

— Kişisel Verileri Koruma Kurumu —

BÜLTEN

Ağustos - Kasım 2024 Sayı:6

**KİŞİSEL VERİLERİN KORUNMASI
VE SİBER GÜVENLİK**



Kişisel Verileri Koruma Kurumu
KVKK Bülten
www.kvkk.gov.tr
Sayı:6
Kişisel Verileri Koruma Kurumu
Adına İmtiyaz Sahibi
Prof. Dr. Faruk BİLİR

Yönetim Yeri
Nasuh Akar Mahallesi 1407. Sokak
No:4 Balgat Çankaya/ANKARA
Tel: [312] 216 50 00

© Bütün hakları, Kişisel Verileri Koruma Kurumu'na aittir. Kaynak gösterilmek kaydıyla, tanıtım amaçlı kısa alıntı dışında yayımcının yazılı izni olmadan hiçbir yolla çoğaltılamaz. Yayımlanan yazıların ve fotoğrafların sorumluluğu yazarlarına ve sanatçısına aittir.

Giriş 5

Röportaj 6

Siber Güvenlik Farkındalık Ayı 10

Siber Zorbalık Nedir? 14

Ulusal Siber Güvenlik Stratejisi ve Eylem
Planı 2024-2028 16

Genel Olarak Kişisel Veri Güvenliğine İlişkin Tedbirler 20

Avrupa Birliği'nin Siber Güvenlik Stratejisinde Dönüşüm:
NIS2 Direktifi 24

Öne Çıkan Gelişmeler 30

Bizden Haberler 48

21. yüzyıl ile birlikte ivme kazanan dijital dönüşüm, fırsatlarla birlikte bazı zorlukları da beraberinde getirmiştir. Bireysel ya da kurumsal bir aktör olarak dijital dönüşüm sürecinin getirdiği imkânlardan faydalanırken, buna yönelik ortaya çıkabilecek risk ve tehditlere karşı hazırlıklı olmak gerekmektedir.

Dijital dönüşümün temel bileşenlerinden biri kuşkusuz siber güvenlidir. Siber güvenlik, “*Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi*”¹ olarak tanımlanmaktadır.

Siber güvenlik, günümüzde bireyler, şirketler ve hatta devletler için hayati bir öneme sahip olduğundan, siber güvenliğe ilişkin farkındalığın artırılması ve buna yönelik çalışmalar yapılması ihtiyacı ile karşılaşılmaktadır.

Bilindiği üzere Ekim ayı, dünya genelinde siber güvenlik farkındalık ayı olarak kabul edilmektedir. Ülkemizde de 2024-2028 yıllarını kapsayan “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı” ile tayin edilen “İnsan Odaklı Siber Güvenlik Yaklaşımı” başlığı altında, “*Siber güvenlik zaafiyetlerinin yaklaşık %80’i insan unsurunun rol oynadığı ihmallerden kaynaklanmaktadır. Siber güvenlik riskleri ve olası tehditler ile maruz kalınabilecek siber olayların etkilerine ilişkin bilgi düzeylerinin ve farkındalık seviyelerinin artırılması, siber güvenliğin sağlanmasında kritik bir rol oynamaktadır.*” şeklinde ifadeler yer verilmiştir.

Siber güvenlik, kişisel veri güvenliğinin sağlanması bakımından da önemli unsurlardan biridir. Kişisel veriler, dijital ortamda çeşitli siber tehditlerin hedefi haline gelmektedir. Bu noktada siber güvenlik uygulamaları, kişisel verilerin güvenliğinin sağlanmasında ve kritik altyapıların korunmasında ciddi bir rol oynamaktadır. Ayrıca siber saldırılara yönelik, bireylerin sınırlı bilgileri olsa dahi ilk müdahaleyi yapabilecek düzeyde farkındalığa sahip olması, olumsuz sonuçların önüne geçilmesi veya azaltılması açısından büyük önem taşımaktadır.

Özetle siber güvenlik, günümüz dünyasının en önemli konularından biridir ve bilgi çağında siber güvenliğin önemi her geçen gün artmaktadır. Dijital ekosistemde mahremiyetin korunması için siber güvenlik ve kişisel veri güvenliği bir bütün olarak ele alınmalı, bireyler ve kurumlar bu konuda bilinçli hareket etmelidir. Bu hususta yeterli farkındalığa sahip olmak, sürdürülebilir bir dijital geleceğin anahtarı olacaktır.

1 Ulusal Siber Olaylara Müdahale Merkezi:“Siber Güvenliğe İlişkin Temel Bilgiler”, https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar.pdf.

SİBERAY İLE RÖPORTAJ



Güvenli internet kullanımı için kullanıcılara ve vatandaşlara yol gösteren, teknolojinin faydalı şekilde kullanılmasını sağlamaya yönelik çalışmalar yapan SİBERAY ile röportaj gerçekleştirerek SİBERAY Programı'nın amacını ve bu çerçevede yapılan çalışmaları sorduk...

1. Bize SİBERAY programından bahsedersiniz? Programın amacı nedir, program ne zamandır uygulanmaktadır, kimlere yöneliktir?

SİBERAY Programı, Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı bünyesinde siber suçun gerçekleşmeden önlenmesi, maddi-manevi mağduriyetlerin önüne geçilebilmesi amacıyla hayata geçirilen ve bünyesinde birçok proje barındıran kapsamlı bir kamusal bilinçlendirme faaliyetidir. Daire Başkanlığımız ve 81 İl Siber Suçlarla Mücadele Şube Müdürlüklerimiz görevlileri aracılığıyla yürütülmektedir.

Programın temel amacı toplumun siber farkındalığının en üst düzeye çıkarılmasıdır. Böylelikle; siber suç türleri ve yöntemleriyle ilgili bilinçlenen internet kullanıcılarının siber suça maruz kalmaları önlenmeye çalışılmaktadır.

2020 yılında hayata geçirilen SİBERAY Programı aracılığıyla başta çocuklar ve gençler olmak üzere farklı hedef kitlelere yönelik "güvenli ve bilinçli internet kullanımı, siber güvenlik, güncel siber risk ve tehditler, siber suç, siber zorbalık, yasa dışı bahisle mücadele, teknoloji bağımlılığı ve dijital okuryazarlık" konularında yazılı ve görsel içerikler geliştirilerek her yaşta internet kullanıcısı vatandaşımızın istifadesine sunmaktayız.

2. Güvenli ve bilinçli internet kullanımı nedir ve neden gereklidir?

İnternetin güvenli ve bilinçli kullanılmasıdır ki; teknolojinin gelişmesiyle beraber bankacılık işlemleri, alışveriş gibi önceleri yüz yüze ya da müşteri temsilcileri aracılığıyla yaptığımız birçok işlemi artık internet bağlantısı aracılığıyla bilişim sistemleri üzerinden çevrim içi olarak yapabilmekteyiz ve bu işlemler esnasında kişisel bilgilerimizi paylaşmaktayız. Güvenli ve bilinçli internet kullanımı da işte tam bu noktada ön plana çıkmakta, paylaştığımız kişisel bilgilerin gerektiği gibi korunması ihtiyacı önem arz etmektedir. Casus yazılımlar, kopya sunucular ve kimlik avı gibi birçok aldatıcı yöntemler kullanarak kişisel verilerimizi ele geçiren siber dolandırıcılar bilginiz ve rızamız dışında parasal işlemler

yapabilmekte ve çeşitli mağduriyetlere sebep olabilmektedirler. İşte bu yüzden internetin güvenli ve bilinçli kullanımı çok önemli. Olası risklerin ne olduğu, bu risklerden kaçınma yollarının ne olduğu ve bu risklere karşı alınabilecek basit ama etkili yöntemlerin ne olduğunun bilinmesi kullanıcıyı birçok tehlikeden koruyacaktır.

3. Ülkemizde gençlerin güvenli ve bilinçli internet kullanımı konusunda bilinç düzeyi nedir? Gençler hangi siber tehditlerle karşı karşıya kalabileceğinin ve bunun çözüm yollarının farkında mıdır? SİBERAY'ın buna yönelik bilinçlendirme çalışmalarını anlatabilir misiniz?

Teknoloji ve internetle tanışma yaşının her geçen gün düştüğü bir dönemde yaşamaktayız. We Are Social Şubat 2024 Türkiye verilerine göre 16-64 yaş arası bir bireyin internette harcadığı süre günde yaklaşık 7 saattir ve internet kullanıcısı ise 74.41 milyon kişidir. Böylesine yaygın bir kullanıma sahip küresel bir alanın kontrol altında tutulması ya da kullanıcıların güvenliğinin sağlanması yalnızca bir kurum ya da kuruluştan beklenemez, bu mümkün de değildir zaten. Dolayısıyla kullanıcıların bilinçlendirilmesi, kendi güvenliklerini kendilerinin sağlaması bir zorunluluktur. SİBERAY programı da bu zorunluluktan dolayı geliştirilmiş bir programdır. Karşılaşabileceği siber tehditlerin farkında olan gençler olduğu gibi olmayanlar da elbette vardır ve SİBERAY görevlileri olarak bizler bu alandaki eksikliği yurt çapında arttırarak sürdürdüğümüz farkındalık faaliyetleri aracılığıyla doldurmaya çalışmakta ve çözüm yollarını öğretmekteyiz.

Bunu yoğun bir şekilde gerçekleştirilen;

» Eğitim ve öğretim kurumları başta olmak üzere kurum/kuruluşlarda gerçekleştirdiğimiz eğitim seminerleri,

» Alışveriş merkezleri, fuar, festival ve etkinlik alanlarında stant faaliyetleri ve bil-kazan bilgi yarışmaları,

» Yasa dışı bahisle mücadele kapsamında üniversite öğrencilerine ve sporseverlere yönelik bilgilendirme faaliyetleri,

» www.siberay.com internet sitesi ve @SiberayEGM kullanıcı adıyla X, Instagram, Facebook, Youtube sosyal medya hesapları üzerinden yapılan bilgilendirici içerik paylaşımlar aracılığıyla gerçekleştirmekteyiz.

» Ayrıca Yüksek Hızlı Tren, Başkentray, Marmaray gibi toplu taşıma sistemleri dijital yolcu ekranlarında, EBA ve TRT Çocuk Ebeveyn Akademisi internet sitesinde uyarıcı ve bilgilendirici içeriklerimiz yayınlanmakta ve TRT Çocuk iş birliği ile hazırlanan "Ekip: SİBERAY" çizgi dizisi ve "Ekip: SİBERAY Güneş Fırtınası" çizgi filmi ile çocuklar için bilgilendirme faaliyetleri sağlamaktayız.

4. Özellikle gençler, internette ve sosyal medyada güvenliklerini sağlamak için bireysel olarak hangi önlemleri alabilir?

İnternette alınabilecek güvenlik önlemleri olarak, okuyucularımızın;

- Tüm hesaplarını tek bir parola ile yönetmemelerini,
- Tanınmayan kişilerden veya teyit edilemeyen kaynaklardan gelen e-posta veya eklerini açmamalarını,
- Güncel anti-virüs programı kullanmalarını,
- Bankacılık gibi şifre gerektiren işlemler için ortak kullanılan internet ağlarını kullanmamalarını,
- Yazılım güncellemelerini ihmal etmemelerini,

Sosyal medyada alınabilecek güvenlik önlemleri olarak;

- Parolalarını sık sık değiştirmelerini,
- İki faktörlü kimlik doğrulamasını muhakkak aktif etmelerini,
- Zaman zaman hesap giriş hareketlerini kontrol etmelerini,
- Fotoğraf etiketleme seçeneklerini düzenlenmelerini,
- Mesaj isteklerine karşı temkinli olmalarını tavsiye edebiliriz.

5. Son zamanlarda oldukça yaygın hale gelen siber zorbalıktan da bahseder misiniz? Siber zorbalık nedir? SİBERAY siber zorbalığa uğrayan vatandaşlara ne tavsiye etmektedir?

Bir kişinin, bir başka kişiyi kasıtlı ve düzenli olarak rahatsız etmesi, zarar verme amacını taşıyan eylemlerde bulunması, incitmesi ya da korkutması olarak tanımlanabilecek siber zorbalık, bugün özellikle sosyal medya mecralarında yoğun bir biçimde yaşanmaktadır. Dijital platformlar, dijital ortamlar ve sosyal medya mecraları aracılığıyla rahatsızlık verme eylemi olarak da tanımlanabilecek olan siber zorbalık, özellikle gençler arasında daha sık gözlemlenmektedir.

Siber Zorbalık;

- Sosyal medyada bir başkasının rahatsızlık verici görüntülerini yayımlamak,
- Bir başkası hakkında yalan ya da uydurma haberler üretmek ve bunları yaymak,
- Bir başkasının özel ya da mahrem bilgilerini sızdırmak,
- Tehdit mesajları yollamak, hakarete varan ifadeler kullanmak,

- Anonim hesaplardan taciz etmek, rahatsızlık vermek,
- Bir başkasının hesaplarını ele geçirmek bu hesaplardan uygunsuz yayınlar yapmak,
- Bir kimsenin paylaşımlarına kasıtlı olarak sürekli olumsuz yorumlar yapmak vb. eylemler olarak karşımıza çıkmaktadır

Siber zorbalığa uğrayan kullanıcılara; zorbaya cevap vermemelerini, delil olabilecek içerikleri saklamalarını, zorbayı engelleyerek ilgili platforma şikâyet etmelerini, durumu yakınlarıyla paylaşmalarını, kolluğa ya da Cumhuriyet Savcılıklarına müracaat ederek siber zorba hakkında suç duyurusunda bulunmalarını tavsiye ediyoruz.





SİBER GÜVENLİK FARKINDALIK AYI

Siber güvenlik, kişisel veri güvenliğinin temini bakımından ciddi bir konudur. Dolayısıyla siber güvenliğe yönelik önlemler almak, kurum ve kuruluşlar açısından önemlidir. Bilindiği üzere Ekim ayı, dünya genelinde “Siber Güvenlik Farkındalık Ayı” olarak kabul edilmekte, bu vesileyle siber güvenliğin önemine dikkat çekilmektedir. Biz de buradan hareketle, kişisel veri güvenliğine dikkat çekmek amacıyla bazı tedbirleri hatırlatmak istedik.

Veri Sorumluları İçin Kişisel Veri Güvenliği Tedbirleri

Günümüzde siber güvenlik, kişisel verilerin korunmasında her zamankinden daha kritik bir role sahiptir. Dijital tehditlerin sürekli geliştiği ve karmaşıklaştığı bir dünyada, yalnızca tek bir güvenlik aracıyla kişisel verilere ilişkin tam bir koruma sağlanamaz. Bu nedenle, verilerin güvenliğini sağlamak için çeşitli tedbirler aynı anda uygulanmalı ve bu tedbirler düzenli olarak gözden geçirilmelidir.

Kişisel veri güvenliğini güçlendirmek için alınabilecek başlıca tedbirlerden bazıları şunlardır:



Kişisel Veri Güvenliği Politikaları Belirleyin

Kişisel veri güvenliğine ilişkin iyi bir politika hazırlanması, bu kapsamdaki risklerin önceden belirlenebilmesini ve istikrarlı bir şekilde önlem alınmasını sağlayacaktır.

Kişisel veri güvenliğine ilişkin belirlenecek doğru ve tutarlı politika ve prosedürler, veri sorumlusunun çalışma ve işleyişine uygun şekilde entegre edilmelidir. Alınacak tedbirlerin önceden belirlendiği iyi bir olay yönetimi, çalışanlar üzerinde ortaya çıkabilecek baskıyı azaltacaktır. Bu nedenle veri sorumlularının, veri kayıt sistemlerinde hangi kişisel verilerin bulunduğu ve mevcut güvenlik önlemlerini inceleyerek diğer yasal yükümlülüklerle uyumlu hareket edildiğinden emin olması gerekmektedir.

