ISSN : 2980-1591
e-ISSN 2980-3845
Yıl/Year : December/Aralık 2024
Cilt/Volume : 2
Sayı/Issue : 3

Veri Madenciliğinin Siber Suçlarda Kötüye Kullanımı

Misuse of Data Mining in Cybercrime

Özgür SAĞIR[1] Nur Banu ALBAYRAK[2]

İnceleme Makalesi
Review Article

Geliş tarihi/Received:
28.12.2023

Son revizyon teslimi/Last revision received:
2.12.2024

Kabul tarihi/Accepted:
20.12.2024

Yayın tarihi/Published:
Aralık 2024

Atıf/Citation:
Sağır, Ö., Albayrak, N. B., (2024). Veri Madenciliğinin Siber Suçlarda Kötüye Kullanımı Journal of Kocaeli Health and Technology University, 2(3), 68-80

DOI:

ÖZET

Günümüz teknolojisinin hızla gelişmesi, internet ortamında işlenen suçların da aynı hızla artmasına neden olmuştur. Önemsiz gibi görünen küçük ayrıntılardan, bu alanın uzmanı veri madencilerinin bilgi üretebilme ihtimalleri göz önünde bulundurulduğunda, istenmeyen sonuçların ortaya çıkması ne yazık ki kaçınılmazdır. Bu nedenle, kişisel bilgilerimiz başta olmak üzere şirket veya kurum bilgilerimizin de çalınma / sızdırılma riski ortaya çıkmıştır. Kişisel verilerimizin ticari bir metaya dönüşmesi, her geçen gün hızla artan siber suçlar, insanların dijital ortamlarda sosyalleşme çabaları neticesinde bilinçsizce paylaşılan kişisel veriler sonucunda bahse konu verilerin genel mevzuat hükümlerine göre korunması konusunda yetersizlik meydana gelmektedir. Sanal bir dünyada kişinin hareketlerini analiz eden ve kişinin kendisi gibi düşünen dijital bir model oluşturmanın mümkün olduğu ve bu yüzden de kişinin sonraki hamlelerinin tahmin edilebileceği artık hayal olmaktan öte, kaçınılmaz bir gerçeklik olarak karşımıza çıkmaktadır. Önemsiz gördüğümüz küçük ayrıntılardan, bu alanın uzmanı veri madencilerinin bilgi üretebilme ihtimalleri göz önünde bulundurulduğunda istenmeyen sonuçlar ortaya çıkabilmektedir. Bu araştırmada veri madenciliği, verilerin elde edilme yöntemleri ve bu yöntemlerle işlenen bazı siber suçların incelenmesi yapılmış ve incelenen suçlara çözüm / önleme önerisi getirebilmek amaçlanmıştır. Suçun çeşitliliğinin daha fazla olacağı göz önünde bulundurularak birkaç örnek verilmiş, bu konu hakkında farkındalık oluşturabilmek amaçlanmış ve önerilerde bulunulmuştur.

Anahtar Kelimeler: Veri madenciliği, siber suçlar, bilişim hukuku

1. *Yüksek Lisans Öğrencisi, Kocaeli Sağlık ve Teknoloji Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilişim Sistemleri Mühendisliği, Kocaeli, Türkiye, ozgur.sagir@kocaelisaglik.edu.tr ORCID: 0009-0005-1361-0902*
2. *Dr. Öğr. Üyesi, Kocaeli Sağlık ve Teknoloji Üniversitesi, Yazılım Mühendisliği, nurbanu.albayrak@kocaelisaglik.edu.tr*

ABSTRACT

The rapid development of today's technology has caused the crimes committed on the internet to increase at the same rate. Considering the possibility that data miners, who are experts in this field, can generate information from seemingly insignificant details, it is unfortunately inevitable that undesirable results will occur. Therefore, the risk of theft/leakage of our company or institutional information, especially our personal information, has emerged. As a result of the transformation of our personal data into a commercial commodity, rapidly increasing cybercrimes every day, and personal data shared unconsciously as a result of people's efforts to socialize in digital environments, there is an inadequacy in the protection of the data in question according to the provisions of the general legislation. The fact that it is possible to create a digital model in a virtual world that analyzes a person's actions and thinks like the person himself, and therefore can predict the person's next moves, is no longer a dream, but an inevitable reality. Unintended consequences can arise when we consider the possibility that data miners, who are experts in this field, can generate information from small details that we consider insignificant. In this research, data mining, methods of obtaining data and some cybercrimes committed with these methods were examined and it was aimed to propose solutions/prevention to the crimes examined. Considering that the diversity of crime is likely to be greater, a few examples are given to raise awareness on this issue and some recommendations are made.

