Solutions for a Safe and Healthy Working Environment

Article Info

Received: 23.09.2024

Accepted: 12.11.2024

Keywords

Abstract: Measures taken to establish and maintain a healthy and safe working environment form the basis of prevention policies. This is because the effective implementation of prevention and safety policies in work environments is fundamental to safeguarding the health and safety of employees. Due to factors such as the diversification of these measures, changes in their content, and the expansion of their boundaries in the digital age, there is a need to discuss the practicality of these measures, the ethical issues they may raise when implemented, and the considerations that need to be considered in the context of prevention policies in the workplace. When considering all these parameters collectively, this paper first addresses the concepts of safety and health. It elaborates on the existing

Occupational safety,
Occupational health,
Prevention policy,
Digitalization

practices, challenges faced, and solutions related to safety and health in the digital age within the workplace. Subsequently, it discusses the measures to be taken and the necessity of prevention within the framework of ethical and legal responsibilities. It is believed that while constructing a sustainable working environment, establishing healthy and safe working conditions, ensuring the physical, mental, and social well-being of employees, and maintaining industrial peace while effectively harnessing all the benefits of the digital age, the situation should be evaluated within legal and ethical boundaries

1.Giriş

Çalışma hayatı, bir insanın tüm hayat serüveninde en büyük yer kaplayan bölümlerden biri olduğundan insanlara güvenli ve sağlıklı bir çalışma ortamı sağlamak son derece önemlidir. Hem işverenler hem de çalışanlar, iş yerlerinde güvenliği ve sağlığı teşvik etmek için birlikte çalışmalıdır. Burada tartışılması gereken ilk husus; güvenli çalışma ve sağlıklı çalışma kavramlarıdır. İşyerinde güvenli ve sağlıklı çalışma denildiğinde olası risk faktörlerinden, iş kazalarından ve meslek hastalıklarından uzak bir çalışma ortamında iş görme kastedilmektedir. Bunu sağlamak için ise; zaman, sabır, emek, güvenlik kültürüne inanç ve mevzuata hakimiyet gerekmektedir. Her ne kadar işyerinde güvenli ve sağlıklı çalışma denildiğinde fiziksel riskler, kimyasal riskler, biyolojik riskler gibi alışlagelmiş risk faktörleri akla gelse de günümüzün değişen dünyasında çalışanları yaptıkları işlerden, değişen teknolojinin beraberinde getirdiği sorumluluklardan, buldukları çalışma ortamları veya ait oldukları yapıdaki psikososyal süreçlerden kaynaklı çok fazla sayıda ve çok farklı çeşitte risk beklemektedir. Tüm bu riskler çalışan sağlığını ve güvenliğini, ayrıca iş barışını ve örgütsel aidiyeti önemli derecede etkilemektedir. Sağlıklı ve güvenli bir çalışma ortamının oluşturulması ve sürdürülmesi, iş yerindeki korunma politikalarının temelini oluşturur. Bu güvenlik ve korunma politikalarının etkili bir şekilde uygulanması, çalışanların sağlığını ve güvenliğini korumanın temelidir. Bu önlemlerin dijital çağda çeşitlenmesi, içeriklerinin değişmesi ve kapsamalarının genişlemesi, uygulanabilirlikleri açısından etkinliklerinin yanı sıra ortaya çıkarabilecekleri etik meseleler ve korunma politikaları çerçevesinde dikkate alınması gereken hususlar arasında tartışılması gereken konulardır (Solove, 2004). Klasik anlamda düşünüldüğünde bir çalışma ortamında güvenli ve sağlıklı çalışma denildiğine olması gerekenler şöyle özetlenebilir. İş sağlığı ve güvenliği eğitimlerinin gerçekleştirilmesi, temizlik ve hijyen kurallarına uyulması, ergonomik çalışma koşullarının düzenlenmesi, işyeri güvenliği ve çalışan güvenliği ekipmanlarının kullanılması, risk analizlerinin yapılması güvenli ve sağlıklı çalışma şartlarından birkaçı olarak sayılabilmektedir. Çalışanların iş sağlığı ve güvenliği konularında eğitim alması önemlidir. İşverenler, çalışanlarına iş yerindeki riskleri ve güvenlik prosedürlerini öğretmelidir. Bu eğitim, iş kazalarını ve meslek hastalıklarını önlemeye yardımcı olur. İş yerlerinde risklerin belirlenmesi ve bu risklerin minimize edilmesi için düzenli olarak risk değerlendirmesi yapılmalıdır. İşverenler, potansiyel tehlikeleri tanımalı ve çalışanların güvende olmalarını sağlamak için gerekli düzenlemeleri yapmalıdır. Risk, olasılık ve şiddetin bileşiminden meydana gelen bir kavramdır. Olasılık, gerçekleşme ihtimali olan durumları içerirken, şiddet ise bu durumların sonuçlarına bağlı olarak ortaya çıkacak etkileri ifade etmektedir. Risk esasen, sonsuz seçeneklere sahip olasılıkların ve bu seçeneklerden herhangi birisinin gerçekleştiğinde bırakacağı izlerin bir kombinasyonudur. Bu zaviyeden bakıldığında riskin öncesi ve sonrası olan girift bir yapıya sahip olduğu düşünülmektedir. Öncesi olarak adlandırılan aşamada, olasılıkların yönetilmesi ve proaktif tedbirlerin alınması gereklidir. Bu aşama, olayların, mekanların, kişilerin ve durumların potansiyel risklerini kontrol altına alınması faaliyetlerini içermektedir. Sonrası olarak nitelendirilen aşama ise; risk gerçekleştiğinde ortaya çıkacak zararların minimize edilmesi ve en düşük kayıpla atlatılması için yapılması gereken faaliyetleri içermektedir (Tepe, 2023). Risk genellikle tehdit olarak algılsa da aslında fırsatlarla da ilişkilidir. Risk analizi, tehlikeleri tespit etmek, önlem almak ve kabul edilebilir düzeye düşürmek için kullanılan yöntemler bütünüdür ve her risk analizi aslında elde olan veya değerlendirilebilecek fırsatları görme adına da önem arz etmektedir. Bu nedenle, risk analizleri sayesinde doğru bir tanım ve etkin bir yönetim süreci ile risklerin fırsatlara dönüşmesi mümkündür. Risk analiz süreçleri, çalışma ortamlarını iyileştirebilir, kişilerin farkındalığını artırabilir ve