Politika ve prosedürler kapsamında; düzenli olarak kontroller yapılmalı, yapılan kontroller belgelenmeli, geliştirilmesi gereken hususlar belirlenmeli ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam edilmelidir.

Ayrıca, her kişisel veri kategorisi için ortaya çıkabilecek riskler ile güvenlik ihlallerinin nasıl yönetileceği de açıkça belirlenmelidir.



Güçlü Parolalar Oluşturun

Güçlü ve karmaşık parolalar kullanın, parolalarınızı periyodik aralıklarla güncelleyin. Parola oluştururken, kişisel bilgilerle ilişkili ve kolay tahmin edilebilecek parolalardan kaçının. Büyük/küçük harfler, rakamlar ve özel karakterlerden oluşan kombinasyonlar tercih edin.

Ayrıca, kaba kuvvet algoritması kullanımı gibi saldırılardan korunmak için şifre girişi deneme sayısını sınırlayın ve mümkünse iki faktörlü kimlik doğrulama aracılığıyla ekstra bir güvenlik katmanı ekleyin.



Erişim Yetkilerini Sınırlandırın

Kişisel veri içeren sistemlere erişimi, yalnızca iş gereği ihtiyaç duyan çalışanlarla sınırlandırın. Erişim yetkilerini, çalışanların iş pozisyonlarına uygun şekilde tanımlayın ve bu yetkileri düzenli olarak gözden geçirin. Erişim yetki ve kontrol matrisleri oluşturun ve erişim politikası ile prosedürlerini uygulamaya alın. Çalışanların işten ayrılması veya görev değişikliği durumunda, hesapların hızlıca kapatılmasını veya yetkilerin güncellenmesini sağlayın.



Yazılım Güncellemelerini Zamanında Yapın

Bilgi teknoloji sistemlerinin güvenliğini sağlamak için yazılım güncellemeleri ve yama yönetimi önemlidir. Bilinen güvenlik açıklarını kapatmak için yazılım ve güvenlik yamalarını zamanında uygulayın. Ayrıca kullanılmayan yazılımları kaldırarak potansiyel güvenlik risklerini azaltın.

Veri Maskeleye ve Şifreleme Uygulayın

Hassas verilerinizi yetkisiz erişimlerden korumak için şifreleme ve veri maskeleye yöntemleri kullanın. Bu sayede yetkisiz kişilerin verilere erişmesi engellenebilir ve veri sızıntıları durumunda verilerin gizliliği korunmuş olur.



Düzenli Veri Yedeklemeleri Gerçekleştirin

Olası veri kayıplarına karşı düzenli yedekleme yaparak verilerinizi güvende tutun. Yedekleme işlemlerini otomatik hale getirin ve bu yedekleri, veri güvenliğini sağlamak üzere şifrelenmiş ve güvenli bir ortamda saklayın.



İnternet Üzerinden Gelen Tehditlere Karşı Korunun

Kişisel veri içeren bilgi teknoloji sistemlerinde, internet üzerinden gelen izinsiz erişim tehditlerine karşı güvenlik duvarı ve ağ geçidi gibi önlemler alınmalıdır. İyi yapılandırılmış bir güvenlik duvarı, kullanılmakta olan ağa derinlemesine etki etmeden önce, gerçekleşen ihlalleri durdurabilir. İnternet ağ geçidi ise çalışanların, kişisel veri güvenliği açısından risk teşkil eden internet sitelerine erişimini önleyebilir.



Antivirüs Yazılımları Kullanın

Kötü amaçlı yazılımlardan korunmak için bilgi sistem ağını düzenli olarak tarayan anti-virüs veya anti-spam gibi yazılımlar kullanın. Bu yazılımları düzenli olarak güncelleyerek sistemlerinizi güvende tutun.



Güvenli Bağlantılar Kullanın

Farklı internet siteleri veya mobil uygulamalar üzerinden kişisel veri toplarken, bu bağlantıların SSL veya daha güvenli yollarla gerçekleştirilmesini sağlayın.



Çalışanlarınızı Düzenli Olarak Eğitin

Çalışanlarınıza siber güvenlik farkındalığı eğitimleri vererek olası tehditlere karşı hazırlıklı olmalarını sağlayın. Sosyal mühendislik saldırıları ve oltalama gibi yaygın tehditler hakkında farkındalık yaratın. Düzenli eğitimler ve güvenlik simülasyonları ile çalışanlarınızı bilinçlendirin ve güvenlik kültürünü şirket genelinde yaygınlaştırın.

» KVKK Bülten



SİBER ZORBALIK NEDİR?



Genel olarak siber zorbalık; “dijital platformlar, dijital ortamlar ve sosyal medya mecraları aracılığıyla rahatsızlık verme eylemi”¹ şeklinde tanımlanmaktadır. Bu tür davranışlar ile sosyal medya, oyun platformları ve anlık mesajlaşma uygulamaları gibi çevrim içi ortamlarda karşılaşılabılır. Siber zorbalık, hedef seçilen kişileri korkutmaya, kızdırmaya ya da utandırmaya yönelik olarak tekrarlanan bir davranıştır². Günümüzde çocuklar kadar yetişkinler de siber zorbalığa maruz kalabilmektedir. Sosyal medyada bir başkasının rahatsızlık verici görüntülerini yayınlamak, uydurma ya da yalan haberler yaymak, tehdit ve hakaret içeren mesajlar yollamak, anonim hesaplardan rahatsızlık vermek, bir kimsenin özel bilgilerini sızdırmak, bir kimsenin paylaşımlarına kasıtlı olarak sürekli olumsuz yorumlar yapmak bu davranışlara örnek olarak verilebilir³.

Siber zorbalıkta fiziksel bir temas söz konusu olmamakla birlikte, bireyler psikolojik olarak zarar görebilmektedir.

1 Siber Suçlarla Mücadele Daire Başkanlığı [SİBERAY], “Siber Zorbalık”, <https://www.siberay.com/siber-zorbalik>.
 2 UNICEF, “Siber zorbalık: Nedir ve nasıl önlenir, Gençlerin siber zorbalıkla ilgili olarak bilmeleri gereken 10 nokta”, <https://www.unicef.org/turkiye/siber-zorbalik-nedir-ve-nas%C4%B1l-nedir-ve-nas%C4%B1l-%C3%B6nlenir>.
 3 SİBERAY, “Siber Zorbalık”.

Siber zorbalığa maruz kaldığınızı düşünüyorsanız;



En kısa zamanda güvendiğiniz bir yakınınıza haber veriniz.

Zorbalığı gerçekleştiren kişiden gelen ve doğruluğunu teyit etmediğiniz hiçbir bilgiye inanmayınız.



Zorbalığı gerçekleştiren kişiyle derhal iletişimi kesin.

Zorbalığı gerçekleştiren kişiyi engelleyebileceğinizi unutmayınız.



Zorbalık bir sosyal medya platformunda gerçekleşiyorsa, platform yetkililerine bildirimde bulununuz.

Kendinizi tehlike altında hissediyorsanız, bu durumu ilgili kurum ve kuruluşlara bildiriniz.



Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın Önemi

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler, sürdürülebilir büyüme ve kalkınmada kilit bir rol oynamaktadır. Özellikle verinin hayatımızdaki konumunun giderek güçlenmesi, veriye dayalı hizmet ve çözümlerin geliştirilmesine katkı sağlamakla birlikte risk ve tehditleri beraberinde getirmiştir. Bu doğrultuda, söz konusu hizmet ve çözümlerin sunulduğu altyapılarda siber risk ve tehditlerin bertaraf edilmesi, sunulan hizmetlerin iyileştirilmesi ve bireylerin güvenliğinin sağlanması zorunlu bir hâle gelmiştir.

Bu kapsamda dijital dünyada verinin korunması, itibar kaybının önlenmesi, siber caydırıcılığın sağlanması hususunda ulusal siber güvenlik politikalarının oluşturulması zorunlu bir ihtiyaç hâline dönüşerek söz konusu ihtiyaçlara binaen ülkemizde, 2013-2014, 2016-2019, 2020-2023 dönemlerini kapsayan Ulusal Siber Güvenlik Stratejileri ve Eylem Planları yayımlanmıştır.

Kapsam

12. Kalkınma Planı çerçevesinde dijital dönüşüme ilişkin küresel eğilimler ve mevcut durum ortaya konularak siber güvenlik konusunda hedef ve politikaların gerçekleştirilmesi amacıyla bir yol haritası çizilmiştir. Bu doğrultuda ülkemizin elde ettiği kazanımların ileriye taşınması ve Kalkınma Planı kapsamında ortaya konulan hedeflerin gerçekleştirilmesi amacıyla Ulaştırma ve Altyapı Bakanlığının koordinasyonunda 2024-2028 yıllarını kapsayan “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı” [Eylem Planı]¹ yayımlanmıştır. Söz konusu Eylem Planı, kamu, özel sektör, sivil toplum kuruluşları ve üniversitelerle iş birliği içerisinde hazırlanmıştır.

Eylem Planı çerçevesinde “*İnsan*”, “*Savunma*”, “*Caydırıcılık*” ve “*İş birliği*” temalarına odaklanılarak 6 stratejik amaç, stratejik amaçlar kapsamında ulaşılmaya planlanan 18 hedef ve ulaşılmaya planlanan hedeflere ilişkin gerçekleştirilecek 61 eylem belirlenmiştir. Bu kapsamda mevcut durum, kapasite, ihtiyaçlar ve zaman unsurları dikkate alınarak sorumlu paydaşlar görevlendirilmiştir.

Stratejik Amaçlar

Eylem Planı kapsamında [1] Siber Dayanıklılık, [2] Proaktif Siber Savunma ve Caydırıcılık, [3] İnsan Odaklı Siber Güvenlik Yaklaşımı, [4] Teknolojinin Güvenli Kullanımı ve Siber Güvenliğe Katkısı, [5] Siber Tehditlerle Mücadelede Yerli ve Milli Teknolojiler ve [6] Uluslararası Alanda Türkiye Markası olmak üzere 6 temel stratejik amaç yer almaktadır.

1) Siber Dayanıklılık

Siber tehditlerin yıkıcı etkilerini azaltmak ve veri trafiğinin güvenli altyapılar üzerinden gerçekleşmesini sağlamak amacıyla savunma etkililiğinin ve siber dayanıklılığın artırılması hedeflenmektedir. Bu kapsamda risk temelli analizlerin yapılması, hazırlık seviyesinin ölçülmesi, uluslararası tatbikatlar yapılması, gerekli tedbirlerin alınması ve denetimlerin sürekliliği önem arz etmektedir.

2) Proaktif Siber Savunma ve Caydırıcılık

Dijital dünyada siber tehditlerin karmaşıklığının giderek artması siber savunma anlayışının da eş güdümlü bir biçimde dönüşmesine neden olmaktadır. Yalnızca siber olay esnasında ve sonrasında değil, siber olay öncesinde proaktif bir siber savunma anlayışı geliştirilerek siber caydırıcılığın sağlanması gerekmektedir. Bu doğrultuda olası tehdit ve zafiyetlerin belirlenmesi, ulusal kapasite ve kabiliyetlerin geliştirilmesi, yapay zekâ ve büyük veri altyapılarıyla tehditlerin erken tespiti ve önlenmesi, Siber Olaylara Müdahale Ekiplerinin kapasitelerinin artırılması hedeflenmektedir.

3) İnsan Odaklı Siber Güvenlik Yaklaşımı

Siber güvenlik zafiyetlerinin büyük bir kısmının insan faktöründen kaynaklanması, bu unsurun önemine işaret etmektedir. Bu kapsamda bilişim teknolojilerinin sunduğu imkânlardan azami ölçüde yararlanılması ve bireylerde bilgi ve farkındalık düzeyinin artırılmasına ilişkin çalışmalar yapılması hedeflenmektedir. Bununla birlikte alana ilgi duyan kişilerin siber uzman olma yolunda desteklenmesi, siber suçlarla mücadelede görev yapan profesyonellerin yetkinliklerinin artırılması ve yeni fırsatlar sunulması planlanmaktadır.

4) Teknolojinin Güvenli Kullanımı ve Siber Güvenliğe Katkısı

Gelişen teknolojiler karşısında, “sıfır güven [zero trust]” anlayışıyla tedbirler belirlenerek güvenli bir siber ortamın sağlanması, yeni teknolojilerin güvenliğine yönelik gereksinimlerin ve asgari güvenlik kriterlerinin değerlendirilmesi ve belirlenmesi, önümüzdeki dönemde gerçekleştirilecek siber savunma ve caydırıcılığın sağlanması çalışmalarının temeli olarak değerlendirilmektedir. Ayrıca yeni teknolojilerin, siber güvenliğinin sağlanmasına ilişkin çalışmalara entegre edilmesine yönelik imkanların araştırılması ve

değerlendirilmesi ile ulusal siber güvenlik çalışmalarına katkı sağlanması planlanmaktadır.

5) Siber Tehditlerle Mücadelede Yerli ve Millî Teknolojiler

Yerli ve millî olarak üretilen teknolojiler, uluslararası arenada devletlerin siber uzaydaki tehditlerden korunmasında önemli bir avantaj olarak öne çıkmaktadır. Bu kapsamda paydaşların iş birliği ile yerli ve millî ürün projelerinin oluşturulması, sertifikasyon ve akreditasyon mekanizmalarının geliştirilmesi, bu alanda verilen teşviklerin artırılması, dışa bağımlılığın azaltılması, sürdürülebilir ekonomik büyümeye ve kalkınmaya destek verilmesi ile siber tehditlere karşı yürütülen mücadelenin bütüncül bir yaklaşımla sürdürülmesi hedeflenmektedir.

6) Uluslararası Alanda Türkiye Markası

Ülkemiz, siber güvenlik alanında gündemin belirlendiği bölgesel ve uluslararası platformlarda aktif rol oynamaktadır. Türkiye markasının etkilerinin artırılması amacıyla ülkemizin uzmanlığının yol gösterici olarak uluslararası seviyede değerlendirilmesine ilişkin çalışmalar yürütülmesi planlanmaktadır. Bu doğrultuda, bölgesel ve uluslararası iş birliklerinde değerlendirilen hususlarla uyumlu şekilde bilgi ve tecrübe paylaşımı sağlanması öngörülmektedir. Ayrıca siber güvenlik alanında ülkemizin tutumunun en iyi şekilde aktarılması ve iş birliğinin geliştirilmesine ilişkin “siber diplomasi” kabiliyetlerimizin artırılması amaçlanmaktadır.