müdahale imkanlarını ortaya çıkarabilir. Riskleri doğru şekilde tanımlayarak ve etkin bir şekilde yöneterek, mevcut durumu korumanın ötesinde, daha iyi bir düzeye taşıma şansı elde edilebilir. Temiz ve hijyenik bir çalışma ortamı, çalışanların sağlığını korumak için önemlidir. İş yerleri düzenli olarak temizlenmeli ve dezenfekte edilmelidir. Ayrıca, çalışanlar için hijyenik önlemler de alınmalıdır. Ergonomik çalışma koşulları, çalışanların rahat ve sağlıklı bir şekilde çalışmalarına yardımcı olur. İşverenler, ergonomik ofis mobilyaları, bilgisayar ekipmanları ve çalışma düzenlemeleri sağlamalıdır. Çalışma hayatındaki stres, çalışanların sağlığını olumsuz etkileyebilir. İşverenler, çalışanların iş stresini yönetmelerine yardımcı olacak politikalar ve programlar geliştirmelidir. Çalışan sağlığı hizmetleri, çalışanların sağlık sorunlarını tespit etmelerine ve tedavi almalarına yardımcı olur. İşverenler, çalışanlara düzenli sağlık kontrolleri ve danışmanlık hizmetleri sunmalıdır. Çalışma koşullarına uygun kişisel koruyucu ekipmanların sağlanması ve kullanılması önemlidir. İşverenler, çalışanlara gerekli ekipmanları sağlamalı ve bu ekipmanların düzgün bir şekilde kullanılmasını teşvik etmelidir. Güvenli ve sağlıklı çalışma koşulları hem işverenlerin hem de çalışanların sorumluluğundadır. İş birliği ve dikkatli planlama ile iş yerlerindeki riskleri minimize edebilir ve çalışanların daha sağlıklı ve mutlu olmaları sağlanabilir. Güvenli ve sağlıklı bir çalışma ortamı hem iş verimliliğini artırır hem de iş kazalarını ve meslek hastalıklarını azaltır (Ertaş,2023). Kısaca ifade edilen bu adımlar, güvenli ve sağlıklı çalışma ortamı oluşturma hususunda önemli adımlardır ancak günümüz şartlarında yeterli değildir. Günümüzde, insanlar ve algoritmalar arasındaki ilişki, geçmiş dönemlere göre daha yakın ve karşılıklı yoğun etkileşim içerisindedir. Çalışma hayatında yapay zekanın, giyilebilir teknolojinin, artırılmış gerçekliğin kullanıldığı, sensörlerin tüm çalışma ortamlarında aktif olarak kullanılmaya başladığı bu dönemde güvenli ve sağlıklı çalışma anlayışı da evrilmektedir. Mevcut durum, veri biliminin sunduğu faydaların yanı sıra beraberinde etik ve yasal sorumlulukları da getirmektedir. Çünkü dijital platformlar ve kullanılan uygulamalar, bireylerin yalnızca sosyal yaşamlarını ve iş hayatlarını bireysel olarak etkilemekle kalmamakta, aynı zamanda iş görme ile ilgili tüm paydaşları kapsamakta ve ekonominin önemli bir parçasını oluşturmaktadır. Bu nedenle dijital çağda artık tartışılması gereken başlıklar; güvenli ve sağlıklı bir çalışma ortamını sağlama adına, veri üretimi, üretilen verinin korunması, iş süreçlerinde dijital ortamlarda etik yaklaşımlara sadık kalınması, yasal sorumlulukları yerine getirirken dijital dünyanın gücünden efektif olarak yararlanılması ve tüm bu işleyiş içerisinde çalışanın haklarının, sağlığının, fiziksel, ruhsal ve sosyal açıdan iyi oluşunun korunacak şekilde çalışma ortamlarının yeniden düzenlenmesi olmalıdır. Bu başlıkların tartışılmasının güvenli ve sağlıklı çalışma ortamı inşa etme adına önemli olduğu düşünülmektedir. Ayrıca önerilecek çözümlerle dijital çağda önleme politikalarının oluşturulmasında dikkat edilmesi gereken değerlere öncülük edileceği ön görülmektedir. Bu çalışmanın araştırma sorusu dijital çağda iş sağlığı ve güvenliği uygulamalarının etkinliğinin çalışanların psikososyal sağlığı üzerindeki etkilerinin neler olduğu hakkında farkındalık oluşturmaktır. Dijital çağda, iş sağlığı ve güvenliği (İSG) uygulamaları, teknolojinin hızla gelişmesiyle birlikte yeni bir boyut kazanmıştır. Uzaktan çalışma, dijital iletişim araçlarının yaygın kullanımı ve veri analitiği gibi unsurlar, çalışanların iş yerindeki deneyimlerini ve psikososyal sağlıklarını doğrudan etkilemektedir. Bu bağlamda, araştırma sorusu, dijitalleşmenin İSG uygulamaları üzerindeki etkilerini ve bu uygulamaların çalışanların psikososyal sağlığına olan yansımalarını incelemeyi amaçlamaktadır. Dijital çağda güvenlik ve sağlık politikalarının uygulanabilirliği ile ilgili hangi zorlukların var olduğu, çalışma ortamında karşılaşılan dijital etik meseleler ve sürdürülebilir bir çalışma ortamı oluşturmak için hangi önlemlerin alınması gerekliliği hakkında farkındalık oluşturmak çalışmanın motivasyonudur.

2. Kavramsal Çerçeve

2.1. Güvenlik ve Sağlık

Güvenlik kelime anlamı olarak toplumda yasal düzenin aksamadan yürütülmesi, bireylerin korkusuzca yaşayabilmeleri ve güven içinde hayatlarını idame ettirebilmeleri durumu şeklinde tanımlanmaktadır (Tepe, 2022). Güvenlik, bir kişinin, bir organizasyonun veya bir topluluğun, zararlı etkilerden, tehlikelerden ve risklerden korunma durumunu ifade etmektedir. Güvenlik, birçok farklı yönü olan karmaşık bir kavramdır ve birçok farklı düzeyde uygulanabilir. Her durumda güvenlik, potansiyel tehlikelere karşı koruma sağlamak, riskleri azaltmak ve olumsuz sonuçları en aza indirmek için çeşitli stratejiler ve önlemler içermektedir. Güvenlik, fiziksel güvenlik, bilgi güvenliği, siber güvenlik,

kişisel güvenlik, toplumsal güvenlik ve iş güvenliği gibi farklı alt başlıklarda incelenebilir. Fiziksel güvenlik, binaları, varlıkları ve insanları fiziksel tehditlere karşı koruma amacı taşır. Örnekler arasında kapılar, kilitler, güvenlik kameraları, alarm sistemleri ve güvenlik personeli yer alabilir. Bilgi güvenliği, verilerin, bilgisayar sistemlerinin ve dijital iletişimlerin yetkisiz erişime, manipülasyona veya zararlı yazılımlara karşı korunmasını içerir. Şifreleme, güvenlik yazılımları, ağ güvenliği önlemleri ve güvenlik protokolleri bilgi güvenliği için kullanılır. Siber güvenlik, dijital ortamda yer alan bilgisayar sistemlerini, ağları ve verileri siber saldırılara karşı koruma amacını taşır. Bu tür tehditler arasında virüsler, kötü amaçlı yazılımlar, bilgi sızdırmaları ve siber suçlar yer alabilir.

Kişisel güvenlik, bireylerin fiziksel ve zihinsel bütünlüklerini koruma çabalarını ifade eder. Bu, kişisel güvenlik önlemleri, acil durum hazırlığı ve kişisel korunma yöntemlerini içerir. Toplumsal güvenlik, toplumun genel olarak güvenliğini ve halkın refahını koruma amacını taşır. Bu başlık, polis, itfaiye, sağlık hizmetleri, acil durum hazırlığı ve kriz yönetimi gibi alanları içermektedir. İş güvenliği, işyerlerinde çalışanların fiziksel sağlığını ve güvenliğini sağlamak amacıyla uygulanan önlemleri içerir. İş güvenliği politikalarının temel amacı iş kazalarını ve meslek hastalıklarını önlemeye yönelik politikalar oluşturmak ve çalışmalar yapmaktır. Sağlık, bireyin fiziksel, zihinsel ve sosyal yönden tam bir iyilik halinde olma durumunu ifade etmektedir. Sağlık, sadece hastalıklardan veya rahatsızlıklardan uzak olmak anlamına gelmez, aynı zamanda kişinin bedensel ve zihinsel fonksiyonlarının uyum içinde çalışması, toplumsal ilişkilere katılma yeteneği ve yaşam kalitesini artırma kapasitesini de içermektedir. Fiziksel Sağlık, bedenin hastaliksız ve işlevsel bir durumda olması anlamına gelmektedir. Bu durum, yeterli beslenme, düzenli egzersiz, vücut ağırlığının kontrolü ve hastalıklardan korunma gibi faktörleri içermektedir. Ruh Sağlığı, zihinsel ve duygusal iyilik hali olarak tanımlanmaktadır. Ruh sağlığı, stresle başa çıkma, ilişkilerde sağlıklı iletişim kurma, psikolojik sorunlarla başa çıkma ve kişisel gelişim gibi alanları içermektedir. Sosyal Sağlık, kişinin toplumsal ilişkilere katılma yeteneğini ve toplum içindeki rolünü sağlıklı bir şekilde sürdürme yeteneğini ifade etmektedir. Sosyal sağlık, destekleyici ilişkiler kurma, toplumsal katılım, adalet ve eşitlik gibi faktörleri içermektedir. Sağlık, birçok faktörün etkileşimi sonucunda elde edilen bir denge durumudur. Bu faktörler arasında genetik yatkınlık, yaşam tarzı seçimleri, çevresel koşullar, ekonomik durum ve sağlık hizmetlerine erişim gibi etkenler yer almaktadır. Sağlıklı bir yaşam sürdürmek için düzenli tıbbi muayeneler, sağlıklı beslenme, egzersiz, stresten kaçınma, zararlı alışkanlıklardan uzak durma ve sosyal ilişkilere önem verme gibi faktörlere dikkat etmek önemlidir.

Sağlık ve güvenlik kavramları çalışma ortamlarında bir arada olması gereken kavramlardır. Çalışanın sağlığının korunduğu ve güvenliğinin sağlandığı bir ortamda çalışması onun motivasyonunu artıracak gibi işletmenin performansını da artıracaktır. Ancak olası kazaların önüne geçme adına faaliyetlerin yapıldığı, çalışma koşullarının iyileştirildiği ve sağlık gözetimlerinin gerçekleştirildiği ortamlarda güvenli ve sağlıklı çalışma gerçekleştirilebileceği düşünülmektedir.

2.2. Dijital Çağda Güvenlik ve Sağlık: Yeni Zorluklar ve Çözümler

2.2.1. Dijital Tehditlere Karşı Güvenlik Önlemleri: İşletmelerin Güvenlik Stratejileri

Dijital çağ, işletmeler için büyük fırsatlar sunarken aynı zamanda yeni güvenlik tehditlerini de beraberinde getirmektedir. Siber saldırılar, veri sızıntıları ve kimlik avı gibi tehditler, çalışanların ve işletmelerin güvenliğini tehlikeye atabilmektedir.

Dijital çağın çalışma hayatına getirdiği yeniliklerle birlikte, işletmeler artık dijital verileri koruma sorumluluğunu taşımaktadır. Ancak, bu veriler siber saldırılar, veri sızıntıları ve kimlik avı gibi tehditlerle karşı karşıya kalabilmektedir. Bu nedenle, işletmelerin dijital tehditlere karşı alabileceği önlemler giderek daha karmaşık hale gelmiştir.

Güçlü şifreleme yöntemleri, verilerin yetkisiz erişimden korunmasında temel bir rol oynar. Hassas verilerin şifrelenmesi, verilerin güvenliğini artırmakta ve yetkisiz kişilerin bu verilere erişimini engellemektedir. İki faktörlü kimlik doğrulama gibi yöntemlerle, kullanıcıların doğrulama süreçleri daha da güçlendirilebilir. Bu durum hesapların daha güvenli bir şekilde korunmasını sağlamaktadır.

Güvenlik yazılımları, işletmelerin bilgisayarlarını ve ağlarını siber saldırılardan korur. Anti virüs yazılımları, kötü amaçlı yazılımları tespit eder ve temizlerken, güvenlik duvarları (firewall) yetkisiz erişimleri engellemektedir. Bu yazılımların düzenli olarak güncellenmesi, yeni tehditlere karşı koruma

sağlayacaktır. Ayrıca, saldırıları tespit edip önleyen Intrusion Detection and Prevention Systems (IDS/IPS) gibi sistemler de kullanılabilir.

İşletmeler, güvenli ağ yapıları oluşturarak içerideki ve dışarıdaki tehditlere karşı koruma sağlayabilmektedirler. Ayrıca, çalışanlar uzaktan erişim gerektiğinde Sanal Özel Ağ (VPN) kullanarak güvenli bir şekilde bağlantı kurabilirler. VPN, verileri şifreleyerek güvenli bir iletişim sağlar ve kamusal ağlardan gelen tehditleri engeller.

İnsan faktörü, dijital güvenliğin en önemli bileşenlerinden biridir. Çalışanlar, güçlü şifreler oluşturma, şüpheli e-postaları tanıma gibi konularda eğitilmelidir. Eğitim programları, çalışanları dijital tehditlere karşı bilinçlendirerek sosyal mühendislik saldırılarına karşı daha dirençli hale getirebilir. Bilinçli kullanıcılar, phishing girişimlerini daha kolay tanır ve verileri koruma konusunda daha dikkatli davranır.

İşletmeler, düzenli güvenlik denetimleri yaparak sistemlerini zayıf noktalara karşı tarayabilirler. Bu denetimler, potansiyel açıkları tespit edip kapatmaya yardımcı olur. Ayrıca, yazılım ve işletim sistemlerinin güncel tutulması da önemlidir. Güvenlik açıklarını gidermek için düzenli güncellemeler yapılırken, güncel yazılımlar ve uygulamalar kullanılarak yeni tehditlere karşı önlem alınabilir.

Dijital güvenlik ihlalleri her zaman engellenemeyebilir. Bu durumda, işletmelerin acil durum planları hazır olmalıdır. Acil durum planları, saldırılar gerçekleştiğinde hızlı ve etkili bir şekilde müdahale etmeyi sağlar. Kriz yönetimi ekipleri, olayın etkilerini değerlendirir, müşterilere ve paydaşlara doğru bilgi verir ve sistemin normale dönmesi için adımları yönlendirir.

Dijital güvenlik, uzmanlık ve deneyim gerektiren bir alandır. İşletmeler, güvenlik açıklarını tespit etmek ve gidermek için dış kaynaklardan yardım alabilirler. Etik hackerlar (ethical hackers) işletmelerin güvenlik açıklarını test ederek belirler ve düzeltmeye yardımcı olabilirler. Ayrıca, güvenlik danışmanlık firmaları, işletmelere özelleştirilmiş güvenlik çözümleri ve stratejiler sunarak dijital güvenliği sağlama konusunda yardımcı olabilirler.

Dijital çağın getirdiği güvenlik tehditleri karşısında işletmelerin bilinçli, hazırlıklı ve güncel kalması hayati öneme sahiptir. Dijital güvenlik stratejileri sürekli olarak gözden geçirilmeli, güncellenmeli ve çalışanlar sürekli eğitilmelidir. Bu şekilde, işletmeler verilerini koruyabilir, müşteri güvenini sağlayabilir ve dijital dünyadaki varlığını güvence altına alabilir.

2.2.2. Dijital Sağlık Takip Sistemleri ve Veri Güvenliği: Çalışan Sağlığını Koruma Stratejileri

Dijital sağlık takip sistemleri, günümüzde işletmelerin çalışanların sağlık durumlarını izlemek, analiz etmek ve değerlendirmek için yaygın olarak kullandığı önemli bir araç haline gelmiştir. Bu sistemler, kalp atış hızı, uyku düzeni, fiziksel aktivite, beslenme alışkanlıkları gibi bir dizi sağlık parametresini ölçebilir. Ancak, bu değerli sağlık verilerinin doğru şekilde korunması ve çalışan gizliliğinin sağlanması büyük bir hassasiyet gerektirir.

İşletmeler, sağlık verilerini korumak için katı veri gizliliği politikaları oluşturmalıdır. Bu politikalar, hangi verilerin toplanabileceğini, nasıl saklanacağını ve kimlerin erişimine izin verileceğini açıkça belirtmelidir. Ayrıca, işletmeler, bu politikaları oluştururken yerel ve ulusal düzeydeki sağlık verileri saklama ve paylaşma yönetmeliklerine uygun hareket etmelidir. Sağlık verilerinin yasa ve yönetmeliklere uygun bir şekilde işlenmesi hem çalışanların güvenliğini hem de işletmelerin yasal uyumunu sağlar.

Sağlık verileri güçlü bir şekilde şifrelenmeli ve güvenli depolama çözümleri kullanılarak saklanmalıdır. Verilerin şifrelenmesi, yetkisiz erişimi engellerken, güvenli depolama çözümleri ise verilerin fiziksel ve dijital tehditlere karşı korunmasını sağlar. Bulut tabanlı güvenli depolama sistemleri, verilere her zaman güvenli bir şekilde erişim sağlar ve aynı zamanda veri kaybını önler.

Sağlık verilerine yalnızca yetkili kişilerin erişim sağlayabilmesi için güçlü yetkili erişim kontrolleri uygulanmalıdır. Kim hangi verilere erişebilir ve ne tür işlemler gerçekleştirebilir gibi parametreler belirlenmeli ve izleme sistemleri ile sürekli olarak denetlenmelidir. Bu izleme sistemleri, verilere yapılan erişimleri kayıt altına alır ve olası güvenlik ihlallerini hızlı bir şekilde tespit etmeyi sağlar.