1 T.C. Ulaştırma ve Altyapı Bakanlığı “Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028”, <https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf>

ULUSAL SİBER GÜVENLİK STRATEJİSİ VE EYLEM PLANI 2024-2028

Hedefler

Eylem Planı kapsamında belirlenen hedefler, politika ve stratejilerin gerçekleştirilmesinde bir yol haritası sunmaktadır. Politikaların ve stratejilerin başarısı; doğru, gerçekçi, izlenebilir ve etkili hedeflerin tespit edilmesine ve bu hedeflere ilişkin gerçekleştirilecek çalışmalara bağlıdır. Bu doğrultuda; belirlenen hedefler, aşağıdaki tabloda yer almaktadır:

Siber Dayanıklılık
H1.1 Kamu kurum ve kuruluşları ile kritik altyapı sektörlerinde, düzenleme ve denetlemeye dayalı siber güvenlik yaklaşımının geliştirilmesi.
H1.2 Kurumsal, sektörel ve ulusal bazda; risk temelli analizlere ve acil durum planlamalarına dayalı siber güvenlik yaklaşımının benimsenmesi.
H1.3 Veri paylaşımının güvenli altyapılar üzerinden gerçekleştirilmesi.
H1.4 Ulusal standardizasyon ve test mekanizmalarının geliştirilmesi.
Proaktif Siber Savunma ve Caydırıcılık
H2.1 Siber olaylara müdahale ekiplerinin yetkinlik seviyelerinin artırılması.
H2.2 Siber risklerin ve tehditlerin tespiti ve bildirimi ile siber tehdit istihbaratı edinimi ve paylaşımına yönelik kabiliyetlerin geliştirilmesi.
H2.3 Kurum ve kuruluşlarda risklere ve tehditlere karşı iyi uygulamaların artırılması.
H2.4 Millî güvenliğin bir parçası olarak ulusal siber güvenliğe ilişkin eşgüdümün artırılması.
H2.5 Siber suçlarla mücadelede yönelik kazanımların artırılması.
İnsan Odaklı Siber Güvenlik Yaklaşımı
H3.1 Siber uzayın güvenli kullanılması çerçevesinde bireysel ve toplumsal farkındalığın artırılması.
H3.2 Kurumlarda ve kuruluşlarda, kurumsal siber güvenlik kültürünün yerleştirilmesi.
H3.3 İnsan kaynağının güçlendirilmesi ve yetkinliğinin artırılması.
Teknolojinin Güvenli Kullanımı ve Siber Güvenliğe Katkısı
H4.1 Yeni teknolojilerin güvenli kullanımının sağlanması, oluşabilecek risklere yönelik önlemlerin alınması.
H4.2 Siber güvenliğin sağlanmasına ilişkin çalışmalarda yeni teknolojilerin kullanımının artırılması.
Siber Tehditlerle Mücadelede Yerli ve Millî Teknolojiler
H5.1 Yenilikçi fikirlerin, yerli ve millî ürün ve hizmetlere dönüşümünün sağlanması.
H5.2 Ar-Ge faaliyetlerinin desteklenerek yerli ve millî siber güvenlik teknolojilerinin geliştirilmesi ve yurt içinde kullanımının yaygınlaştırılması.
Uluslararası Alanda Türkiye Markası
H6.1 Uluslararası paydaşlarla bilgi paylaşımının ve iş birliğinin artırılması.
H6.2 Yerli ve millî siber güvenlik çözümlerinin uluslararası alanda rekabet gücünün artırılması.

GENEL OLARAK KİŞİSEL VERİ GÜVENLİĞİNE İLİŞKİN TEDBİRLER

Veri güvenliği, kişisel verilerin korunmasının ayrılmaz ve temel bir unsurudur. Kişisel verilerin korunması, bireylerin mahremiyeti ile temel hak ve özgürlüklerinin güvence altına alınmasını hedeflemekte olup bu hedeflerin etkin bir biçimde sağlanabilmesi için veri güvenliği önlemlerinin titizlikle uygulanması şarttır. Veri güvenliği; yetkisiz erişim, veri sızıntıları ve veri kaybı gibi durumların gerçekleşmesinin önüne geçerek, kişisel verilerin korunmasını mümkün kılan bir güvenlik çerçevesi sunmaktadır. Bu bağlamda, veri güvenliği olmadan kişisel verilerin tam anlamıyla korunması düşünülemez.

Kişisel veri güvenliği temel olarak üç unsurdan meydana gelmektedir. Kişisel verilerin yalnızca yetkili kişilerce erişilebilir olmasını ve yetkisiz kişilerin eline geçmemesini sağlamayı amaçlayan “gizlilik” ilkesi; kişisel verilerin yetkisiz kişiler tarafından değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı tamlığının ve doğruluğunun korunmasını ifade eden “bütünlük” ilkesi; kişisel verilerin her ihtiyaç duyulduğunda yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olması şeklinde tanımlanabilecek “erişilebilirlik” ilkesi kişisel veri güvenliğinin unsurlarını oluşturmaktadır. Veri güvenliği de bu üç unsurun korunması adına alınması gereken tedbirleri ifade etmekte olup bu unsurlardan birinin zarar görmesi halinde veri ihlali gündeme gelecektir.

6698 sayılı Kişisel Verilerin Korunması Kanununun [“Kanun”] 12 nci maddesinde veri güvenliğine ilişkin yükümlülükler düzenlenmiş olup bu maddeyle veri sorumlularının kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlü olduğu ifade edilmiştir.

Bununla birlikte, veri sorumluları veri güvenliğine ilişkin hükümlerin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

Kanunda veri sorumluları uygun güvenlik düzeyini temin etmeye yönelik her türlü teknik ve idari tedbiri almakla yükümlü tutulmuş ancak bu konuda herhangi bir açıklık getirilmemiştir. Kanunun 22 nci maddesinin [1] numaralı fıkrasının [f] bendinin Kurulun görev ve yetkileri kapsamında sayılmış olan “*Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak*” hükmü kapsamında; kişisel verilerin işlenmesi sürecinde veri sorumlularının alması gereken teknik ve idari tedbirler konusunda uygulamada açıklık sağlanması ve iyi uygulama örnekleri oluşturması amacıyla Kişisel Verileri Koruma Kurulu [“Kurul”] tarafından Kişisel Veri Güvenliği Rehberi [“Rehber”] hazırlanmıştır.

Veri sorumlularının öncelikli olarak, işlenen tüm kişisel verilerin neler olduğu, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığı ve gerçekleşmesi durumunda yol açacağı kayıpları doğru bir şekilde belirleyerek buna uygun tedbirleri alması gerekmektedir.

Kişisel veri güvenliğinin sağlanması hususunda çalışanların çok büyük önem taşıdığı bilinmelidir. Bu nedenle çalışanların kişisel verilerin korunmasına yönelik olarak gerekli eğitimi aldığından emin olunmalı ve



farkındalık çalışmaları ile bu eğitimler desteklenmelidir. Gerçekleşen veri ihlallerinin önemli oranda iç unsurlar tarafında meydana geldiği düşünüldüğünde, düzenlenecek eğitim ve farkındalık faaliyetlerinin oynadığı rol daha iyi anlaşılacaktır.

Kişisel verilerin korunmasında önem taşıyan bir diğer nokta da kişisel veri güvenliğine ilişkin hazırlanacak olan politika ve prosedürlere ilişkindir. Veri sorumluları tarafından, kişisel verilere yönelik politikalar hazırlanması risklere karşı tedbirlerin alınabilmesini sağlayacaktır.

Diğer yandan veri sorumluları, sistemlerine içeriden ya da dışarıdan gelebilecek saldırılara karşı bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi ve tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması gibi önlemleri almalıdır.

Siber ortamların yanında kişisel veriler aynı zamanda fiziksel ortamlarda da saklanmaktadır. Bu şekilde saklanan kişisel verilere yönelik kaybolma, çalınma gibi ihtimallere karşı fiziksel güvenlik önlemleri sağlanmalıdır.

Bunların yanında günümüzde bulut teknolojileri hızla gelişmekte ve veri işleme süreçlerinde önemli bir yer tutmaktadır. Kişisel verilerin bulutta depolanması veri sorumlusunun kendi bilgi teknolojileri sisteminden ayrılmasına ve kişisel verilerin bulut depolama hizmeti sağlayıcıları tarafından işlenmesine neden olduğundan, bu konuda da gerekli önlemlerin alınması veri güvenliğinin sağlanmasında önem taşımaktadır.

Veri sorumluları tarafından mevcut sistemlerin gözden geçirilmesi, geliştirilmesi veya iyileştirilmesi ile ilgili gereksinimler zaman zaman ortaya çıkmaktadır. Bu durumlarda da kişisel verilerin güvenliği gereksinimleri göz önünde tutulmalı, yeni bir sistem geliştirilecekse tasarımdan itibaren ve varsayılan olarak mahremiyet ilkelerine uygun hareket edilmeli, sistemlerin geliştirme ve bakımı için ise kişisel veri içeren cihazlar açısından gerekli güvenlik önlemleri sağlanmalıdır.

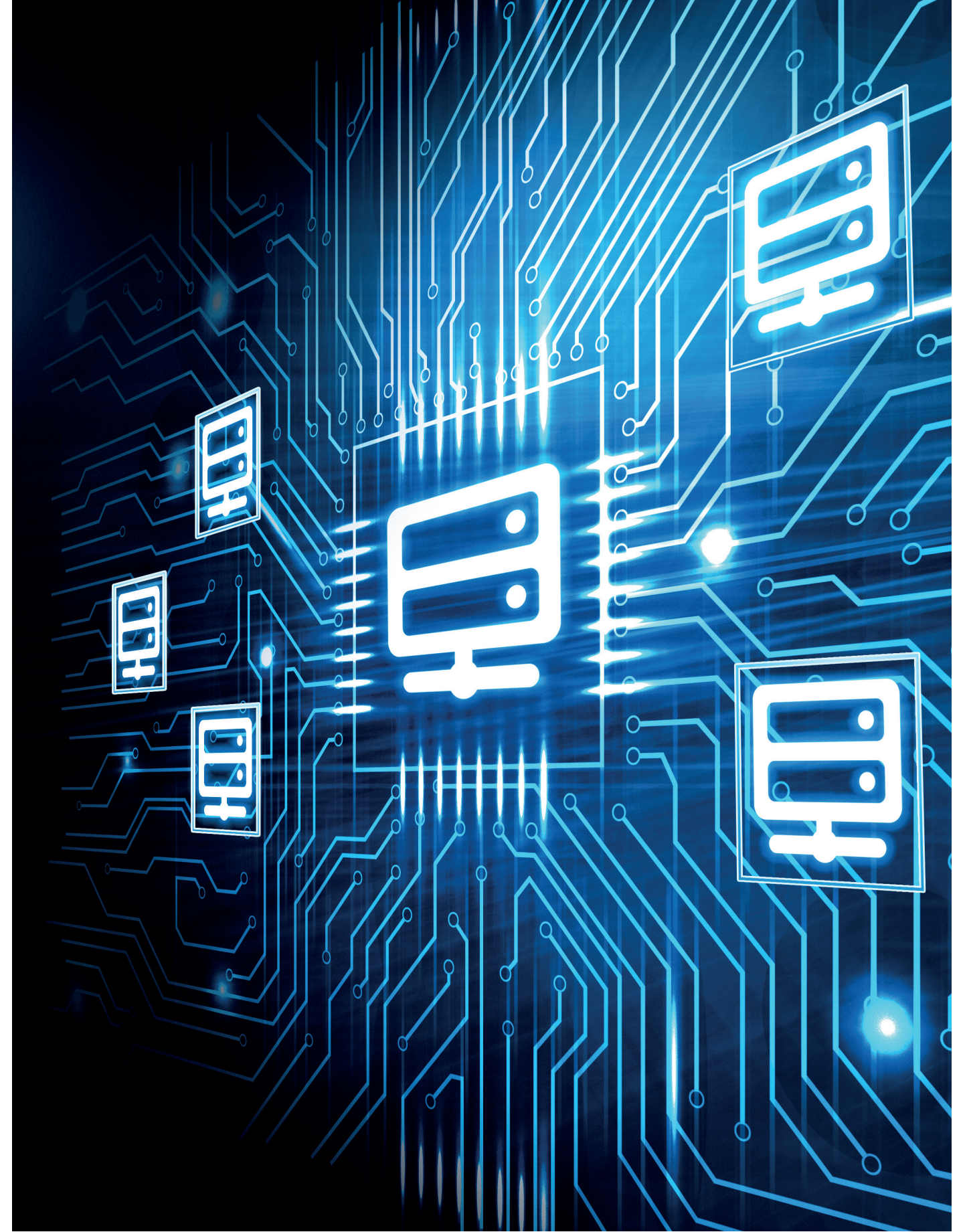
Veri güvenliğinin sağlanamaması, herhangi bir sebeple kişisel verilerin şifrlenmesi, çalınması, yok olması, zarar görmesi ve benzeri durumlarda veri sorumluları yedeklenen kişisel verileri kullanarak en kısa sürede faaliyete geçmelidir. Bu sebeple de kişisel veriler düzenli olarak yedeklenmeli, yedeklenen kişisel verilerin de hem siber ortamda hem de fiziksel olarak güvenliği sağlanmalıdır.

Veri güvenliğinin çeşitli nedenlerle sağlanamaması durumunda veri ihlali durumu ortaya çıkacaktır. Bu durumda da Kanunun 12 nci maddesinin [5] numaralı fıkrasıyla veri sorumlularına veri ihlalinin en kısa sürede ilgisine ve Kurula bildirme yükümlülüğü getirilmiştir. Hem ilgili kişiye hem Kişisel Verileri Koruma Kuruluna yapılacak bildirimlerle ilgili Kurul tarafından alınan Karar ile bu hususların çerçevesi çizilmeye çalışılmıştır.



İhlal nedeniyle kişiler hakkında ortaya çıkabilecek olumsuz sonuçların bir an önce önüne geçilmesi veya en aza indirilmesine imkan verecek önlemler alınması, Kurul tarafından bu konuda alınacak kararlar arasında herhangi bir uyumsuzluğa mahal verilmemesi ve uygulamada bir standartlaşma sağlanabilmesi amacıyla alınmış olan Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/10 sayılı Kararı ile Kurula bildirimde “en kısa sürede” ifadesinin 72 saat olarak yorumlanmasına, Kurula yapılacak bildirimlerde “Kişisel Veri İhlal Bildirim Form”unun kullanılmasına, veri ihlali gerçekleşmesi halinde veri sorumlusu tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir veri ihlali müdahale planı hazırlanarak belirli aralıklarla bu planın gözden geçirilmesine karar verilmiştir.

İlgili kişilere yapılacak bildirimde ise yine aynı Kararla veri sorumlusunca söz konusu veri ihlalden etkilenen kişilerin belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde bildirim yapılmasına karar verilmiş, Kişisel Verileri Koruma Kurulunun 18.09.2019 tarih ve 2019/271 sayılı Kararı ile de ilgili kişilere yapılacak bildirimde yer alması gereken asgari unsurlar belirlenmiştir. Bu Karara göre; veri sorumlusu tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması ve asgari olarak; ihlalin ne zaman gerçekleştiği, hangi kişisel verilerin ihlalden etkilendiği, kişisel veri ihlalinin olası sonuçları, veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler, ilgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da veri sorumlusunun web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları unsurlarına yer verilmesi gerektiğine karar verilmiştir.



AVRUPA BİRLİĞİ’NİN SİBER GÜVENLİK STRATEJİSİNDE DÖNÜŞÜM: NIS2 DİREKTİFİ

Avrupa Birliği genelinde siber güvenlik risklerine karşı daha dirençli bir ekosistem oluşturulması amacıyla hazırlanan NIS2 Direktifinin, üye devletlerin iç hukuklarına aktarılması için belirlenen son tarih 17.10.2024 idi. Bu yazıda; NIS2 Direktifine duyulan ihtiyaç, düzenlemenin temel unsurları, kapsadığı sektörler ve uyumluluğun sağlanamadığı durumlarda karşılaşılabilecek yaptırımlar gibi hususlara ilişkin açıklamalarda bulunulacaktır.

Küresel ölçekte dijital dönüşüm hızla ivme kazanırken, siber güvenlik hem kurumlar hem de bireyler için stratejik bir öncelik hâline gelmiştir. Günümüzde siber tehditler yalnızca bilgi elde etmek ya da sistemlere zarar vermekle sınırlı kalmayıp, kritik altyapıları hedef alarak geniş çaplı güvenlik sorunlarına yol açmaktadır. Özellikle sağlık, finans ve enerji gibi kritik sektörlerdeki dijital ağlar ve bilgi sistemlerine yönelik siber saldırılar, siber güvenlik ihlallerinin etkilerini yalnızca kurumsal zararlarla sınırlı kalmayan toplumsal güvenlik meselelerine dönüştürmektedir.