Çalışanlar, sağlık verilerinin hassasiyeti konusunda bilinçlendirilmeli ve eğitilmelidir. Sağlık verilerinin doğru şekilde saklanması, paylaşılması ve erişimi konusunda çalışanlara rehberlik eden

eğitim programları düzenlenmelidir. Ayrıca, sosyal mühendislik saldırılarına karşı dikkatli olma, güçlü şifreler oluşturma ve şüpheli aktiviteleri rapor etme gibi konular da vurgulanmalıdır.

Dijital sağlık takip sistemlerinin veri güvenliği hem çalışanların sağlığını korumak hem de güvenli ve etik bir çalışma ortamı oluşturmak açısından kritik öneme sahiptir. Bu nedenle, işletmelerin bu sistemleri kullanırken en güncel güvenlik protokollerine uymaları ve çalışanlarını bu verilerin güvenliği konusunda bilinçlendirmeleri sağlamak için sürekli çaba göstermeleri gerekmektedir.

İşletmeler, dijital sağlık takip sistemlerini düzenli olarak değerlendirmeli ve denetlemelidir. Bu değerlendirmeler, sistemin güvenliğini, potansiyel açıkları ve zayıf noktaları belirleme açısından kritik öneme sahiptir. Güvenlik açıkları tespit edildiğinde, hızlı bir şekilde müdahale edilmeli ve gerekli güvenlik önlemleri alınmalıdır. Bu değerlendirmeler, sistemlerin sürekli olarak güncel ve güvenli kalmasını sağlar.

Eğer işletme dış kaynak kullanımına gitmişse ve dijital sağlık takip sistemlerini üçüncü taraf hizmet sağlayıcılardan temin ediyorsa, bu hizmet sağlayıcıların güvenilirliği dikkatlice değerlendirilmelidir. Sözleşmelerde sağlık verilerinin güvenliği ve gizliliği konusunda net hükümler bulunmalıdır. Hizmet sağlayıcılar, sağlık verilerini korumak için en güncel güvenlik standartlarına uymalı ve düzenli olarak denetlenmelidir.

Eğer bir güvenlik ihlali meydana gelirse, işletmeler hızlı ve etkili bir olay yanıtı planına sahip olmalıdır. Bu planlar, olayın tespit edilmesi, müdahale edilmesi, etkilerinin değerlendirilmesi ve gerekirse ilgili mercilere bildirilmesi gibi adımları içermelidir. Kriz yönetimi ekipleri, olayın yönetimi ve müşterilere doğru bilgi verme süreçlerini yönetir. Hızlı ve profesyonel bir şekilde hareket edilmesi, olayın etkilerini minimize eder.

Sonuç olarak, dijital sağlık takip sistemlerinin sağlık verilerinin güvenliği konusundaki hassasiyeti büyük bir öneme sahiptir. İşletmeler, bu sistemleri kullanırken güvenliğe odaklanmalı, sürekli olarak güncel güvenlik protokollerini takip etmeli ve çalışanları bu konuda eğitmeye devam etmelidir. Sağlık verilerinin doğru şekilde korunması hem işletme hem de çalışanlar açısından güvenli ve sağlıklı bir çalışma ortamını destekler.

3. Dijital Çağda Güvenlik ve Sağlık: Etik ve Yasal Sorumluluklar

3.1. Dijital Etik ve Çalışan Hakları:

Dijital çağda, teknolojinin hızlı ilerlemesiyle birlikte çalışanların dijital hakları ve mahremiyeti daha önce hiç olmadığı kadar kritik bir öneme sahip hale gelmiştir. Şirketler, çalışanların kişisel verilerini korumak ve mahremiyetlerini sağlamak için katı etik standartlara uymak zorundadır. Bu, çalışanların dijital ortamda güvenliğini ve gizliliğini sağlamak için şirket içinde oluşturulan politika ve uygulamaları içerir.

Şeffaflık ve Rıza Alınması: Çalışanlardan kişisel verilerin toplanması konusunda şeffaflık önemlidir. İşverenler, hangi verilerin toplandığını ve ne amaçla kullanılacağını açıkça belirtmelidir. Ayrıca, çalışanlardan bu verilerin toplanması için açık rıza alınmalıdır.

Veri Erişim Sınırlamaları: Şirket içinde, kişisel verilere sadece belirli yetkilendirilmiş personelin erişebileceği net bir şekilde belirlenmelidir. Bu, veriye yetkisiz erişimleri sınırlayarak verilerin güvenliğini sağlamak için önemlidir.

Adaletli Kullanım: Toplanan veriler, yalnızca belirli ve adil amaçlar için kullanılmalıdır. Örneğin, sağlık verileri sadece sağlık sigortası veya sağlık hizmetlerini yönetme gibi belirli alanlarda kullanılmalıdır. Verilerin amacı dışında kullanılması etik dışıdır ve çalışanların güvenini sarsabilir.

Dijital Saygı ve İnternet Etiketi: Çalışanların dijital platformlarda saygı görmesi ve mahremiyet haklarının korunması işverenlerin sorumluluğundadır. Şirket içindeki eğitim programları, dijital etik kurallarını içermeli ve çalışanları sanal dünyada saygılı ve etik bir şekilde davranmaya teşvik etmelidir. Modern uygulamaların çalışan iş -yaşam dengesini gözetme hususundaki özverisi dijital saygı ile ilintilidir (Allen vd., 2020).

3.2.Dijital Çağda Yasal Sorumluluklar:

Dijital güvenlik ve sağlık konularında işletmeler, mevcut yasal düzenlemelere tam uyum sağlamakla yükümlüdür. Yasalar ve yönetmelikler, çalışanların kişisel verilerinin korunması, çevrimiçi güvenlik standartları ve sağlık verilerinin saklanması gibi konularda işletmelerin uyması gereken belirli kuralları içerir.

Genel Veri Koruma Yönetmeliği gibi uluslararası yasalar, kişisel verilerin nasıl toplanacağını, saklanacağını ve işleneceğini belirler. Bu yasalara uyum sağlamak, çalışanların mahremiyetini korumanın yanı sıra işletmelerin de yasal yükümlülüklerini yerine getirmesini sağlar.

Payment Card Industry Data Security Standard (PCI DSS) gibi standartlar, çevrimiçi ödeme işlemlerinde güvenliği sağlamak için belirli kurallar ve protokoller sunar. İşletmeler, müşterilerinin finansal verilerini güvenli bir şekilde korumak için bu standartlara uygun hareket etmelidir.

Sağlık verileri özellikle hassas bir doğaya sahiptir. Bu verilerin saklanması ve paylaşılması konusunda sağlık sektöründe ve diğer endüstrilerde geçerli olan yasal düzenlemelere tam uyum sağlanmalıdır. Bu durum hem çalışanların sağlığına saygı göstermek hem de yasal sorumlulukları yerine getirmek açısından önemlidir. Dolayısıyla, işletmelerin dijital çağda güvenlik ve sağlık konularında etik ve yasal sorumluluklarına tam uyum sağlaması, çalışanların haklarını korumanın ve güvenli bir çalışma ortamı oluşturmanın temel taşıdır. Uygulanan etik standartlar ve yasal uyum, hem çalışanların güvenini sağlayarak moral ve motivasyonlarını artırır hem de işletmenin itibarını korur. İşletmelerin bu konuda başarılı olması için şu adımları atmaları önemlidir:

Hukuki Danışmanlık: İşletmeler, dijital güvenlik ve sağlık konularında uzmanlaşmış hukuk danışmanlarından destek almalıdır. Bu profesyoneller, güncel yasal düzenlemeleri takip ederek işletmeye uygun önlemleri almayı sağlar.

Personel Eğitimi: Çalışanlara, dijital güvenlik ve mahremiyet konularında düzenli eğitimler verilmelidir. Bu eğitimler, güçlü şifre kullanımından sosyal mühendislik saldırılarına kadar geniş bir yelpazeyi kapsamalıdır.

Veri Güvenliği Politikaları: İşletmeler, net ve anlaşılır veri güvenliği politikaları oluşturmalıdır. Bu politikalar, hangi verilerin nasıl kullanılacağını, kimlerin erişim sağlayabileceğini ve güvenlik önlemlerini içermelidir.