Fidye yazılımı, ortalama ve DDoS gibi yaygın saldırılar, kurumların iş sürekliliğini tehdit ederken aynı zamanda kullanıcıların kişisel verilerinin güvenliğini ve mahremiyetini de tehlikeye atmaktadır. Bu saldırıların, kişisel verilerin gizliliğine yönelik riskleri artırması ve kurumları daha güçlü güvenlik tedbirleri almaya zorlaması, kapsamlı düzenlemelere olan ihtiyacı daha belirgin bir hâle getirmektedir. Tam da bu noktada, siber tehditlere karşı daha güçlü ve bütüncül önlemler alınması amacıyla hazırlanan NIS2 Direktifi, kritik altyapılarda güvenliği sağlamaya yönelik önemli bir adım olarak öne çıkmaktadır.

NIS Direktifi’nin Güncellenmesi Yönündeki İhtiyaç ve NIS2 Direktifi

2016/1148 sayılı NIS Direktifi [Network and Information Systems Directive]¹, Avrupa Birliği’nin [AB] ilk kapsamlı siber güvenlik düzenlemesi olarak, Birlik içerisindeki ağ ve bilgi sistemlerinin dayanıklılığını artırmayı amaçlayan ve üye devletlerin ortak bir güvenlik düzeyine ulaşmasına yardımcı olan yatay bir iç pazar aracıdır. Bununla birlikte, dijital dönüşümün hızlanması ve COVID-19 krizinin etkisiyle birlikte genişleyen tehdit ortamı, yenilikçi ve uyarlanabilir güvenlik önlemlerinin benimsenmesini zorunlu hâle getirmiştir.

Bu bağlamda Avrupa Komisyonu [Komisyon], NIS Direktifinin etkisini analiz etmek ve eksikliklerini değerlendirmek amacıyla kapsamlı bir paydaş danışma süreci yürütmüştür. Bu sürecin sonunda, NIS Direktifinin temel sınırlamalarının ve eksikliklerinin şu hususlar olduğu belirlenmiştir:

- » AB’de faaliyet gösteren işletmelerin siber dayanıklılık seviyelerinin yetersizliği,
- » Üye devletler ve sektörler arasında siber dayanıklılığa ilişkin uyumsuzluklar,
- » Üye devletler arasında temel tehditler ve zorluklar hakkında ortak bir anlayışın eksikliği,
- » Ortak bir kriz müdahale yaklaşımının bulunmaması.

Bu eksiklikleri gidermek ve dijitalleşme ile artan tehditlere yanıt vermek amacıyla Komisyon, Aralık 2020’de NIS Direktifinin revize edilmesine yönelik bir dizi kural önermiştir. Bu öneriler, AB’nin siber dayanıklılığını artırmaya yönelik “geleceğe uygun” bir düzenlemeler bütünü olarak hazırlanmış ve 2022/2555 sayılı NIS2 Direktifi² 27.12.2022 tarihli AB Resmi Gazetesinde yayımlanmıştır. NIS2 Direktifi, 16.01.2023 tarihinde yürürlüğe girmiş ve üye devletlere düzenlemeyi iç hukuklarına aktarmaları için 17.10.2024 tarihine kadar süre tanınmıştır. 17.10.2024 tarihinde Komisyon, NIS2 Direktifi kapsamında ilk uygulama kurallarının kabul edildiğini de duyurmuştur³.

NIS2 Direktifinin Temel Unsurları

- » NIS Direktifinin eksikliklerini gidermek ve mevcut gereksinimlere uygun bir siber güvenlik çerçevesi sağlamak amacıyla hazırlanan NIS2 Direktifi, önceki düzenlemenin yönelmediği sektörleri de kapsayacak şekilde genişletilmiştir. Bu bağlamda, seçilmiş sektörlerdeki tüm orta ve büyük ölçekli işletmelerin, düzenleme kapsamına dahil edileceği net bir büyüklük eşiği belirlenmiş ve yüksek güvenlik riski profiline sahip küçük işletmelerin de düzenleme kapsamına dahil edilmesine ilişkin olarak üye devletlere takdir yetkisi tanınmıştır.

1 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148>

2 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227&qid=1729928200533>

3 https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5342

- » “Temel [essential] hizmet operatörleri” ile “dijital hizmet sağlayıcıları” arasındaki ayrım kaldırılmıştır. Kuruluşlar önemlerine göre “temel” ve “önemli” olmak üzere iki kategoriye ayrılmış ve bunların farklı denetim rejimlerine tabi tutulacağı düzenlenmiştir.
- » Uygulanması gereken temel güvenlik unsurlarını içeren asgari bir liste oluşturulmuş ve olayların bildirilme/raporlanma süreci, raporların içeriği ve zaman çizelgelerine ilişkin daha net düzenlemeler getirilmiştir.
- » Tedarik zinciri güvenliğine yönelik adımlar atılmış ve şirketlerin tedarik zinciri risklerini ele almaları zorunlu kılınmıştır. Ayrıca, AB düzeyinde temel bilgi ve iletişim teknolojilerine yönelik tedarik zinciri güvenliğini güçlendirme çalışmaları yürütüleceği belirtilmiştir.
- » Ulusal otoriteler için daha sıkı denetim ve yaptırım gereklilikleri öngörülmüş, üye devletler arasında yaptırım rejimlerinin uyumlu hâle getirilmesi hedeflenmiştir.
- » Üye devletler arasında stratejik politika kararlarının şekillendirilmesinde İş Birliği Grubu’nun rolü güçlendirilmiş ve ulusal otoriteler arasında bilgi paylaşımı ve iş birliği desteklenmiştir. Diğer yandan, büyük ölçekli siber güvenlik olaylarının ve krizlerinin koordineli bir şekilde yönetilmesini desteklemek amacıyla “AB Siber Kriz İrtibat Organizasyonu Ağı” (EU-CyCLONe) oluşturulmuştur.
- » Yeni keşfedilen güvenlik açıklarının AB genelinde koordineli bir şekilde bildirilmesini sağlayacak temel bir çerçeve oluşturularak, AB Siber Güvenlik Ajansı (ENISA) tarafından işletilecek olan AB güvenlik açığı veri tabanının oluşturulması düzenlenmiştir. Bu veri tabanı ile, bilgi teknolojileri ürünleri ve hizmetlerindeki güvenlik açıklarının takip edilmesi amaçlanmıştır.

NIS2 Direktifinin Kapsadığı Sektörler ve Kuruluş Türleri

NIS2 Direktifi, aşağıdaki sektörlerde faaliyet gösteren kuruluşları kapsamaktadır:

- **Yüksek Kritiklikteki Sektörler:**
 - Enerji (elektrik, merkezi ısıtma ve soğutma, petrol, gaz ve hidrojen),
 - Ulaşım (hava, demir yolu, su ve kara ulaşımı),
 - Bankacılık,
 - Finansal pazar altyapıları,
 - Sağlık (aşı ve ilaç üretimi dâhil olmak üzere),
 - İçme suyu,
 - Atık su,

- Dijital altyapı (internet değişim noktaları, DNS hizmet sağlayıcıları, TLD isim kayıt şirketleri, bulut bilişim hizmet sağlayıcıları, veri merkezi hizmet sağlayıcıları, içerik dağıtım ağları, güven hizmeti sağlayıcıları, kamuya açık elektronik iletişim ağları ve kamuya açık elektronik iletişim hizmetleri sağlayıcıları),
- Bilgi ve iletişim teknolojileri hizmet yönetimi (yönetilen hizmet sağlayıcıları ve yönetilen güvenlik hizmet sağlayıcıları),
- Kamu yönetimi,
- Uzay.

• Diğer Kritik Sektörler:

- Posta ve kurye hizmetleri,
- Atık yönetimi,
- Kimya,
- Gıda,
- Tıbbi cihaz, bilgisayar ve elektronik, makine ve ekipman, motorlu taşıtlar, römork ve yarı römork ile diğer ulaşım ekipmanlarının üretimi,
- Dijital sağlayıcılar (çevrim içi pazar yerleri, çevrim içi arama motorları ve sosyal ağ platformları),
- Araştırma kuruluşları.

NIS2 Direktifinin Gerekliliklerine Uyulmamasının Yaptırımı

NIS2 Direktifinde belirtilen siber güvenlik risk yönetimi ve raporlama yükümlülüklerinin ihlaline yönelik olarak asgari bir idari yaptırım listesi oluşturulmuştur. Bunlar arasında; bağlayıcı talimatlar, bir güvenlik denetiminin tavsiyelerini uygulama emri, güvenlik önlemlerini Direktifin gereklilikleriyle uyumlu hâle getirme emri ve idari para cezaları gibi yaptırımlar yer almaktadır.

İdari para cezaları açısından bakıldığında, yükümlülüklerin adil bir şekilde dengelenmesini sağlamak adına “temel kuruluşlar” ile “önemli kuruluşlar” arasında ayrıma gidilmiştir.

- Temel kuruluşlar açısından; 10 milyon avroya kadar veya yıllık küresel cirosunun %2’sine kadar (hangisi daha yüksekse),
- Önemli kuruluşlar açısından; 7 milyon avroya kadar veya yıllık küresel cirosunun %1.4’üne kadar (hangisi daha yüksekse) idari para cezası uygulanabilmektedir.

Ayrıca NIS2 Direktifi, kurumsal düzeyde siber güvenlik önlemleri için gerçek anlamda hesap verebilirliği sağlamak amacıyla, düzenlemenin kapsamına dâhil olan kuruluşlarda üst düzey yönetici pozisyonlarında bulunan gerçek kişilerin sorumluluğuna ilişkin hükümler getirmektedir.

Sonuç olarak bakıldığında NIS2 Direktifi, dijital dönüşümün günden güne hız kazandığı bu dönemde, AB genelinde siber güvenlik standartlarını yükselterek kritik altyapıların ve dijital hizmetlerin güvenliğini sağlamayı hedefleyen kapsamlı bir düzenleme olması yönüyle önem taşımaktadır. Bu bağlamda Direktif, özellikle risk yönetimi, tedarik zinciri güvenliği ve kurumlar arası iş birliğini güçlendiren hükümleriyle, üye devletler arasında uyumlu ve güçlü bir siber güvenlik altyapısı oluşturulmasına katkı sağlayacak niteliktedir.

Dijital dünyada karşılaşılan güvenlik zorluklarının üstesinden gelmede NIS2'nin sağladığı bütüncül yaklaşım, toplumsal güvenliği desteklemekte ve dijital ekosistemin daha güvenilir bir hâle getirilmesine katkı sağlamaktadır. Bu yönleriyle NIS2 Direktifi, geleceğe yönelik güçlü bir siber güvenlik altyapısı kurulması yolunda, AB'nin dijital güvenlik stratejisinde kritik bir işlev görmektedir. Diğer yandan bu düzenleme, AB sınırları içerisinde yüksek güvenlik standartları sağlamanın ötesinde, küresel boyutta siber güvenliğin sağlanması açısından da önemli bir çerçeve sunmaktadır.





- * 2024/2847 sayılı Siber Dayanıklılık Yasası, 20.11.2024 tarihli AB Resmî Gazetesinde yayımlandı¹. İnternete bağlı ürünlerin piyasaya sürülmesinden önce güvenli olmasını sağlamak amacıyla, dijital bileşenlere sahip ürünler için güvenlik gereksinimlerine yer verilen düzenlemenin temel unsurları arasında;
 - Donanım ve yazılım ürünlerinin tasarım, üretim ve piyasaya sunulma süreçlerinde AB genelinde siber güvenlik gereklilikleri getirilmesi (örneğin, düzenlemenin gerekliliklerine uygun olduğunu göstermek üzere ürünlerde CE işareti bulunması),
 - Doğrudan veya dolaylı olarak başka bir cihaza veya ağa bağlı olan tüm ürünler için bu düzenlemenin geçerli olması,
 - Tüketicilerin, uygun siber güvenlik özelliklerine sahip donanım ve yazılım ürünleri seçebilmelerinin sağlanması gibi hususlar yer almaktadır.

Düzenleme, AB Resmî Gazetesinde yayımlanmasını takip eden yirminci günde yürürlüğe girecek ve 11.12.2027 tarihi itibarıyla tüm hükümleriyle uygulanacaktır.

1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847, 20.11.2024.

- * Birleşik Krallık Veri Koruma Otoritesi (ICO), kuantum teknolojilerinin veri koruma üzerindeki olası etkilerinin ele alındığı bir rapor yayımladı². Raporda; kuantum bilgisayarlar, iletişim, sensör, zamanlama ve görüntüleme teknolojilerinin gizlilik ve veri koruma üzerindeki etkileri incelenmektedir.

Bu kapsamda, kuantum bilgisayarların mevcut kriptografik algoritmaları kırma potansiyeline sahip olabileceği belirtilmekte ve bu nedenle kuruluşların şimdiden kuantum dirençli kriptografiye hazırlanmaları gerektiği vurgulanmaktadır. Diğer yandan, mahremiyetle ilgili mevcut riskleri artırabilecek olmakla birlikte, bu teknolojilerin kişisel verilerin korunmasına yönelik yeni fırsatlar sunabileceği de ifade edilmektedir.

- * Birleşik Krallık Veri Koruma Otoritesi (ICO), işe alım süreçlerinde yapay zekâ araçlarının kullanımına ilişkin gerçekleştirilen denetimlerden ulaşılan bulguların değerlendirildiği bir rapor yayımladı³. Raporda, iş arayan kişilerin haklarının korunmasını sağlamak amacıyla, yapay zekâ araçlarını geliştirenler, sağlayıcılar ve bu araçları kullanan profesyonellere yönelik çeşitli tavsiyeler paylaşılmaktadır.

Bu çerçevede, işe alım süreçlerinin desteklenmesi amacıyla yapay zekâ araçlarının kullanılmasından önce değerlendirilmesi gereken temel hususlar ise Otorite tarafından şu şekilde belirtilmektedir:

- Veri koruma etki değerlendirmesi gerçekleştirilmesi,
- Kişilerin verilerin hangi hukuki sebebe dayalı olarak işlendiğinin belirlenmesi,
- Sorumlulukların belgelendirilmesi ve veri işleme talimatlarının net bir şekilde ortaya konulması,
- Yapay zekâ araçlarının ortaya çıkarabileceği ön yargıların sağlayıcı tarafından yeterince azaltılıp azaltılmadığının kontrol edilmesi,
- Yapay zekâ aracının şeffaf bir şekilde kullanılıp kullanılmadığının tespit edilmesi,
- Yapay zekâ aracının amacına ulaşması için asgari seviyede kişisel veri elde edildiğinden emin olunması ve işleme amacı kapsamında gerekli olmayan işlemlerin nasıl sınırlandırılabilceğinin belirlenmesidir.

2 <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-quantum-technologies/>, 09.10.2024.

3 <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/11/thinking-of-using-ai-to-assist-recruitment-our-key-data-protection-considerations/>, 06.11.2024.

- * Birleşik Krallık Veri Koruma Otoritesi (ICO), verilerin korunmasına ilişkin olarak genomik teknolojilerin ortaya çıkarabileceği risklerin incelendiği bir rapor yayımladı⁴. Raporda, DNA kullanılarak hastalıkların tahmin edilmesi ve önlenmesi, sigorta poliçelerinin genetik sağlık göstergelerine göre ayarlanması ve fitness planlarının kişiselleştirilmesi gibi genomik veriden önemli faydalar elde edilebilecek günlük kullanım alanlarına değinilirken, aynı zamanda genomik teknolojilerin inovatif potansiyeline de dikkat çekilmektedir.

Genomik teknolojilerin gündeme getirdiği olası veri koruma endişeleri arasında ise şu hususlar yer almaktadır:

- Genomik verilerin hangi durumlarda kişisel veri olarak kabul edilebileceğine ilişkin zorluklar (özellikle ölen kişilere ait genomik veriler veya başlangıçta önemsiz/iliskilendirilemez görünmekle birlikte araştırmalar ilerledikçe kişisel veri niteliği kazanabilecek veriler gibi),
- Bazı genomik verilerin anonim hâle getirilmesinin neredeyse imkânsız olması nedeniyle bu verilerin kötüye kullanılmasına veya bireylerin kimliklerinin tanımlanmasına yönelik riskler,
- Genomik verilerin sigorta veya kolluk kuvvetleri gibi alanlarda kullanılmasının, özellikle mevcut ön yargıları güçlendirebilecek modellerle birleştirilmesi hâlinde sistemik ayrımcılığa yol açma potansiyeli,
- Sağlık hizmetleri gibi sektörlerdeki kuruluşlar arasında veri paylaşımının, bireylerin genomik verilerinin nasıl ve hangi amaçla kullanıldığını anlamalarını zorlaştırması,
- Genomik verilerin doğası gereği aile üyeleriyle ilgili olması nedeniyle, bir kişi hakkında paylaşılan verilerin başka bir kişi hakkındaki hassas nitelikli bilgileri ortaya çıkarabilmesi,
- Genomik veri kullanımının orijinal amacının ötesine genişleme potansiyelinin, veri minimizasyonu ve amacın sınırlandırılması ilkelerine ilişkin endişeler yaratması.

Diğer yandan Otorite, tasarımda mahremiyet ilkesini benimsemeleri ve “düzenleyici koruma alanına” [*regulatory sandbox*] katılmaları yönünde geliştiricilere çağrıda bulunmakta; ayrıca genomik veriler ve mahremiyet konularında bireylerin bilgilendirilmesi ve endişelerinin anlaşılması adına kamu ile etkileşimin artırılmasının hedeflendiğini belirtmektedir.

4 <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/11/privacy-must-still-come-first-were-calling-for-collaboration-with-developers-as-report-reveals-future-innovations-and-data-protection-concerns-in-genomics/>, 07.11.2024.

- * Fransa Veri Koruma Otoritesi (CNIL); mobil uygulamaların, mahremiyetin korunmasını temin edecek şekilde tasarlanmasına yardımcı olmak üzere, mobil uygulama ekosistemindeki paydaşlara yönelik bir dizi tavsiye yayımladı⁵.

- * Avrupa Veri Koruma Kurulu (EDPB), Avrupa Birliği Genel Veri Koruma Tüzüğü’nün (GDPR) 6[1][f] düzenlemesi kapsamında, bir veri işleme şartı olarak “meşru menfaat”e ilişkin değerlendirmelerin yer aldığı rehberini yayımladı ve bu çerçevede Rehber’e ilişkin geri dönüşlerin iletilebileceği belirtildi⁶.

- * Avrupa Komisyonu, Veri Yasası’na [*Data Act*] ilişkin sık sorulan soruların açıklandığı bir doküman yayımladı⁷. Hatırlanacak olursa; gönüllü veri paylaşım mekanizmalarına olan güveni artıran Veri Yönetişimi Yasası’nı [*Data Governance Act*] tamamlayıcı nitelikte olan Veri Yasası, verilere erişilmesi ve bunların kullanımı konusunda hukuki açıklık sağlamaktadır. Bu kapsamda Veri Yasası; endüstriyel veriler başta olmak üzere, verilerin kullanılabilirliğini artıran ve veri ekonomisinde yer alan aktörler arasında verinin değerinin dağıtımında adaleti sağlarken veri odaklı inovasyonu teşvik eden bir düzenleme olup 12.09.2025 tarihinde uygulanmaya başlanacaktır.

- * Avrupa Parlamentosu Araştırma Servisi (EPRS); AB Yapay Zekâ Yasası’nın hazırlanma ve yasalaşma süreci, düzenlemenin temel noktaları ve gündeme getirdiği birtakım hususlara ilişkin açıklamalarda bulunan bir çalışma yayımladı⁸.

- * Bağımsız uzmanlar tarafından hazırlanan, genel amaçlı yapay zekâ uygulama kurallarının ilk taslağı yayımlandı⁹.

- * OECD, finans alanında yapay zekâ kullanımına yönelik farklı düzenleyici yaklaşımların analiz edildiği bir çalışma yayımladı¹⁰.

5 <https://www.cnil.fr/en/mobile-applications-cnil-publishes-its-recommendations-better-privacy-protection>, 24.09.2024.

6 https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en, 09.10.2024

7 <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>, 06.09.2024.

8 [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)698792](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792), 02.09.2024.

9 <https://digital-strategy.ec.europa.eu/en/library/first-draft-general-purpose-ai-code-practice-published-written-independent-experts>, 14.11.2024.

10 https://www.oecd.org/en/publications/regulatory-approaches-to-artificial-intelligence-in-finance_f1498c02-en.html, 05.09.2024.

- * Avrupa Komisyonu, güvenilir ve güvenli yapay zekânın gelişimini teşvik etmek adına AB Yapay Zekâ Paktını ve gönüllü taahhütlerini imzalayan yüzlerce şirketin ismini duyurdu¹¹. İmzacılar arasında; bilgi teknolojileri, telekomünikasyon, sağlık, bankacılık, otomotiv ve havacılık gibi çeşitli sektörlerden çok uluslu şirketler ile Avrupa'daki küçük ve orta ölçekli işletmeler yer almaktadır.

AB Yapay Zekâ Paktı'nda yer alan taahhütler, katılımcı şirketleri en az üç temel eyleme bağlı kalmaya çağırılmaktadır:

- Yapay zekânın kuruluş aşamasında benimsenmesini teşvik etmek ve AB Yapay Zekâ Yasası'na gelecekte uyum sağlamak için yapay zekâ yönetim stratejisi,
- Yüksek riskli yapay zekâ sistemlerinin haritalandırılması ve AB Yapay Zekâ Yasası kapsamında yüksek riskli olarak sınıflandırılması muhtemel yapay zekâ sistemlerinin belirlenmesi,
- Çalışanlar arasında yapay zekâ okuryazarlığını ve farkındalığını teşvik etmek, etik ve sorumlu yapay zekâ geliştirilmesini sağlamak.

Bu temel taahhütlere ek olarak, imzacıların yarısından fazlasının insan gözetimi sağlama, riskleri azaltma ve deepfake gibi içerik türlerini şeffaf bir şekilde etiketleme gibi ek taahhütlerde bulunacaklarını bildirdikleri de açıklandı.

- * Avrupa Komisyonu, güvenilir yapay zekâyâ ilişkin Avrupa liderliğini güçlendirmek için yapay zekâ fabrikaları kurulması yönünde çağrıda bulundu¹². Avrupa Yüksek Performanslı Hesaplama ağı etrafında oluşturulacak ve yeni kurulan şirketler, endüstri ve araştırmacılar gibi çeşitli Avrupa kullanıcılarına sunulacak olan yapay zekâ fabrikalarının; hesaplama gücü, veri ve yetenek olmak üzere yapay zekânın başarıya ulaşması için gerekli temel bileşenleri bir araya getireceği belirtilmektedir.

11 https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4864, 25.09.2024.

12 <https://digital-strategy.ec.europa.eu/en/news/eu-boosts-european-ai-developers-ai-factories-call-proposals>, 10.09.2024.

- * Avustralya'da, kuruluşların güvenli, güvenilir ve sorumlu bir şekilde yapay zekâ sistemleri geliştirmelerine ve kullanmalarına rehberlik etmesi amacıyla hazırlanan "Gönüllü Yapay Zekâ Güvenlik Standardı" yayımlandı¹³. Bahse konu dokümanda; on temel koruyucu önlem, bunların nasıl kullanılacağı ve ne zaman uygulanacağına dair örnekler, standardın nasıl geliştirildiği, standarda yönelik temel kavramlar ve hukuki bağlamı gibi hususlara yer verilmekte olup on temel koruyucu önlem ise şu şekilde belirtilmektedir:

- Yönetişim, dahili kapasite ve düzenleyici uyumluluk için bir strateji dahil olmak üzere hesap verebilirlik süreci oluşturulması, uygulanması ve yayımlanması,
- Riskleri belirlemek ve azaltmak için bir risk yönetimi süreci oluşturulması ve uygulanması,
- Yapay zekâ sistemlerinin korunması, veri kalitesini ve kaynağını yönetmek için veri yönetimi önlemleri uygulanması,
- Modelin performansını değerlendirmek ve kullanım aşamasında sistemi izlemek için yapay zekâ modellerinin ve sistemlerinin test edilmesi,
- Yaşam döngüsü boyunca anlamlı insan gözetimi elde etmek için bir yapay zekâ sisteminde insan kontrolünün veya müdahalesinin etkinleştirilmesi,
- Yapay zekâ destekli kararlar, yapay zekâ ile etkileşimler ve yapay zekâ tarafından oluşturulan içerik hakkında son kullanıcıların bilgilendirilmesi,
- Yapay zekâ sistemlerinden etkilenen kişilerin kullanım veya sonuçlara itiraz edebilmesi için süreçler oluşturulması,
- Yapay zekâ tedarik zincirindeki diğer kuruluşların, riskleri etkili bir şekilde ele almalarına yardımcı olmak üzere veriler, modeller ve sistemler hakkında şeffaf olunması,
- Üçüncü tarafların bu koruyucu önlemlere uyumu değerlendirmelerine olanak sağlamak amacıyla kayıt tutulması ve tutulan bu kayıtların saklanması,
- Paydaşların sürece dahil edilmesi ve güvenlik, çeşitlilik, kapsayıcılık ve adillik konularına odaklanarak paydaşların ihtiyaçların ve koşulların değerlendirilmesi.

13 <https://www.industry.gov.au/publications/voluntary-ai-safety-standard#read-the-voluntary-ai-safety-standard-2>, 05.09.2024.

* Dünya Ekonomik Forumu, üretici yapay zekâ alanındaki hızlı gelişmelere yanıt olarak Accenture ile iş birliği içerisinde bir rapor yayımladı¹⁴. Raporda, üretici yapay zekâ için dayanıklı bir yönetim çerçevesi sunulmakta olup bu kapsamda, kamu-özel sektör iş birliklerinin teşvik edilmesi ve uluslararası iş birliğiyle öngörülü yönetim modelleri geliştirilmesi hedeflenmektedir. Raporda öne çıkan hususlar arasında; düzenleyici boşlukların doldurulması, paydaşların karşılaştıkları yönetsel zorlukların ele alınması ve önümüzdeki süreçte karşılaşılabilecek teknolojik gelişmelere hazırlıklı olunmasına yönelik öneriler yer almaktadır.

* Fransız Siber Güvenlik Ajansı ve Alman Federal Bilgi Güvenliği Ofisi tarafından hazırlanan bir raporda, yapay zekâ kodlama araçlarının güvenli kullanımına yönelik öneriler sunulmaktadır¹⁵. Raporda, bu araçların yazılım geliştirme sürecinde sunduğu fırsatlar ile beraberinde getirdiği riskler ele alınmakta ve bu risklerin nasıl azaltılabileceğine dair somut örnekler paylaşılmaktadır.

Fırsatlar:

- Verimlilik: Kod oluşturma, test senaryoları ve kod biçimlendirme gibi görevleri otomatikleştirerek geliştiricilerin iş yükünü hafifletir.
- Kodu Anlama: Yeni projelerde kodu açıklamak suretiyle geliştiricilerin projelere hızlı bir şekilde adapte olmasına yardımcı olur.
- Programlama Dilleri Arasında Çeviri: Eski kodları, modern programlama dillerine çevirerek bakım süreçlerini kolaylaştırır.

Riskler:

- Veri Güvenliği: Kullanıcı girdileri hassas bilgiler içerebilir ve bu bilgiler sızabilir.
- Kod Kalitesi: Oluşturulan kodun kalitesi ve güvenliği garanti edilemez, güvenlik açıkları bulunabilir.
- Saldırı Riski: Yazılım geliştirme sırasında büyük dil modelleri tabanlı yapay zekâ sistemlerinin kullanılması, kötü niyetli aktörler tarafından istismar edilebilecek yeni saldırı türlerinin ortaya çıkmasına olanak tanıyabilir.

Öneriler:

- Tecrübeli Geliştiriciler: Yapay zekâ, deneyimli geliştiricilerin yerini almamalı ve destekleyici olarak kullanılmalı.
- Risk Analizi: Yapay zekâ araçlarını kullanmadan önce güvenlik riskleri değerlendirilmelidir.
- Kod Kontrolü: Yapay zekâ tarafından oluşturulan kod, geliştiriciler tarafından gözden geçirilmeli ve doğrulanmalıdır.

* TBMM Genel Kurulunda, yapay zekâyla ilgili Meclis Araştırma Komisyonu kurulması kabul edildi¹⁶.

* T.C. İletişim Başkanlığı, sosyal medya kullanımında kamu kurumlarına yol göstermesi amacıyla “Kurumsal Sosyal Medya Kullanım Rehberi” hazırlandığını duyurdu¹⁷. Toplam on bölümden oluşan bu Rehber’de, kamu kurumlarının sosyal medyayı bilinçli, etkili ve sorumlu bir şekilde kullanmalarının sağlanması amaçlanmaktadır. Rehber’de; kurumsal sosyal medya kullanımında genel ilkeler, kurumsal sosyal medya hesabının güvenliğine ilişkin öneriler, kurumsal sosyal medya hesap yönetimi, etik kurallar ve hukuki sorumluluklar, sosyal medyada kriz iletişimi, dezenformasyonla mücadele ve sosyal medyada teyit, sosyal medya hesapları için önerilen örnek uygulamalar gibi konular ele alınmaktadır.

Bahse konu Rehber’de kişisel verilerin korunmasına ilişkin belirlemeler de yer almakta olup bu çerçevede;

- Sosyal medyada yüzde yüz güvenliğin söz konusu olmadığı, bu nedenle nüfus cüzdanının fotoğrafı, kimlik numarası, annenin evlenmeden önceki soyadı gibi kişisel bilgilerin mesajlaşma ve sosyal medya uygulamaları aracılığıyla paylaşılması,
- Kurumsal sosyal medya kullanımında genel ilkeler kapsamında, kişisel verilerin korunması ve gizliliğine özen gösterilmesi ve ilgili mevzuata uygun hareket edilmesi,
- Sosyal medya hesaplarının kullanımı, etkileşimi ve paylaşımları hususlarında 6698 sayılı Kişisel Verilerin Korunması Kanunu da dâhil olmak üzere bir dizi kanun ve diğer mevzuat hükümlerine uyulması,
- Etik kurallar ve hukuki sorumluluklar bağlamında, kişisel verilere ilişkin mevzuata uygun hareket edilmesi ve özel hayatın gizliliğinin korunması gerektiği belirtilmektedir.

* Avrupa Veri Koruma Kurulu (EDPB), 2002/58/EC sayılı e-Gizlilik Direktifi’nin 5/3 maddesi kapsamında değerlendirilebilecek takip teknolojilerine ilişkin açıklamalarda bulunulan ve 2023 yılı içerisinde kamuoyu görüşüne açılan Rehber’in son versiyonunu yayımladı¹⁸. E-Gizlilik Direktifi’nin 5/3 maddesinin farklı teknik çözümlere uygulanabilirliğinin ele alındığı Rehber’de, anılan maddenin çerezlerin yerini alabilecek veya yeni iş modelleri yaratabilecek yeni izleme yöntemlerine uygulanmasına ilişkin belirsizliklerin giderilmesi amaçlanmaktadır.

Bu kapsamda Rehber içerisinde; “bilgi”, “abonenin veya kullanıcının terminal ekipmanı”, “halka açık iletişim ağı”, “erişim sağlanması” ve “bilginin depolanması ve depolanan bilgi” kavramları analiz edilmekte ve URL-piksel takibi, yerel işleme, yalnızca IP adresine dayalı izleme, aralıklı ve aracılı nesnelerin interneti raporlaması ile benzersiz tanımlayıcılar gibi yaygın izleme tekniklerini içeren kullanım senaryolarına yer verilmektedir.