Güvenli Altyapı: İşletmeler, güvenli ağ yapıları ve güvenlik yazılımları kullanarak dijital altyapılarını korumalıdır. Güvenlik yazılımları, zararlı yazılımları tespit edebilir ve engelleyebilir.

Kriz Yönetimi Planları: İşletmeler, olası güvenlik ihlallerine karşı hazır olmak adına kriz yönetimi planları oluşturmalıdır. Bu planlar, olayın tespitinden başlayarak müdahale, iletişim ve krizin yönetimine kadar tüm aşamaları içermelidir.

İç Denetimler: Düzenli iç denetimler, işletmenin dijital güvenlik önlemlerinin etkinliğini değerlendirmek için önemlidir. Bu denetimler, var olan politika ve prosedürlerin uygun şekilde uygulanıp uygulanmadığını gösterir.

Sürekli İyileştirme: Teknoloji ve tehditler sürekli olarak evrildiğinden işletmeler güvenlik önlemlerini sürekli olarak gözden geçirmeli ve iyileştirmelidir. Bu iyileştirmeler, yeni tehditlere ve güvenlik zafiyetlerine karşı daha hazır olmayı sağlar.

Dijital çağda güvenlik ve sağlık, işletmeler için stratejik bir öneme sahiptir. Bu konuda başarılı olmak için etik ve yasal sorumluluklarına tam uyum sağlayan işletmeler, hem çalışanlarına güvenli bir çalışma ortamı sunar hem de rekabet avantajı elde eder. Bu nedenle, işletmelerin dijital güvenlik ve sağlık konularında sürekli olarak bilgi sahibi olmaları, güvenlik önlemlerini güncel tutmaları ve çalışanlarını bu konuda eğitmeleri kritik öneme sahiptir. Bu şekilde hem işletme hem de çalışanlar için sağlıklı, güvenli ve etik bir dijital çalışma ortamı oluşturulabilir.

4.Dijital Çağın Gölgesinde İş Sağlığı ve Güvenliği

Dijital çağ, teknolojik ilerlemelerin hızla arttığı bir dönemi temsil ettiğinden bu dönem, iş dünyasını büyük ölçüde dönüştürmüş ve çalışma hayatında iş süreçlerini dijitalleştirmiştir. Bilgisayarlar, internet, yapay zekâ, robotlar ve diğer teknolojiler, iş yerlerinde daha etkin ve verimli çalışmayı mümkün kılmaktadır. Ancak, bu teknolojik gelişmelerin iş sağlığı ve güvenliği üzerinde önemli etkileri

vardır. Teknolojik gelişmelerin iş sağlığı ve güvenliği üzerindeki etkilerine bakıldığında ilk akla gelen meseleler; ergonomik problemler, dijital yorgunluk, veri güvenliği, otomasyon ve robotlaşma olarak düşünülebilmektedir. İş yerlerinin ergonomik olarak tasarlanması ve çalışanlara ergonomik eğitim verilmesi, fiziksel sağlığı korumak için önemlidir. Ayarlanabilir masalar ve ergonomik ofis mobilyaları kullanmak, çalışanların daha iyi bir postürde çalışmasına yardımcı olabilir. Günümüz çalışma şartlarında bilgisayar kullanımı arttıkça, ergonomik sorunlar da artmaktadır. Yanlış pozisyonlarda oturma, klavye ve fare kullanımı, ekran parlaklığı gibi faktörler, çalışanların fiziksel sağlığını etkileyebilir. Uzun saatler boyunca bilgisayar başında çalışan kişilerde boyun ağrıları, sırt ağrıları ve karpal tünel sendromu gibi problemler yaygın hale gelmiştir. Sürekli bilgisayar ekranlarına veya diğer dijital cihazlara bakmak, göz yorgunluğuna neden olabilir. Ayrıca, sürekli olarak e-posta, mesajlar ve diğer dijital iletişim araçlarıyla iletişim kurmak, zihinsel yorgunluğa yol açabilir. Çalışanlara düzenli aralıklarla bilgisayar ekranlarından uzaklaşma molası verilmesi, göz yorgunluğunu azaltabilir. Aynı zamanda, dijital iletişim araçlarına olan sürekli bağlılığı azaltmak için işyeri politikaları oluşturulmalıdır. Dijital çağda işlerin büyük bir kısmı çevrimiçi olarak gerçekleştirildiği için, veri güvenliği ve gizliliği önemli bir sorundur. Bilgi sızıntıları, kötü niyetli yazılımlar ve siber saldırılar iş yerlerini tehlikeye atabilir. İşyerlerinde artan otomasyon ve robot kullanımı, işyerindeki fiziksel tehlikeleri azaltabilir ancak dijital tehlikeleri artırabilir. Örneğin, bir işyerinin veri tabanına yapılan bir saldırı, iş faaliyetlerini ciddi şekilde bozabilir. Çalışanlara siber güvenlik eğitimi verilmesi ve şirket içi gizlilik politikalarının düzenli olarak gözden geçirilmesi, veri güvenliği ve gizliliğini korumak için önemlidir. İş yerlerinin siber güvenlik önlemlerini sürekli olarak güncellemesi ve güvenlik açıklarını kapatması gerekmektedir. Ayrıca, kriz durumlarına karşı hazırlıklı olmak ve siber saldırıların etkilerini azaltmak için planlar oluşturulmalıdır.

Dijital çağ, çalışma şekillerini dönüştürmüş ve birçok avantajlar sunmuştur, ancak dijitalleşme ile birlikte aynı zamanda iş sağlığı ve güvenliği konularında yeni sorunlar ortaya çıkarmıştır. İş yerlerinin, çalışanların fiziksel ve zihinsel sağlığını korumak ve dijital tehlikelere karşı savunma mekanizmalarını güçlendirmek için önlemler almaları gerekmektedir (Kahraman ve Yürüten Özdemir,2022). Bu, dijital çağın iş dünyasında başarıyla uygulanabilmesi için kritik bir adımdır. Geleneksel iş sağlığı ve güvenliği uygulamaları, dijital çağın gereksinimlerine uyum sağlamakta zorlanabilir. Dijitalleşme ile birlikte, yeni teknolojilerin kullanımı işyerlerinde yeni tehlikelerin ortaya çıkmasına neden olabilir. Örneğin, artan robot kullanımı işçiler için fiziksel tehlikeleri artırabilir. Dijitalleşme, sürekli bağlantı ve bilgi bombardımanı gibi nedenlerle çalışanların zihinsel sağlığını olumsuz etkileyebilir. Dijitalleşme, işyerlerinde daha fazla veri kullanımını beraberinde getirir. Bu da veri güvenliği ve gizliliği endişelerini artırmaktadır. Çalışanları dijital tehlikeler konusunda eğitmek ve farkındalıklarını artırmak, iş sağlığı ve güvenliği açısından temel bir öneme sahiptir. Şirketler, düzenli eğitim programları düzenleyerek çalışanları bu konuda bilinçlendirebilir. İş sağlığı ve güvenliği için yeni teknolojilerin kullanımı, tehditleri belirlemek ve önlemek adına etkili bir yol olabilir. Örneğin, giyilebilir teknolojilerle çalışanların sağlık verileri izlenebilir ve tehlikeli durumlar tespit edilebilir.

Hükümetler ve endüstri kuruluşları, dijitalleşmeyle ilgili iş sağlığı ve güvenliği standartlarını belirleyerek, şirketleri uygun tedbirler almaya teşvik edebilir. Dijital çağ, iş dünyasını daha verimli hale getirirken, iş sağlığı ve güvenliği alanında yeni zorluklar yaratmaktadır. Bu zorluklarla başa çıkmak için eğitim, teknolojik çözümler ve uygun yasal düzenlemeler önemli rol oynamaktadır. İş dünyası, çalışanların sağlığını ve güvenliğini korumak için dijitalleşmenin getirdiği bu yeni zorlukları anlamalı ve uygun önlemleri almalıdır.

4.1. Dijital Çağda Ergonomik Problemler ve İSG

Uzaktan çalışma modeli, çalışma hayatında yeni ve önemli bir dönüşümü temsil etmektedir, uzaktan çalışmanın getirileri hem iş verenlerce hem de çalışanlarca memnuniyetle karşılandığından kendisine talep oldukça fazladır; ancak uzaktan çalışmanın çalışanların ergonomik sağlığı açısından önemli sorunlar doğurduğu gün geçtikçe daha çok ortaya çıkmaktadır. Uzaktan çalışma koşullarında, çalışanların uygun bir çalışma ortamına sahip olması, doğru pozisyon alma, ekran ve klavye düzeni gibi ergonomik faktörlere dikkat etmeleri gerekmektedir. Bu durum, çalışanların fiziksel sağlığını doğrudan etkileyebilir; kas-iskelet rahatsızlıkları, bel ağrıları, göz yorgunluğu gibi sorunlar uzaktan çalışanlarda daha sık görülebilir. Uzaktan çalışma, modern iş dünyasında yaygınlaşan bir uygulamadır. Ancak,

uzaktan çalışmanın ergonomik faktörlerinin göz ardı edilmesi, çalışanların fiziksel ve zihinsel sağlığını olumsuz etkileyebilir. Uzaktan çalışmanın ergonomik etkileri, yanlış oturma pozisyonları, bilgisayar kullanımı ve göz yorgunluğu gibi sorunlara yol açabilir. Uzun süreli uzaktan çalışma, kas-iskelet sistemi rahatsızlıkları ve stres gibi sağlık sorunlarına neden olabilir. Uzaktan çalışanlara ergonomik eğitimler düzenleyerek doğru oturma pozisyonları ve bilgisayar kullanımı konusunda bilinçlendirme yapılmalıdır. Ayarlanabilir masalar gibi ergonomik ofis mobilyaları kullanarak çalışma ortamları iyileştirilmelidir. Düzenli mola süreleri ve bilgisayar ekranlarından uzaklaşma araları çalışanların göz yorgunluğunu azaltabilir. Dijital çağın hediyelerinden bir olan uzaktan çalışma, sadece fiziksel-ergonomik sorunları değil mahremiyet, ağır iş yükü, mesai saati karmaşası ve ev-iş hayatı dengesini kuramama gibi psikososyal problemleri de beraberinde getirmiştir. Bu problemler çalışan için önlenmesi gereken risk faktörleridir. Uzaktan çalıştığı için her an ulaşılabilir olması gerektiği düşüncesine kapılan çalışan bir süre sonra ev hayatı-iş hayatı dengesini kurmakta zorluk yaşamakta ve işyerinde bulunduğundan daha fazla bir süre teknolojik cihazlara bağlı olarak iş görmektedir. Bu durum ise psikososyal bir risk haline gelmekte ve çalışanı olası iş kazaları / meslek hastalıkları adına tehdit etmektedir. Dijital çağın bu problemlerini önleme adına uzaktan çalışanlar için kanun koyucunun yeni düzenlemeler getirmesi elzem görünmektedir.

4.2. Dijital Çağda Veri Analitiği ve İSG

İş sağlığı ve güvenliği verilerinin analizi, gelecekteki kazaları öngörmek ve iş güvenliği önlemlerini geliştirmek için hayati öneme sahiptir. İş sağlığı ve güvenliği verileri, büyük veri analizi, makine öğrenimi ve istatistiksel modeller gibi teknikler kullanılarak derinlemesine incelenebilir. Bu analizler, işyerlerindeki risk faktörlerini belirleme, güvenlik politikalarını iyileştirme ve iş kazalarını tahmin etme konularında değerli bilgiler sunar. İş sağlığı ve güvenliği verilerinin analizinde kullanılan metodolojiler, bu analizlerin iş sağlığı ve güvenliği yönetimindeki rolü ve gelecekteki potansiyel uygulamaları dijital çağda önemi artan konulardandır.

İş sağlığı ve güvenliği verilerinin doğru analiz edilmesi, iş yerlerindeki güvenlik politikalarının geliştirilmesi ve güvenlik standartlarının yükseltilmesi açısından da kritiktir. İş sağlığı ve güvenliği veri analizi, iş yerlerindeki riskleri belirlemeye ve iş kazalarını önlemeye yardımcı olabilir. Ayrıca, doğru analizlerle iş güvenliği politikaları daha etkili bir şekilde oluşturulabilir. Büyük veri analizi, makine öğrenimi ve istatistiksel modeller gibi tekniklerle veriler analiz edilmelidir. Söz konusu verileri segmentlere ayrılarak, risk faktörleri daha net bir şekilde belirlenebilir ve buna göre önlemler alınabilir. İlgili verilerle gerçekleştirilen analizler düzenli olarak tekrar edilmeli ve sonuçlar güvenlik politikalarının geliştirilmesinde kullanılmalıdır.

4.3. Dijital Çağda Yapay Zekâ ve İSG Otomasyonu

Yapay zekâ ve otomasyon teknolojileri, iş sağlığı ve güvenliği alanında çığır açıcı potansiyele sahiptir. Yapay zekâ, veri analizi, risk değerlendirmesi ve güvenlik tahminleri gibi alanlarda kullanılarak iş kazalarını önleme süreçlerini optimize edebilmektedir. Bu teknolojiler aynı zamanda tehlikeli durumları tespit ederek anında müdahale imkânı da sunmaktadır. Yapay zekânın iş sağlığı ve güvenliği alanındaki uygulamaları, mevcut endüstriyel uygulamalar ve gelecekteki olası gelişmeler analiz edildiğinde bu süreçlerin iş sağlığı ve güvenliği yönetimindeki etkileri rahatlıkla gözlemlenebilecektir.

Yapay zekâ ve otomasyon teknolojileri, her alanda olduğu gibi iş sağlığı ve güvenliği alanında da önemli yenilikler getirebilir. Ancak, bu teknolojilerin etkili bir şekilde kullanılabilmesi için doğru stratejiler ve uygulamalar geliştirilmelidir. Yapay zekâ tabanlı risk değerlendirmesi, otomatik tehlike tespiti ve anında müdahale sistemleri gibi uygulamalar, iş yerlerindeki güvenlik standartlarını artırabilir. Bununla birlikte, yanlış kullanım veya eksik uygulamalar riskleri de beraberinde getirebilir. Yapay zekâ tabanlı güvenlik uygulamaları, uzmanlar tarafından tasarlanmalı ve doğru şekilde eğitilmelidir. İş sağlığı ve güvenliği otomasyonu için endüstriyel uygulamalar geliştirilirken, iş yerlerindeki spesifik ihtiyaçlar dikkate alınmalıdır. Sürekli güncellenen yapay zekâ algoritmaları, iş yerlerindeki güvenlik önlemlerini sürekli olarak iyileştirmek için kullanılmalıdır.

4.4. Dijital Çağda Veri Gizliliği ve İSG

İş sağlığı ve güvenliği verileri, çalışanların mahremiyeti ve şirketin güvenliği açısından son derece hassas bilgiler içermektedir. Bu verilerin doğru şekilde toplanması, saklanması, işlenmesi ve paylaşılması gerekmektedir. Veri gizliliğini sağlamak için kriptografi, anonimleştirme ve güvenli veri paylaşımı gibi teknikler kullanılabilir. İş sağlığı ve güvenliği verilerinin gizliliğiyle ilgili karşılaşılan zorluklar, bu zorlukların nasıl aşılabileceği, veri gizliliği politikalarının oluşturulması ve uygulanması gibi konular ele alınarak, elde edilen bu verilerinin güvenliğinin sağlanması için gereken adımlar detaylı bir şekilde çalışma hayatında tartışılmalıdır.

İş sağlığı ve güvenliği verileri hassas bilgiler içerdiği için, bu verilerin doğru şekilde saklanması ve paylaşılması, ancak iş yerlerinde veri gizliliği politikalarının doğru bir şekilde oluşturulmasıyla mümkündür. Veri güvenliği önlemlerinin eksik veya yanlış uygulanması durumunda, iş sağlığı ve güvenliği verileri sızdırılabilir ve kötü niyetli kullanıma açılabilir. Bu da hem çalışanların güvenliğini hem de şirketin itibarını tehlikeye atar. Kriptografi ve anonimleştirme gibi güvenlik teknikleriyle iş sağlığı ve güvenliği verileri korunmalıdır. Veri paylaşımı ve erişimiyle ilgili sıkı düzenlemeler oluşturularak, yetkisiz erişimler engellenmelidir. İş sağlığı ve güvenliği verilerinin korunumu ve paylaşılma süreçleri ilgili olarak çalışanlara düzenli eğitimler verilerek, çalışanların veri gizliliği konusunda farkındalıkları artırılmalıdır.