16 <https://www.tbmm.gov.tr/Haber/Detay?Id=b6c9a6c7-d544-42f1-8b16-01924ea8ae5f>, 02.10.2024.

17 <https://www.iletisim.gov.tr/turkce/duyurular/detay/iletisim-baskanligindan-kurumsal-sosyal-medya-kullanim-rehberi>, 10.10.2024.

18 https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_en, 16.10.2024.

14 <https://www.weforum.org/publications/governance-in-the-age-of-generative-ai/>, 08.10.2024.

15 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/ANSSI_BSI_AI_Coding_Assistants.html, 04.10.2024.

* Avrupa Veri Koruma Kurulu (EDPB), GDPR kapsamında bir veri işleme şartı olarak “meşru menfaat”ın hangi durumlarda ne şekilde uygulanabileceğine ilişkin bir içerik paylaştı¹⁹. Genel olarak bakıldığında, bahse konu işleme şartına dayanılabilmesi için dikkate alınması ve bir arada bulunması gereken üç koşul şu şekilde belirtilmektedir:

- Veri sorumlusunun veya üçüncü bir tarafın meşru menfaatinin olup olmadığı netleştirilmelidir. Bu menfaat, kuruluşun gerçek faaliyetlerle ilgili olmalı ve AB ya da üye devlet düzenlemelerine aykırı olmamalıdır. Ayrıca, veri işleme tarihinde geçerli, açık ve somut bir menfaat bulunmalıdır. Diğer bir ifadeyle bahse konu menfaat, varsayımsal bir şekilde belirlenmemelidir.
- Bahse konu işlemenin, meşru menfaat için gerçekten gerekli olup olmadığı değerlendirilmelidir. Bu değerlendirme yapılırken, meşru menfaatin elde edilmesi için bireylerin temel hak ve özgürlüklerini daha az kısıtlayıcı yollarla amaca ulaşılıp ulaşılamayacağı dikkate alınmalıdır. İşleme, yalnızca belirlenen meşru menfaatin gerektirdiği ölçüde yapılmalı ve veri minimizasyonu ilkesine riayet edilmelidir.
- Bireylerin temel hak ve özgürlüklerinin, söz konusu meşru menfaat karşısında üstün gelip gelmediği değerlendirilmelidir. Bu değerlendirme sırasında, bireylerin ilgili kuruluşla olan ilişkilerinden doğan makul beklentileri de göz önünde bulundurulmalı ve işlemenin etkisini sınırlandıran hafifletici önlemler alınmalıdır.

* G7 ülkelerinin dijital kimliğe ilişkin yaklaşımlarındaki ortak noktaların belirlendiği bir rapor OECD tarafından yayımlandı²⁰. Önümüzdeki süreçte birlikte çalışabilirlik çalışmalarını desteklemesi amacıyla hazırlanan Rapor’da; konuya ilişkin kavramlar ve tanımlar, uluslararası teknik standartların kullanımı ve güvence düzeylerine yönelik yaklaşımlara yer verilmektedir.

* Avrupa İnsan Hakları Mahkemesi, “Yeni Teknolojiler”in ele alındığı kararlara ilişkin bilgi notunun güncellenmiş versiyonunu yayımladı²¹. Derleme kapsamında;

- Kitaplar ve müzik eserlerinin telif hakkı,
- Elektronik veriler,
- E-posta,
- Yüz tanıma teknolojisi,
- GPS,
- Radyo veya telekomünikasyona müdahale,

- İnternet,
- IP adresleri,
- Mobil uygulamalar,
- Cep telefonları,
- Çevrim içi taciz,
- Uydu antenleri,
- Gizli kameraların kullanımı,
- Video ile izleme başlıkları altında çeşitli karar özetlerine yer verilmektedir.

* Avrupa Veri Koruma Denetçisi (EDPS), gelişmekte olan teknolojilere ilişkin trendlerin öngörüldüğü “TechSonar”ın 2024-2025 yılına ilişkin raporunu yayımladı²². Bu sayıda;

- Almayla Artırılmış Üretim [*Retrieval-augmented generation*]
- Cihaz Üzerinde Yapay Zekâ [*On-device AI*]
- Makine Öğrenmesinde Unutma [*Machine Unlearning*]
- Çok Modlu Yapay Zekâ [*Multimodal AI*]
- Ölçeklenebilir Gözetim [*Scalable Oversight*]
- Nöro-Sembolik Yapay Zekâ [*Neuro-symbolic AI*] teknolojilerine yer verilmektedir.

19 https://www.linkedin.com/posts/eu-edpb_summary-legitimate-interest-when-and-how-activity-7256583210472501248-40WA?utm_source=share&utm_medium=member_desktop, 28.10.2024.

20 https://www.oecd.org/en/publications/g7-mapping-exercise-of-digital-identity-approaches_56fd4e94-en.html, 15.10.2024.

21 https://www.echr.coe.int/documents/d/echr/FS_New_technologies_ENG, Ekim 2024.

22 <https://www.edps.europa.eu/data-protection/our-work/publications/reports/2024-11-15-techsonar-report-2025>, 15.11.2024.

- * Dünya Ekonomik Forumu, gelişmekte olan teknolojilerle ilişkili riskler ve fırsatların incelendiği, bu kapsamda siber dayanıklılığı artırmak adına veri odaklı iç görülerin paylaşıldığı ve çeşitli önerilerin sunulduğu bir çalışma yayımladı²³.

Geleneksel “tasarımda güvenlik” (*security by design*) yaklaşımının, karmaşık ve gelişen tehdit ortamı karşısında yetersiz kalması nedeniyle “tasarımda dayanıklılık” (*resilience by design*) yaklaşımının benimsenmesine yönelik acil bir gereksinim bulunduğu vurgu yapılan Çalışma’nın temel bulguları arasında şu hususlar yer almaktadır:

- Genişleyen Teknolojik Ortam: Günümüzün dijital ekosistemini şekillendiren ve gelişmekte olan 200’den fazla teknoloji, bu teknolojilerin değerlendirilmesi ve buna uygun güvenlik stratejileri geliştirilmesinde geniş ve kapsayıcı bir yaklaşım gerektirmektedir.
- Artan Saldırı Yüzeyi: Bağlı cihazların sayısının 2030 yılına kadar 32 milyarı aşacağı tahmin edilmekte olup bu durum, siber saldırıların potansiyel giriş noktalarının önemli ölçüde artmasına neden olmaktadır.
- Yapay Zekâya Özgü Tehditler: Veri zehirlenmesi ve model manipülasyonu gibi yapay zekâya özgü saldırıların önlenmesi, stratejilerin güncellenmesi ve sürekli bir şekilde yenilenmesini gerektirmektedir.
- Kuantum Hesaplama Riskleri: Kuantum teknolojisi, mevcut şifreleme yöntemleri için önemli tehditler oluşturduğundan, kuantum dirençli kriptografi çözümleri geliştirilmesine duyulan ihtiyaç artmaktadır.
- Tedarik Zinciri Zafiyetleri: Bilgi ve iletişim teknolojileri tedarik zincirlerinin karmaşık ve küresel yapısı, bunları siber tehditler için birincil hedef hâline getirdiğinden, tüm zincir boyunca kapsamlı güvenlik önlemleri alınması gerekmektedir.
- Düzenleyici Zorluklar: Teknolojik ilerlemelerin hızının, mevcut düzenleyici çerçevelerin önüne geçtiği dikkate alınarak inovasyonu ve güvenliği dengeleyen esnek, uyarlanabilir düzenlemelere ihtiyaç bulunmaktadır.
- Yetkinlik Açığı: Gelişen teknolojiler konusunda uzmanlığa sahip siber güvenlik profesyonellerinin eksikliği, bu sistemlerin ortaya çıkardığı tehditlere yanıt vermede önemli zorluklara neden olmaktadır.

Bu kapsamda geliştirilen öneriler arasında ise;

- Yenilikçi çözümler oluşturmak üzere sürekli bir şekilde araştırma ve geliştirmeye yatırım yapılması,
- Siber güvenlik zorluklarının ele alınmasını sağlamak adına hükümet, endüstri ve akademi arasındaki iş birliğinin güçlendirilmesi,
- Güvenlik ve dayanıklılığın tasarıma entegre edilmesini teşvik eden ve uluslararası iş birliğini kolaylaştıran düzenleyici çerçeveler geliştirilmesi,

- Kapsamlı ve etkili siber dayanıklılık planlaması yapılması ve olay müdahale planlarının düzenli olarak test edilmesi,
- Gelişmekte olan teknolojilerin sorumlu bir şekilde geliştirilmesi ve kullanılmasına yönelik sağlam yönetim yapıları kurulması,
- Siber güvenlik stratejilerinin, yeni teknolojilerin ortaya çıkardığı tehditlere göre uyarlanması gibi hususlar sayılmaktadır.

- * Avrupa Birliği genelinde siber güvenlik risklerine karşı daha dirençli bir ekosistem oluşturulması amacıyla hazırlanan ve 16.01.2023 tarihinde yürürlüğe giren 2022/2555 sayılı NIS2 Direktifinin, üye devletlerin iç hukuklarına aktarılması için belirlenen süre 17.10.2024 tarihinde sona ermiş olup yine bu tarihte Avrupa Komisyonu, NIS2 Direktifi kapsamında ilk uygulama kurallarının kabul edildiğini duyurmuştur²⁴.

- * Avustralya Veri Koruma Otoritesi (OAIC), yapay zekâ ürünlerinden faydalanarak ürün veya hizmet sunan kuruluşlarca dikkat edilmesi gereken hususlara yönelik tavsiyelerin yer aldığı bir rehber yayımladı²⁵. Kuruluşların, ticari olarak sunulan yapay zekâ ürünlerini kullanırken gizlilik yükümlülüklerine uymalarına yardımcı olunması amaçlanan Rehber’den çıkarılabilecek başlıca noktalar şu şekildedir:

- Gizlilik yükümlülükleri, bir yapay zekâ sistemine girilen tüm kişisel bilgiler ve yapay zekâ tarafından üretilen çıktılar [kişisel bilgileri içeriyorsa] için geçerlidir. Ticari olarak sunulan bir yapay zekâ ürününü kullanmayı düşünen kuruluşların, ürünün amaçlanan kullanımlara uygun olduğundan emin olmak için gerekli özeni göstermeleri önem taşımakta olup bu kapsamda ürünün öngörülen kullanımlara yönelik test edilip edilmediği, insan gözetiminin süreçlere nasıl entegre edilebileceği, potansiyel gizlilik-güvenlik riskleri ve kimlerin bu verilere erişim sağlayabileceği gibi hususlar göz önünde bulundurulmalıdır.
- Kuruluşların gizlilik politikaları ve bildirimleri, yapay zekâ kullanımına ilişkin açık ve şeffaf bilgiler içerecek şekilde güncellenmelidir. Ayrıca, şeffaflığın ve gizliliğin korunmasını sağlamak için yapay zekâ sistemlerinin kullanımı konusunda uygun politika ve prosedürler oluşturulmalıdır.
- Kişisel bilgi üretmek veya çıkarımlarda bulunmak için yapay zekâ kullanıldığı durumda, kuruluşlar Avustralya Gizlilik İlkelerine (APP) uygun hareket etmelidirler. Diğer yandan, yapay zekâ modelleri tarafından üretilen çıkarımsal, hatalı veya yapay olarak oluşturulan bilgiler (halüsinasyon veya deepfake gibi), belirli veya makul ölçüde belirlenebilir bir bireyle ilgili olduğu durumda, bu bilgilerin işlenmesinde Avustralya Gizlilik İlkelerine riayet edilmelidir.
- Kişisel bilgilerin bir yapay zekâ sistemine girilmesi durumunda bu bilgiler, yalnızca toplandıkları amaca uygun olarak kullanılmalıdır. Bunun dışındaki bir kullanım, ancak bireyin rızasının olması ya da ikincil kullanımın birey tarafından makul bir şekilde beklenebilir olması ve birincil amaçla ilişkili (hassas bilgiler için ise doğrudan ilişkili) olması durumunda mümkün olabilmektedir.

23 <https://www.weforum.org/publications/navigating-cyber-resilience-in-the-age-of-emerging-technologies-collaborative-solutions-for-complex-challenges/>, 16.10.2024.

24 https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5342, 17.10.2024.

25 <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products>, 23.10.2024.

- Otorite tarafından iyi uygulama örneği olarak; önemli ve karmaşık gizlilik riskleri taşımaları nedeniyle, hassas nitelikli bilgiler başta olmak üzere kişisel bilgilerin kamuya açık üretici yapay zekâ araçlarına girilmemesi önerilmektedir.
- * Avustralya Veri Koruma Otoritesi [OAIC], üretici yapay zekâ modelleri veya sistemleri geliştiren taraflarca dikkat edilmesi gereken hususlara yönelik tavsiyelerin yer aldığı bir rehber yayımladı²⁶. Kişisel bilgileri kullanarak üretici yapay zekâ modellerini eğiten veya ince ayar yapan kuruluşların gizlilik yükümlülüklerine uymalarına yardımcı olunması amaçlanan Rehber'den çıkarılabilecek başlıca noktalar şu şekildedir:
 - Geliştiriciler, üretici yapay zekâ modellerinin doğruluğunu sağlamak için, yüksek kaliteli veri kümelerini kullanmak ve uygun testleri yapmak da dâhil olmak üzere, makul adımları atmalıdırlar. Yapay zekâ kullanımının getirdiği risk düzeyine bağlı olarak, modellerin doğruluğunu sağlamak için gerekli önlemler alınmalıdır ve yüksek risk taşıyan kullanımlarda ek güvenlik önlemleri uygulanmalıdır.
 - Verilerin kamuya açık veya başka bir şekilde erişilebilir olması, bunların üretici yapay zekâ modelleri ya da sistemlerini eğitmek veya ince ayar yapmak için kullanılmasının hukuka uygun olduğu anlamına gelmemektedir. Geliştiriciler, kullanmayı veya toplamayı amaçladıkları verilerin [kamuya açık veriler de dâhil] kişisel bilgi içerip içermediğini değerlendirmeli ve gizlilik yükümlülüklerine uygun hareket etmelidirler. Bu yükümlülüklerin karşılanabilmesi için [örneğin, bilgilerin silinmesi gibi] atılması gereken ek adımlar bulunup bulunmadığı değerlendirilmelidir.
 - Geliştiriciler, hassas nitelik taşıyan bilgiler konusunda özellikle dikkatli olmalıdırlar. Bu çerçevede, bilgilerin bireyden rıza alınmaksızın web üzerinden kazanması veya üçüncü bir tarafın veri kümesinden elde edilmesinin hukuka aykırılık teşkil edebileceği ihtimali üzerinde durulmalıdır.
 - Geliştiriciler, hâlihazırda sahip oldukları kişisel bilgileri bir yapay zekâ modelini eğitmek amacıyla kullanmayı planladıklarında, bunun toplama amacına uygun olup olmadığını değerlendirmelidirler. İkincil kullanım için bireyden rıza alınmadığı durumda, bu kullanımın birey tarafından makul bir şekilde beklenip beklenemeyeceğinin ve ilk toplama amacı ile arasındaki ilişkinin boyutu [hassas bilgiler için ise doğrudan ilişkili olup olmadığı] dikkatli bir şekilde değerlendirilmelidir.
 - Yapay zekâ ile ilgili ikincil kullanımın, ilk toplama amacına uygunluğu ve bunun birey tarafından makul olarak beklenebilir olup olmadığı hususları açık bir şekilde ortaya konulamadığında, bu kullanım için rıza alınmalı ve/veya bireylere bu kullanımdan vazgeçme konusunda anlamlı ve bilgilendirilmiş bir seçenek sunulmalıdır.