4.5. Dijital Çağda Giyilebilir Teknoloji ve İSG

Giyilebilir teknolojiler, son yıllarda hızla gelişen ve çeşitlenen bir alan olarak dikkat çekmektedir. Bu teknolojiler, kullanıcıların üzerine takılan veya giyilebilen cihazlar aracılığıyla veri toplama, analiz etme ve iletişim kurma yeteneğine sahiptir (Ada & Aksoy, 2020). Giyilebilir teknolojilerin iş güvenliği alanında taşıdığı potansiyeli ve bu teknolojilerin işyerlerindeki risklerin erken tespiti, çalışan güvenliğinin artırılması ve verimliliğin iyileştirilmesi gibi faktörlere büyük oranda katkı sağlayabileceği düşünülmektedir (Bozkurt, 2018). Giyilebilir teknolojilerin iş güvenliği açısından en önemli rollerinden biri, işyerlerindeki risklerin erken tespit edilmesidir. Giyilebilir cihazlar, üzerlerinde bulunan sensörler, kameralar, giyilebilir ekranlar ve akıllı cihazlar sayesinde çeşitli verileri toplarlar. Bu veriler, işyerindeki tehlikeli maddelerin varlığını algılamak, çalışanların vücut sıcaklığını izlemek, yorgunluk ve stres düzeylerini değerlendirmek gibi iş güvenliği açısından önemli bilgiler sunar (Çulhağil Kır & Yıldırım, 2023). Giyilebilir teknolojiler ayrıca, çalışanların kişisel koruyucu ekipmanlarını takip etme ve doğru şekilde kullanma konusunda da yardımcı olabilir. Bir giyilebilir cihaz, çalışanın koruyucu ekipmanlarını takip edebilir ve uygun şekilde kullanılıp kullanılmadığını kontrol edebilir. Bu durum, çalışanların yanlış kullanımı nedeniyle oluşabilecek riskleri azaltabilir ve güvenlik çalışma ortamı oluşturma konusunda yardımcı olabilir (Çiftçi & Tüysüz, 2021). Giyilebilir teknolojilerin iş güvenliği açısından taşıdığı bir diğer potansiyel de verimliliği artırma yeteneğidir. Örneğin, giyilebilir ekranlar aracılığıyla çalışanlar, talimatları doğrudan görebilir ve işlerini yerine getirebilirler. Bu süreç çalışanların daha hızlı ve daha verimli bir şekilde çalışmalarına olanak tanır. Ayrıca, giyilebilir cihazlar aracılığıyla çalışanların hareketleri ve aktiviteleri izlenir, böylece iş süreçlerinin analizi yapılabilir ve iyileştirme fırsatları belirlenebilir (Gökçen & Bahadır Ünal, 2023).

Giyilebilir teknolojilerin yaygınlaşması beraberinde veri toplama, saklama ve paylaşma sorunlarını getirmektedir. Çünkü giyilebilir teknoloji sayesinde çalışanın anlık sağlık bilgilerine ulaşılması, bu bilgilerin üçüncü şahıslarla paylaşılması kişisel verilerin korunumu hususunda problem teşkil etmektedir. Daha fazla veri transferi ve daha fazla etkileşim, gizlilik ve güvenlik endişesini gündeme getirmekte çalışanın kişisel verilerinin korunması, izinsiz erişimlerin engellenmesi gibi konular gittikçe önem kazanmaktadır. Bu problemler çalışma hayatında önemli risk faktörleri olduğundan dijital çağda nasıl önlenmesi gerektiğine dair çalışmalar yapılması gereken parametrelerdir.

5. Dijital Çağda Önleme: Dijital Dönüşümün Zorlu Serüveni

Günümüz çalışma hayatında, dijital dönüşüm kavramı artık oldukça yaygın hale gelmiştir. İşletmeler, ana motivasyon kaynakları ayakta kalmak ve sürdürülebilir olabilmek olduğundan teknolojik gelişmelere uyum sağlayarak rekabet avantajı elde etmeyi ve sürekli büyümeyi hedeflemektedirler. İçinde yaşadığımız bilgi toplumunda rekabet içerisindeki kurumlar hedef kitlelerinin değişen taleplerini

karşlamak için dijital dönüşüme evrilmişlerdir (Öztürk ve Zeybek, 2021). Ancak dijital dönüşümün başarıyla sürdürülebilmesi için kat edilmesi gereken zorlu bir yolculuk serüveni olduğu düşünülmektedir. Dijital dönüşüm, işletmelerin geleneksel iş süreçlerini ve operasyonlarını dijital teknolojilere dayalı, veri odaklı bir yaklaşımla yeniden şekillendirmeyi içerir. Ancak bu yolculuk, bir dizi zorlukla doludur. Bunlardan ilki direnç ve kültürel değişim olarak düşünülebilir. İnsanların alışkanlıklarını değiştirmek ve yeni teknolojilere uyum sağlamalarını teşvik etmek, kurumsal kültürde derin değişiklikler gerektirir. Direnç, bu konuda en büyük engel olabilir ve işletmelerin bu kültürel dönüşümü yönetmeleri gerekecektir. Güvenlik kültürünü oluşturma adına dijital dönüşüm için yapılan veya yapılması planlanan tüm değişimlerde farklı büyüklüklerde dirençle karşılaşılması olağandır. Çünkü çalışanların konfor alanlarından çıkmalarını sağlamak oldukça zor ve zahmetli bir süreçtir. Dijital dönüşüm, genellikle büyük yatırım gerektirir. Hem teknoloji altyapısının hem de personel eğitiminin finanse edilmesi zorlayıcı olabilir. Bu durum, işletmelerin kısa vadeli maliyetlerle başa çıkmalarını gerektirir. Yatırım ve maliyet problemleri dijital dönüşüm yolunda karşılaşılabilecek bir başka risk faktörüdür. Dijital dönüşüm, büyük miktarda verinin toplanmasını ve analiz edilmesini gerektirir. Veri güvenliği, gizliliği ve uyumluluk konularında ciddi endişeler olabilir. İşletmeler, verilerini etkili bir şekilde yönetmek ve korumak zorundadır. Teknolojik gelişmeler hızla ilerlediği için, işletmelerin bu hızla başa çıkabilme yeteneği önemli bir husustur. Donanım ve yazılım güncellemeleri, sürekli olarak takip edilmesi gereken konulardır. Rekabet Baskısı bir diğer risk faktörüdür. Dijital dönüşümü tamamlayamayan işletmeler, rekabetin gerisinde kalabilirler. Diğer işletmeler hızla yeni teknolojilere ve dijital süreçlere geçiş yaparken, rekabetçi bir avantaj elde etmek zorlaşabilir. Dijital dönüşüm, iş süreçlerini temelden yeniden düşünmeyi gerektirmektedir. İş süreçlerinin yeniden tasarımı zaman alıcı ve zor bir süreç olabilir. İşletmelerin mevcut süreçleri gözden geçirip optimize etmeleri gerekecektir. Bu da yoğun planlama, koordineli çalışma, uygulamalar yapma ve sürekli kontrol gerektiğinden geçiş süreci zorlu olabilmektedir. Dijital dönüşüm, bir sonraki teknoloji trendini takip etmeyi ve sürekli öğrenmeyi gerektirir. İşletmelerin personeli sürekli olarak eğitilmeli ve güncel kalmalıdır. Sürekli öğrenme ve gelişme dijital çağda en önemli gereksinimlerden biridir. Dijital dönüşümün zorlu yolculuğu, işletmelerin gelecekte başarılı olmaları için atlamaları gereken engellerle dolu bir maraton gibidir. Ancak bu zorluklar, doğru strateji ve yönetimle aşılabilecek engellerdir. İşletmeler, dijital dönüşümü bir fırsat olarak görmeli ve bu yolculuğa kararlılıkla devam etmelidirler. Dijital dönüşümü başarıyla tamamlayan işletmeler, rekabetçi bir avantaj elde ederken, geleceğe daha hazır bir şekilde ilerlerler. Böylece hem çalışanlar hem işletmeler adına sürdürülebilir bir çalışma ekosistemi oluşturulmuş olur. Oluşturulan bu sürdürülebilir çalışma ekosisteminde şüphesiz dikkat edilmesi gereken en önemli husus önleme politikalarıdır. Önleme politikaları sayesinde sağlıklı ve güvenli çalışma şartları yerine getirilebilecektir.