- * Avustralya Veri Koruma Otoritesi [OAIC], özel sektör kuruluşlarının internet sitelerinde üçüncü taraf takip pikselleri kullanırken yasal yükümlülüklerini yerine getirmelerine yardımcı olmak amacıyla bir rehber yayımladı²⁷.
- * Birleşik Krallık Bilim, İnovasyon ve Teknoloji Bakanlığı'na bağlı Sorumlu Teknoloji Benimseme Birimi ile Birleşik Krallık Veri Koruma Otoritesi [ICO] tarafından, mahremiyet artırıcı teknolojilere ilişkin "Maliyet-Fayda Farkındalık Aracı" yayımlandı²⁸. Kuruluşların, çeşitli mahremiyet artırıcı teknolojileri benimsemeleri ile ilişkili maliyetleri ve faydaları anlamalarına ve bunları değerlendirmelerine yardımcı olmak amacıyla tasarlandığı belirtilen araç; homomorfik şifreleme, güvenli çok taraflı hesaplama ve diferansiyel mahremiyet gibi gelişmekte olan mahremiyet artırıcı teknolojilere odaklanmaktadır. Bunun yanı sıra, kuruluşların bu teknolojileri değerlendirirken dikkate alabilecekleri faktörlere ilişkin bir kontrol listesi de ilgililere sağlanmaktadır.
- * Avrupa Komisyonu, "Çocuklar için Daha İyi İnternet" [Better Internet for Kids-BIK] portalının yenilenen versiyonunun kullanıma sunulduğunu duyurdu²⁹. Çevrim içi güvenliğe yönelik kapsamlı bir bilgi kaynağı sunan portal, dijital dünyada güvenli ve bilinçli bir şekilde hareket edebilmeleri amacıyla çocuklar, ebeveynler, eğitimciler ve politika yapıcılara rehberlik sağlamaktadır.

Portala eklenen "Ebeveyn ve Bakıcılar Köşesi"; ekran süresi yönetimi, oyun bağımlılığı ve ebeveyn kontrolleri gibi konularda yol gösterici bilgiler sunarken, popüler uygulamalar ve sosyal medya platformlarına ilişkin çeşitli güncel kaynakları da içermektedir. "Gençlik Köşesi"nde ise gençlerin çevrim içi güvenlik konusundaki farkındalıklarının artırılması ve bu alanda aktif bir şekilde rol almalarının teşvik edilmesi amaçlanmaktadır.

Diğer yandan bahse konu portalda, çocukların çevrim içi güvenliğine yönelik merkezi bir bilgi erişim noktası olarak hizmet veren "BIK Bilgi Merkezi" ile ilgili çeşitli bilgiler de paylaşılmaktadır.

- * Birleşik Krallık Veri Koruma Otoritesi [ICO] tarafından yürütülen "Children's Data Lives" projesine ilişkin rapor yayımlandı³⁰. Çocukların çevrim içi dünyadaki davranışları ve bu davranışların kişisel verilerin korunmasına ilişkin haklarla nasıl kesiştiği konusunda temel bir anlayış sunulması amaçlanan projede, çocukların veri mahremiyetine ilişkin farkındalıkları ile mahremiyetin korunmasına verdikleri önem araştırılmaktadır.

9 ila 17 yaş arasındaki 30 çocuğun günlük yaşamlarının gözlemlendiği bu uzun vadeli proje kapsamında ulaşılan temel bulgulardan bazıları şu şekildedir:

- Çocuklar kimi zaman, mahremiyetlerine önem verdiklerini düşündüren şekillerde davransalar dahi verilerinin korunmasına ilişkin sahip oldukları hakların nadiren farkındadırlar. Diğer yandan, çocukların yaşamlarının giderek daha fazla çevrim içi hâle gelmesi ile birlikte verilerini paylaşmaları sıradanlaştığından, çoğu zaman bu davranışı "veri paylaşımı" olarak görmemektedirler.

26 <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-developing-and-training-generative-ai-models>, 23.10.2024.

27 <https://www.oaic.gov.au/news/media-centre/oaic-publishes-guidance-on-tracking-pixels-and-privacy-obligations>, 04.11.2024.

28 <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/11/using-privacy-enhancing-technologies-pets-to-unlock-value-from-data-responsibly/>, 15.11.2024.

29 <https://digital-strategy.ec.europa.eu/en/news/something-bik-has-happened>, 22.10.2024.

30 <https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/children-s-data-lives-research/>, Ekim 2024.

- Yaş gruplarına göre çocukların davranışları farklılık göstermektedir. Örneğin, küçük yaş grubundaki çocuklar [9-11] teknolojiyi oyun ve eğlence aracı olarak görürken; daha büyük yaştaki çocuklar sosyal statüye ve arkadaş ağı oluşturmaya odaklanmaktadır. Bu şekilde bir sosyal motivasyon, belirli noktalarda gizliliğin korunmasını teşvik etse de beğeni, görüntülenme ve popüler uygulamalara erişim isteği gibi durumlar veri mahremiyeti ile çatışabilmektedir.
- Çocuklar açısından konum paylaşımı, aile ve arkadaşlar ile bir yakınlık göstergesi veya ilgi belirtisi olarak algılanmaktadır. Özellikle daha büyük yaştaki çocuklar için, ilişkileri sürdürmenin kabul görmüş ve hatta beklenen bir yönü hâline geldiği anlaşılmaktadır.
- Çocukların platformları kullanma isteği, gizlilik politikalarını göz ardı etmelerine neden olmaktadır. Diğer yandan, verilerine erişilmesi riski soyut bir durum olarak algılanmakta ve şirketlerle veri paylaşımı, genellikle uygulamalara veya hizmetlere erişmek ve bunları kullanmak için gerekli bir adım olarak düşünülmektedir. Ayrıca gizlilik politikalarının görünür olmaması, karmaşık bir şekilde hazırlanmış olması veya bazı platformların çocuklara hitap eden oyun benzeri tasarımlarının veri paylaşımını bir eğlence unsuru gibi göstermesi, çocukların kararları üzerinde etkili olabilmektedir.
- Gerekli kontrolleri ayarlama ve çocukları izleme sorumluluğunun çoğu ebeveynlere aittir. Bu araştırmada yer alan ebeveynlerin, çocuklarının çevrim içi güvenliği konusundaki endişelerinin [kandırılma, uygunsuz içeriklere maruz kalma, çevrim içi zorbalığa uğrama gibi], çocuklarının verilerinin kötüye kullanılması olasılığı ile ilgili endişeleri gölgede bıraktığı görülmektedir. Öte yandan, çocuklarının sosyal hayatta zorluk çekebileceği kaygısı ile bazı ebeveynlerin, çocuklarının platformlara erişimini sağlamak için yaş sınırlamalarını aşmalarına dahi göz yumabildikleri görülmektedir.

* 30.10.2024 tarih ve [mükerrer] 32707 sayılı Resmî Gazete’de yayımlanan “2025 Yılı Cumhurbaşkanlığı Yıllık Programı”nda belirtilen hususlar arasında, 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun Avrupa Birliği Veri Koruma Tüzüğü [GDPR] ile uyumlaştırılmasına yönelik çalışmaların tamamlanacağı [Tedbir 359.2.] da yer almaktadır³¹.

* Kişisel Verileri Koruma Kurulunun 17.10.2024 tarih ve 2024/1793 sayılı kararı ile, veri sorumlusu ve veri işleyenlerin bildirim yükümlülüklerini internet üzerinden daha hızlı ve etkin bir biçimde yerine getirebilmeleri amacıyla hazırlanan “Standart Sözleşme Bildirim Modülü” vasıtasıyla bildirimlerin yapılabilmesine karar verilmiş olup; söz konusu modül ilgililerin kullanımına sunulmuştur³². Standart Sözleşme Bildirim Modülü ekranları ile ilgili detaylı bilgilerin yer aldığı Kılavuza da ilgili Modül üzerinden ulaşılabilir³³.

* Kurumumuz tarafından hazırlanan “Sohbet Robotları [ChatGPT Örneği] Hakkında Bilgi Notu” yayımlandı³⁴. Bahse konu dokümanda genel olarak; yapay zekâ sohbet robotlarının ne işe yaradığı, bu robotlar aracılığıyla hangi kişisel verilerin işlendiği ve sohbet robotu uygulamaları geliştirirken nelere dikkat edilmesi gerektiği hususlarına yer verilmektedir.

* Norveç’te sosyal medya kullanım yaşının 15’e çıkarılması planlanıyor³⁵. Sosyal medya kullanımına ilişkin olarak ülkede hâlihazırda asgari yaş sınırı 13 olsa da Norveç Medya Otoritesi tarafından yapılan araştırmaya göre, 9 yaşındaki çocukların yarısından fazlası, 10 yaşındaki çocukların %58’i ve 11 yaşındaki çocukların %72’si sosyal medyayı kullanıyor.

Bu kapsamda, Hükümet’in çocukların yaş sınırlamalarını aşmasını önlemek amacıyla ek güvenlik önlemleri almayı planladığı; bunlar arasında, sosyal medya platformlarının kullanıcıların kişisel verilerini işleyebilmesi için kullanıcının en az 15 yaşında olmasını gerektirecek şekilde kişisel verilerin korunması mevzuatında değişiklik yapılması ve sosyal medya için bir yaş doğrulama bariyeri geliştirilmesi gibi unsurların yer aldığı belirtilmektedir.

* Avustralya’da, 16 yaş altı çocukların sosyal medya kullanımının yasaklanmasını öngören bir yasa tasarısı Meclis’e sunuldu³⁶. Yasağı ihlal eden şirketlere 49.5 milyon Avustralya dolarına [32.2 milyon ABD doları] kadar para cezası uygulanması öngörülen Tasarı’nın; Snapchat, TikTok, Instagram ve X gibi platformları kapsadığı belirtilirken, sağlık ve eğitim hizmeti sunan platformlar [Headspace, Google Classroom ve YouTube gibi] için istisnalar içerdiği ifade edilmektedir.

* Dünyanın en büyük yayınevlerinden birisi olan Penguin Random House’un [PRH], telif hakkıyla korunan çalışmalarının büyük dil modelleri ve diğer yapay zekâ araçlarını eğitmek için kullanılmasını önlemek amacıyla telif hakkı sayfalarındaki ifadeleri güncellediği bildirildi³⁷. Yeni ifade, tüm yeni eserlere ve yeniden basılan eserlere dahil edilecek.

PRH tarafından küresel olarak tüm baskılarda kullanılacak olan telif hakkı beyanında; “...Bu kitabın hiçbir bölümü, yapay zekâ teknolojileri veya sistemlerinin eğitilmesi amacıyla hiçbir şekilde kullanılamaz veya çoğaltılamaz. 2019/790 sayılı Dijital Tek Pazar Direktifi’nin 4[3] maddesi uyarınca, PRH bu eseri metin ve veri madenciliği istisnasından açıkça kapsam dışı bırakır.” ifadesi yer alıyor.

31 <https://www.resmigazete.gov.tr/eskiler/2024/10/20241030M1-1.pdf>, 30.10.2024.

32 <https://www.kvkk.gov.tr/Icerik/8043/Standart-Sozlesme-Bildirim-Modulu-Hakkinda-Kamuoyu-Duyurusu>, 25.10.2024.

33 <https://standartsozlesme.kvkk.gov.tr/sharedFolder/kullanim-kilavuzu.pdf?v=190123456>, Ekim 2024.

34 <https://www.kvkk.gov.tr/Icerik/8047/Sohbet-Robotlari-ChatGPT-Ornegi-Hakkinda-Bilgi-Notu>, 08.11.2024.

35 <https://www.theguardian.com/world/2024/oct/23/norway-to-increase-minimum-age-limit-on-social-media-to-15-to-protect-children>, 23.10.2024.

36 <https://www.engadget.com/social-media/australia-introduces-a-bill-that-would-ban-children-under-16-from-social-media-174547712.html>, 21.11.2024.

37 <https://www.thebookseller.com/news/penguin-random-house-underscores-copyright-protection-in-ai-rebuff>, 18.10.2024.

* Avustralya’da bir avukatın, yapay zekâ yazılımı kullanarak mahkemeye yanlış bilgi sunduğu ortaya çıktı³⁸. Melbourne’da bir avukat, aile mahkemesinde görülen bir davada yapay zekâ tarafından hazırlanan ve gerçekte var olmayan davaları içeren bir liste sunduğu gerekçesiyle şikâyet edildi. Hâkimin, listede yer alan davaların var olmadığını fark etmesinin ardından avukat, yapay zekâ destekli bir yazılım kullandığını ve oluşturulan listeyi doğrulamadan mahkemeye sunduğunu kabul etti.

* Kaliforniya’da yaşlı bir adam, yapay zekâ ile oğlunun sesinin taklit edilmesi sonucu, oğlunun korkunç bir kazaya karıştığını ve hapisten kefaletle çıkmak için paraya ihtiyacı olduğunu düşünerek dolandırıcılara 25.000 dolar kaptırdı³⁹. Telefonda duyduğu sesin, oğlunun sesiyle tamamen aynı olduğunu iddia eden adam, panikle harekete geçerek dolandırıcıların taleplerini yerine getirdi.

Bu olay, yapay zekâ kullanılarak yapılan dolandırıcılıklara karşı dikkatli olmanın ve acil para talepleri karşısında durumun doğruluğunu farklı kanallardan teyit etmenin önemini bir kez daha göstermektedir.

* Polonya’da, bünyesinde çalışan gazetecileri işten çıkaran ve yapay zekâ tarafından oluşturulan “sunucular” kullanarak yayın hayatına devam edeceğini açıklayan “OFF Radio Krakow”, gelen tepkiler üzerine bu karardan vazgeçildiğini duyurdu⁴⁰. Radyo istasyonunun editörü tarafından yapılan açıklamada, yapay zekâ tarafından oluşturulan sunucuların kullanımının esasen bir “deney” olduğu ve üç ay sürmesi planlanan bu deneyin yoğun tepkiler nedeniyle yalnızca bir hafta sürebildiği belirtildi.

Bu karar alınmadan önce, yakın zamana kadar radyo istasyonunda program yapmış olan bir gazeteci, çalışanların yapay zekâ ile değiştirilmesine karşı çıkan açık bir mektup yayımlamış ve bunun “herkesi etkileyen tehlikeli bir emsal” teşkil ettiğine dikkat çekmişti. Medya sektörü ve yaratıcı endüstrilerde yıllar boyu tecrübe kazanmış kişilerin makinelerle değiştirilmesi riskine vurgu yapan bu çağrı, ülke genelinde büyük yankı uyandırmış ve 23.000’den fazla kişi tarafından imzalanmıştı.

* Türkiye’nin ilk kuantum bilgisayarı “QuanT” tanıtıldı⁴¹.

* Çocuk haklarının korunması ve geliştirilmesi misyonu çerçevesinde Türkiye İnsan Hakları ve Eşitlik Kurumu (TİHEK) tarafından hazırlanmış olan TİHEK Çocuk web sitesinin kullanıma açıldığı duyuruldu⁴². Çocukların haklarını öğrenmeleri, kendilerini ifade edebilmeleri ve hak ihlalleriyle karşılaştıklarında nereden destek alabileceklerini bilmeleri için önemli bir araç niteliği taşıdığı belirtilen internet sitesinde, çocuk haklarıyla ilgili bilgi materyallerinin sunulduğu ve öğretmenler, veliler ve bu alanda çalışan herkes için rehber niteliğinde kaynakların yer aldığı ifade edilmektedir.

38 <https://www.theguardian.com/law/2024/oct/10/melbourne-lawyer-referred-to-complaints-body-after-ai-generated-made-up-case-citations-in-family-court-ntwnfb>, 10.10.2024.