6.Sonuç ve Öneriler

İş sağlığı ve güvenliği, sahip olduğu multidisipliner yapısıyla çalışma ortamlarında çalışanların fiziksel, sosyal ve ruhsal sağlığını koruma ve iş kazalarını önleme amacıyla uygulanan bir dizi önlemleri içermektedir. Dijital teknolojiler, iş sağlığı ve güvenliği uygulamalarını desteklemek ve geliştirmek için güçlü bir araç haline gelmiştir. Dijital sensörler ve izleme cihazları, çalışanların güvenliğini ve sağlığını izlemek için kullanılan önemli yardımcı bileşenlerdir. Bu cihazlar, tehlikeli koşulları tespit edebilir, çalışanların konumunu izleyebilir ve tehlikeli alanlara girişlerini kontrol edebilir. Dijital platformlar, iş sağlığı ve güvenliği eğitimleri ve bilinçlendirmeler için etkili araçlar sunabilir. Eğitim videoları, simülasyonlar ve interaktif eğitim materyalleri, çalışanlara işyerindeki riskleri ve güvenlik protokollerini anlama konusunda yardımcı olabilir. Dijital teknolojiler, işyerindeki verileri analiz etmek ve potansiyel tehlikeleri öngörmek için kullanılabilir. Veri analitiği, işyerindeki eğilimleri ve riskleri belirlemek için değerli bilgiler sunar. Ayrıca, öngörücü bakım uygulamaları, ekipman arızalarını önceden tahmin ederek beklenmedik durumları önleyebilir. Dijital iletişim araçları, acil durumların yönetilmesi ve iletilmesi için hayati öneme sahiptir. Anında bildirimler, SMS, e-posta ve diğer iletişim kanalları, acil durumlar sırasında çalışanların hızla bilgilendirilmesine yardımcı olabilir. Dijital teknolojiler, çalışanların sağlık sorunlarını izlemek ve tele tıp yoluyla uzaktan sağlık hizmetleri sunmak için kullanılabilir. Ayrıca, işyeri güvenliği uzmanlarının uzaktan iş güvenliği danışmanlığı sağlamalarına olanak tanır. Dijital

işaretler ve yönlendirme sistemleri, çalışanları tehlikeli alanlardan uzak tutabilir ve güvenli çıkış yollarını belirlemelerine yardımcı olabilir. Bu durum, acil durumlar sırasında hızlı bir şekilde yönlendirme yapılmasına olanak tanır.

Çalışma hayatı, teknolojik ve sosyal değişimlerle hızlı bir evrim geçirmekte ve bu değişimlerin anlaşılması çalışanların esenliği ve psikososyal risklerin efektif şekilde yönetilmesi bağlamında kritik önem arz etmektedir (Şen, 2024). Çalışma hayatında gün geçtikçe daha fazla yer bulan dijital önlemler, iş sağlığı ve güvenliği açısından önemli bir rol oynamaktadır. Çünkü söz konusu önlemler temelde korunma politikalarını oluşturmakta ve güvenlik kültürünü yaygınlaştırma adına faaliyetlerde bulunmaktadır. Ancak, bu teknolojilerin etkili bir şekilde kullanılabilmesi için işletmelerin uygun altyapıyı oluşturması, çalışanları eğitmesi ve sürekli iyileştirme çabalarına odaklanması gerekmektedir. İş sağlığı ve güvenliği alanında dijital teknolojilerin kullanılması, çalışanların sağlığını ve güvenliğini koruma konusunda gerekli ve önemli bir adımdır. Bu süreçlerde göz ardı edilmemesi gereken riskler ise etik yaklaşımlar, dijital bağımlılık, dijital eşitlik, veri gizliliği, dijitalleşmenin getireceği psikososyal problemler ve doğru teknolojinin doğru alanda efektif kullanımınıdır.

Sonuç olarak dijital önlemler, çalışma ortamlarındaki riskleri azaltmaya yönelik girişimlerde bulunurken ve çalışma ortamlarının daha güvenli ve sağlıklı hale getirilmesine önemli katkılar sağlarken bu önlemlerin başarıyla uygulanabilmesi için işletmelerin stratejik bir yaklaşımla hareket etmesi gerekliliği önem kazanmaktadır. Dijitalleşmeye uygun bir altyapı oluşturulması ve önleme politikalarının hayata geçirilmesi gerekmektedir. Ancak bu sayede, iş sağlığı ve güvenliği standartlarının yükseltilmesi, çalışanların güvende olması, sağlıklı ve güvenli çalışma şartlarının yerine getirilebilmesinin sağlanabileceği düşünülmektedir.

Kaynaklar

- Ada, A., & Aksoy, R. (2020). Giyilebilir Teknolojik Ürünlerde Tüketicilerin Algıladıkları Risklerin Farklılaşması: Akıllı Saat Kullanıcılarına Dönük Bir Araştırma. *Herkes İçin Spor ve Rekreasyon Dergisi*, 2(1), 50-61.
- Allen, T. D., & Shockley, K. M. (2020). Flexibility in the New World of Work. *Current Directions in Psychological Science*, 29(4), 365-370.
- Bozkurt, A. (2018). Giyilebilir Teknolojilerin Eğitim Amacıyla Kullanımına Yönelik Kavramsal Bir Değerlendirme. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 4(4), 87-102.
- Çiftçi, A., & Tüysüz, M.F. (2021). Giyilebilir Teknolojiler için Ara yüz Tasarımı ile Aktivite Takibi. *Harran Üniversitesi Mühendislik Dergisi*, 6(2), 121-140. 67.
- Çulhagil Kır, Ö., & Yıldırım, F. (2023). Türkiye'de Giyilebilir Teknoloji Ürünleri Pazarı ve Kullanımına İlişkin Nitel Bir Araştırma. *İstanbul Ticaret Üniversitesi Girişimcilik Dergisi*, 7(13), 50-63.
- Ertaş, M. F. (2023). İş Güvenliği Uzmanlarının İş Yüklerinin İyileştirilmesi İçin Yönetimsel Strateji Önerileri. *İnsan Ve Toplum Bilimleri Araştırmaları Dergisi*, 12(2), 626-644. <https://doi.org/10.15869/itobiad.1247291>.
- Gökçen, Ö., & Bahadır, Ü. (2023). Yaşlılık ve Giyilebilir Teknolojiler. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 11(1), 89-98.
- Kahraman, Z., & Yürüten Özdemir, K. (2022). Dijitalleşmenin İş Sağlığı ve Güvenliğine Entegrasyonu ve Uygulanabilirliği. *OHS ACADEMY*, 5(3), 208-221. <https://doi.org/10.38213/ohsacademy.1128402>
- Öztürk, İ. D., Zeybek, B. (2021). Dijitalleşme ve Etik Sorunlar: Nesnelerin İnterneti Teknolojisini Gözetim, Gizlilik, Güvenlik Kapsamında Değerlendirme. *İletişim Kuram ve Araştırma Dergisi*, 2021(55),1-15. doi.org/10.47998/ikad.932173
- Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. NYU Press.
- Şen, S. (2024). Çalışma Yaşamında Esenlik ve Psikososyal Riskler: Değişen Dinamiklerle Başa Çıkma Stratejileri. *OHS ACADEMY*, 7(1), 54-63. <https://doi.org/10.38213/ohsacademy.1393212>
- Tepe, S., (2022). İşletmelerde Çalışan ve Lider Düzeyinde Risk Algısı ile Risk Yönetim İlkeleri, Güvenlik Kültürü ve Güvenlik İklimi, Nobel Yayını.

Tepe, S., (2023). Saęlık Kurumlarında Risk Yönetimi, Saęlık Sektöründe İş Saęlığı ve Güvenlięi, Akademisyen Yayınevi.