39 <https://nypost.com/2024/10/18/us-news/scammers-swindle-elderly-california-man-out-of-25k-by-using-ai-voice-technology-to-claim-his-son-was-in-horrible-accident-needed-money-for-bail-absolutely-his-voice/>, 18.10.2024.

40 <https://apnews.com/article/poland-media-radio-ai-bba6be01d523c6727d650c69da14960>, 28.10.2024.

41 <https://www.aa.com.tr/tr/bilim-teknoloji/turkiyenin-ilk-kuantum-bilgisayari-quant-tanitildi/3400083>, 21.11.2024.

42 <https://www.tih.gov.tr/tih-cocuk-web-sitesi-lansmani-gerceklestirildi>, 21.11.2024. Bahse konu internet sitesine ulaşmak için bkz. <https://cocuk.tih.gov.tr/>

ADALET BAKANIMIZ SAYIN YILMAZ TUNÇ'UN KURUMUMUZU ZİYARETİ

Adalet Bakanımız Sayın Yılmaz TUNÇ, 13 Kasım 2024 tarihinde Kurumumuzu ziyaret etti. Kurum Başkanımız Faruk BİLİR ve Kurul Üyeleri, Sayın Bakanımıza Kurumumuzun yürütmekte olduğu çalışmalar hakkında bilgi verdi.



DÜNYA ÇOCUK HAKLARI GÜNÜ VE KVKK PROGRAMI

“Dünya Çocuk Hakları Günü ve KVKK” programı, Kurumumuz Konferans Salonunda gerçekleştirildi. Programa öğretmenleriyle birlikte davet edilen ortaokul öğrencileri katıldı. Programın açılış konuşmasını Kurum Başkanımız Prof. Dr. Faruk BİLİR yaptı. BİLİR konuşmasına Çocuk Hakları Günü’ne ilişkin bilgiler vererek başladı.

Çocuk hakları kavramının evrensel bir kavram olduğunu söyleyen BİLİR, Çocuk Haklarına Dair Sözleşme’nin tarihte en geniş kabul gören insan hakları belgesi olduğunu, 20 Kasım 1989 tarihinde imzaya açılan bu sözleşme sayesinde, çocuk haklarının yasalarca tanındığını ifade etti.

Ülkemizin Çocuk Haklarına Dair Sözleşme’yi 1990 yılında imzaladığını ve böylelikle 20 Kasım’ın ülkemizde de “Çocuk Hakları Günü” olarak kutlandığını hatırlatan BİLİR, günümüzde çocukların sahip olduğu haklardan birinin kişisel verilerin korunmasını isteme hakkı olduğunu dile getirdi.

Dijital ortamlarda zaman geçiren bireylerin çoğunluğunun çocuklardan ve gençlerden oluştuğuna dikkat çeken BİLİR, “Çocukları sadece fiziksel dünyanın tehlikelerinden korumak, günümüzde yeterli bir önlem olmaktan çıkmıştır. Çocukları dijital dünyadaki tehlikelerden de korumak gerekli hale gelmiştir. Dijital dünyada çocukların korunması, veri koruma ve mahremiyet bilincinin zihinlere yerleşmesi ve toplumsal kültürün oluşması ile mümkündür.” dedi.

Kişisel verileri işleyen kişi, kurum ve kuruluşların Kişisel Verilerin Korunması Kanunu’na göre birtakım kurallar çerçevesinde hareket etmek durumunda olduğunu belirten BİLİR, bununla birlikte bireylerin de tercihleri doğrultusunda önlemler almasının önemli olduğunu vurguladı.

Kişisel verilerin korunması ve teknoloji kullanımı arasındaki ilişkiden de söz eden BİLİR, şunları söyledi: “Kişisel verilerin korunması; teknolojiden uzak durmak, teknolojik gelişmelere kendimizi kapatmak değildir. Elbette dijitalleşmenin getirdiği kolaylıklardan ve imkanlardan yararlanacağız. Bununla birlikte veri koruma bilincini ve bu kapsamda dikkat etmemiz gerekenleri günlük hayatımızda bir alışkanlık haline getireceğiz. Dijital dünyada riskler, tehlikeler her zaman olacaktır. Burada hepimize düşen görev, tehlikelerin farkında olmak ve tedbirlerimizi buna göre almaktır.”

Öte yandan öğrencilerin de katılımıyla interaktif bir şekilde gerçekleştirilen program kapsamında Kurumumuz Uzman Yardımcılarından Cemre Berfin TÜZÜN “Mahremiyet Çağında Çocukların Kişisel Verilerinin Korunması” konulu bir sunum yaptı.

Kurumumuz Uzmanlarından Uğur TOKMAKÇI, Kurumumuz tarafından hazırlanan eğitici videoların gösterimini yaparak öğrencilerle güvenli parola oluşturma uygulamaları gerçekleştirdi.

Kurumumuz Uzman Yardımcılarından Büşra DURMUŞOĞLU GÜNEY ve Ezgi TURGUT BİLGİÇ ise, Kurumumuzun kişisel verilerin korunmasına ilişkin hazırladığı farkındalık çalışmalarını anlattılar.



4. KİŞİSEL VERİLERİ KORUMA ZİRVESİ

4. Kişisel Verileri Koruma Zirvesi, Kurumumuz ile Türkiye Bilişim Derneği'nin (TBD) iş birliğinde Kurumumuz Konferans Salonunda gerçekleştirildi. Zirveye Kurum Başkanımız Prof. Dr. Faruk BİLİR, Kişisel Verileri Koruma Kurulu Üyeleri, Türkiye Bilişim Derneği Başkanı Rahmi AKTEPE ile kamu ve özel sektörden çok sayıda temsilci katıldı. "Dijital Çağda Hukuk" temasıyla düzenlenen Zirvenin açılış konuşmasını Kurum Başkanımız Prof. Dr. Faruk BİLİR yaptı.

BİLİR, kişisel verilerin korunmasının dijital çağda hukukun en önemli konularından biri olduğunu, bilişim alanındaki ilerlemeyle internet ve dijital platformlarda büyük miktarda veri toplandığını ve bu verilerin kötüye kullanılmasını önlemek için hukuki düzenlemelerin varlığının önem taşıdığını

belirterek bunun sonucunda dünyada veri koruma ve gizlilik düzenlemelerinin ön plana çıktığını, ülkemizde ise bu konuyu kapsamlı bir şekilde ele alan başlıca düzenlemenin 6698 Sayılı Kişisel Verilerin Korunması Kanunu olduğunu söyledi.

Kişisel Verilerin Korunması Kanunu kapsamında kişisel veri güvenliğinin önemli olduğunu altını çizen BİLİR, günümüz dünyasında kişisel veri güvenliğinin, hem bireyler hem de kurum ve kuruluşlar açısından daha fazla öneme sahip olduğunu, verilerin güvenli bir şekilde muhafaza edilmesinin yalnızca idari tedbirlerle değil, aynı zamanda teknik tedbirlerle de desteklenmesi gerektiğini vurguladı.



SİBER DÜNYA VE KİŞİSEL VERİLERİN KORUNMASI ETKİNLİĞİ



Anadolu Bilişim Buluşmaları kapsamında, “Siber Dünya ve Kişisel Verilerin Korunması” etkinliği Kurumumuz ev sahipliğinde gerçekleştirildi. Etkinlik kapsamında teknolojiye gelişmeler ve dijitalleşme sonucu artan siber tehditlere ve siber güvenlik risklerine dikkat çekilerek kişisel verilerin korunmasına yönelik strateji ve uygulamalar güncel gelişmeler ışığında, alanında uzman kişiler tarafından ele alındı.

Etkinliğin açılışında konuşan Kurum Başkanımız Prof. Dr. Faruk BİLİR, kişisel verilerin korunmasının genel olarak bireylerin verilerinin başka kişi veya kuruluşlar tarafından yetkisiz kullanımına karşı sahip oldukları bir hak olduğunu söyleyerek, bu hakkın teknolojinin kötüye kullanımından doğabilecek olumsuz etkilere karşı, bireyin korunmasını esas alan temel bir insan hakkı olduğunu ifade etti.

Özellikle yapay zekâ ve nesnelerin interneti gibi güncel teknolojiler sayesinde kişisel verilerin daha fazla ve daha etkin işlenmesinin mümkün olduğunu kaydeden BİLİR, kişisel verilerin korunması hakkının teknoloji ve mahremiyet arasında düzenleyici ve dengeleyici bir mekanizma olduğunu, dolayısıyla bireyin mahremiyetine yönelik oluşabilecek risk ve tehditlere karşı önleyici bir rol üstlendiğini dile getirdi.



KAYMAKAM ADAYLARINA KİŞİSEL VERİLERİN KORUNMASI HAKKINDA SEMİNER

Kurum Başkanımız Prof. Dr. Faruk BİLİR, İçişleri Bakanlığı Eğitim Dairesi Başkanlığınca düzenlenen 109. Dönem Kaymakamlık Kursu kapsamında, kaymakam adaylarına “6698 Sayılı Kişisel Verilerin Korunması Kanunu” hakkında seminer verdi.



TİHEK AKADEMİ SÖYLEŞİLERİ ETKİNLİĞİ

Kurum Başkanımız Prof. Dr. Faruk BİLİR, Türkiye İnsan Hakları ve Eşitlik Kurumu tarafından düzenlenen “TİHEK Akademi Söyleşileri” etkinliğine konuşmacı olarak katılım sağladı. Etkinlik kapsamında “Kişisel Verilerin Korunması Kanunu ve Uygulaması” temalı seminer veren BİLİR, Kanuna ilişkin çeşitli bilgiler paylaştı.



ULUSLARARASI VERİ BİLİMİ VE İSTATİSTİK KONGRESİ

Kurum Başkanımız Prof. Dr. Faruk BİLİR, Türkiye İstatistik Derneği tarafından düzenlenen “Uluslararası Veri Bilimi ve İstatistik Kongresi IDSSC 2024” etkinliği açılış programına katılım sağladı. Etkinlik kapsamındaki açılış panelinde oturum başkanı olarak “yapay zekâ ve mahremiyet” temalı konuşma gerçekleştiren BİLİR, kişisel verilerin korunması mevzuatı ve yapay zekâ hakkında çeşitli bilgiler paylaştı.



46. KÜRESEL MAHREMİYET ASAMBLESİ

Jersey Veri Koruma Otoritesi'nin ev sahipliğinde düzenlenen ve veri koruma alanında dünyadaki önemli aktörleri bir araya getiren Küresel Mahremiyet Asamblesi'nin 46'ncı Konferansına Kurumumuzu temsilen Kurum Başkanımız Prof. Dr. Faruk BİLİR ve beraberindeki heyet tarafından katılım sağlandı.

Veri koruma otoriteleri temsilcilerinin yanı sıra uluslararası kuruluşlar, özel sektör ve sivil toplum kuruluşlarından çok sayıda uzman konuşmacının yer aldığı Konferansa yoğun ilgi gösterildi.

Konferansın ilk üç gününde kamuya açık şekilde oturumlar gerçekleştirildi. Yapay zekâ ve etik, insani kriz durumlarında mahremiyetin önemi, sınır ötesi veri aktarımı, çocukların kişisel verilerinin korunması ile siber güvenlik konularında sunumlar ve paneller gerçekleştirildi. Son iki günde ise sadece veri koruma otoritelerinin katılımına açık şekilde toplantılar gerçekleştirilerek GPA Çalışma Gruplarının raporları görüşüldü ve İlke Kararları kabul edildi.



SOHBET ROBOTLARI (CHATGPT ÖRNEĞİ) HAKKINDA BİLGİ NOTU



SOHBET ROBOTLARI (CHATGPT ÖRNEĞİ) HAKKINDA BİLGİ NOTU

Sohbet robotlarının kişisel veriler ile temas ettiği noktaların daha iyi anlaşılabilmesi amacıyla "Sohbet Robotları (ChatGPT Örneği) Hakkında Bilgi Notu" yayımlandı.

Söz konusu bilgi notunda genel olarak; yapay zekâ sohbet robotlarının ne işe yaradığı, bu robotlar aracılığıyla hangi kişisel verilerin işlendiği ve sohbet robotu uygulamaları geliştirilirken nelere dikkat edilmesi gerektiği hususlarına yer verildi.

VERİCAN İLE KİŞİSEL VERİLERİ ÖĞRENIYORUM

Kişisel verilerin neler olduğunu, kişisel verilerin nasıl korunacağını ve çevrim içi ortamda güvende kalmanın yollarını çocuklara öğretmeyi amaçlayan “VERİCAN İle Kişisel Verileri Öğreniyorum” isimli çizgi roman serisi yayımlandı.

Kurumumuz internet sitesi www.kvkk.gov.tr üzerinden yayımlanan;

- » Verican ile Kişisel Verileri Öğreniyorum
- » Verican'dan Ebeveynlere Tavsiyeler
- » Verican ile Okulda Bir Gün
- » Verican Siber Zorbalığa Müdahale Ediyor
- » Verican Oyun Bağımlılığına Karşı
- » Verican Hastanede

olmak üzere toplamda altı farklı hikayeden oluşan çizgi roman serisi, çocukların kişisel veri güvenliği ve mahremiyet konusunda bilgi sahibi olmasını amaçlamaktadır.



ÇARŞAMBA SEMİNERLERİ

- » “Rekabet Hukuku Bakımından Veri Taşıma”
 - » “Kişisel Veriden Reklama, Hedefli Reklamcılık ve Reklam Kurulu Kararları”
- konulu Çarşamba Seminerleri, Kurumumuz Konferans Salonunda düzenlendi.



KAMUOYU DUYURULARI

- » Veri Sorumluları Sicili
 - » Araştırma Şirketlerinin İstatistiksel Araştırma Yapmak Amacıyla “Rastgele Numara Çevirme ile Telefon Mülakatı Yöntemi” Kullanarak Gerçekleştirdikleri Kişisel Veri İşleme Faaliyetleri
 - » Standart Sözleşme Bildirim Modülü
- hakkında kamuoyu duyuruları yayımlandı.



SOMALİ VERİ KORUMA OTORİTESİNİN KURUMUMUZU ZİYARETİ

Somali Veri Koruma Otoritesi ile Kurumumuz arasında yapılan görüşmede; her iki Kurumun Başkanları, Somali Devleti Türkiye Büyükelçisi ve heyetleri arasında olası iş birliği konuları görüşüldü. Görüşmede, ülkemiz ile Somali arasında farklı konulardaki iş birliğinin, kişisel verilerin korunması alanına da taşınmasının önemine vurgu yapıldı.



KURUMUMUZ İLE TİCARET BAKANLIĞI ARASINDA İŞ BİRLİĞİ PROTOKOLÜ

Hedefli reklamcılık ve aldatıcı ticari tasarım uygulamaları hakkında toplumun her kesiminde farkındalığın artırılması, dijital reklam ve uygulamalar ile kişisel verilerin kullanımına ilişkin ortak alanlarda uluslararası düzenlemelerin ve uygulamaların takip edilmesi ve mevcut ya da olası ihlallere karşı ortak politika üretilmesi amacıyla, Kurumumuz ile Ticaret Bakanlığı Tüketicinin Korunması ve Piyasa Gözetimi Genel Müdürlüğü arasında iş birliği protokolü imzalandı.

Kişisel Verileri Koruma Kurumu ile Ticaret Bakanlığı Arasında İş Birliği Protokolü İmzalandı



PODCAST



"Bir Küçük Farkındalık Yeter" isimli podcast kanalımızda; kişisel verilerin korunmasına ilişkin gelişmeler konusunda bilgi paylaşımını amaçlayan podcast serimizin yeni bölümleri yayınlandı.



kvvkkurumu



Kişisel Verileri Koruma Kurumu

Nasuh Akar Mahallesi 1407. Sokak

No.4 06520 Çankaya | ANKARA

T. 0312 216 50 00

www.kvkk.gov.tr