Keywords: Data mining, cyber crimes, information law

1. GİRİŞ

Veri, sensörler aracılığıyla topladığımız ham değerlere denir. Veri madenciliği ise yapısal veri tabanlarında depolanmış büyük ölçekli veriler arasından geçerli, yeni, potansiyel olarak yararlı ve nihayetinde anlaşılabilir örüntülerin tanımlanması, değerli olan bilginin elde edilmesi işlemidir. Burada amaç faydalı olan bilgiye, verilerin içinde kolayca görülemeyen ilişkileri bularak, yani derine inip bilgiyi madenleyerek ulaşmaktır (1).

Bilişim hukuku, teknolojideki gelişmelerle beraber oluşacak olan itilafların çözümü ile ilgilenen hukuk dalıdır. Bilgi ve teknolojinin kötüye kullanımı ile insanlara zarar verilmesini önlemek amacıyla ortaya çıkmıştır (2).

Bilişim suçu veya bilgisayar suçu ise bir bilgisayar veya bilgisayar ağı kullanılarak işlenen herhangi bir suçu ifade etmektedir. Bilgisayar, bir suçun işlenmesinde kullanılabileceği gibi, bir suçun hedefi de olabilir. Bilişim, işlenen suçta araç veya hedef olmalıdır.

Kişisel veri, belirli veya belirlenebilir nitelikteki bir kişiyle alakalı her türlü bilgiye denir. Kişinin mesleki, ailevi ya da şahsi özelliklerini belli eden, o kişinin diğer kişilerden ayırt

edebilmeye ve özelliklerini ortaya çıkarmaya yarayan her türlü bilgidir. Kişisel veriyi, kişisel olmayan verilerden ayırabilmek için verinin bir kişiye ilişkin olması ve bu kişinin de belirli ya da belirlenebilir ve ayırt edici nitelikte olması ölçütü aranmaktadır (3).

Kişisel verilerimizin ticari bir metaya dönüşmesi, her geçen gün hızla artan siber suçlar, insanların dijital ortamlarda sosyalleşme çabaları neticesinde bilinçsizce paylaşılan kişisel veriler sonucunda bahse konu verilerin genel mevzuat hükümlerine göre korunması konusunda yetersizlik meydana gelmektedir (4).

Kötü niyetli veri madenciliği yapılmasının amacı yalnızca kişisel veri elde etmek olmayabilir. Kurum veya şirket verileri ve bilgilerini ele geçirerek, bunları izinsiz pazarlamak veya yaymak da amaç dahilinde olabilmektedir.

1.1. Veri Madenciliği Yöntemi ile Verilerin Elde Edilmesi

Veri madenciliği, günümüzün en önemli bilgi işlem alanlarından biridir ve verilerden değer yaratmanın bir yoludur. Bu yöntem ile verilerden gizli kalmış bilgiler açığa çıkarılabilir ve bu bilgilerden yeni iş fırsatları, stratejiler ve ürünler geliştirilebilir. Veri madenciliği yöntemi ile verileri elde etmek, bu sürecin ilk adımı olarak büyük önem taşır (Şekil 1).

1.1.1 Veri Temizliği (Data Cleaning)

Eldeki verilerden hatalı, tutarsız, gürültülü veya eksik olan verilerin temizlendiği ve düzeltildiği süreçtir. Gürültü, ana veri üzerine işlenmiş veya eklenmiş olan istenmeyen verilerdir. Bu aşama, doğru ve güvenilir analizler yapabilmek için kritik bir öneme sahiptir.

1.1.2. Veri Zenginleştirme (Data Enrichment)

Mevcut veri setine yeni ve genellikle dış kaynaklardan elde edilen bilgilerin eklenmesini içerir. Bu süreç, veri setini daha kapsamlı hale getirerek analizlerin daha derinlemesine yapılmasına olanak tanır.

1.1.3. Veri Birleştirme ve Bütünleştirme (Data Unification and Integration)

Veri birleştirme, farklı kaynaklardan gelen veri setlerini bir araya getirme sürecini ifade eder. Bütünleştirme ise bu birleştirilmiş veri setlerini uyumlu bir yapıya getirme işlemidir. Bu sayede tutarsızlık ve çakışma sorunları giderilir.

1.1.4. Veri Seçme (Data Selection)

Analiz için en uygun olan veri setinin belirlenmesini içerir. Bu aşamada, belirli özelliklere sahip verilerin filtrelenmesi ve seçilmesi sağlanır. Ayrıca, veri tabanlarından alınmış olan analiz sonucu, ilgili verilerden hedefle alakalı olan verilerin seçildiği süreçtir.

1.1.5. Veri Dönüştürme (Data Transformation)

Veri setindeki formatları, birimleri veya yapıları değiştirme sürecidir. Verilerin uygun olan formlara dönüştürülmesi ve veri madenciliği için kullanılabilecek hale getirilmesidir. Bu süreçte boyut azaltılabilir veya veri dengelenebilir. Bu, veriyi analiz veya raporlama için daha uygun hale getirmeyi amaçlar.

1.1.6. Veri Madenciliği Uygulaması (Data Mining)

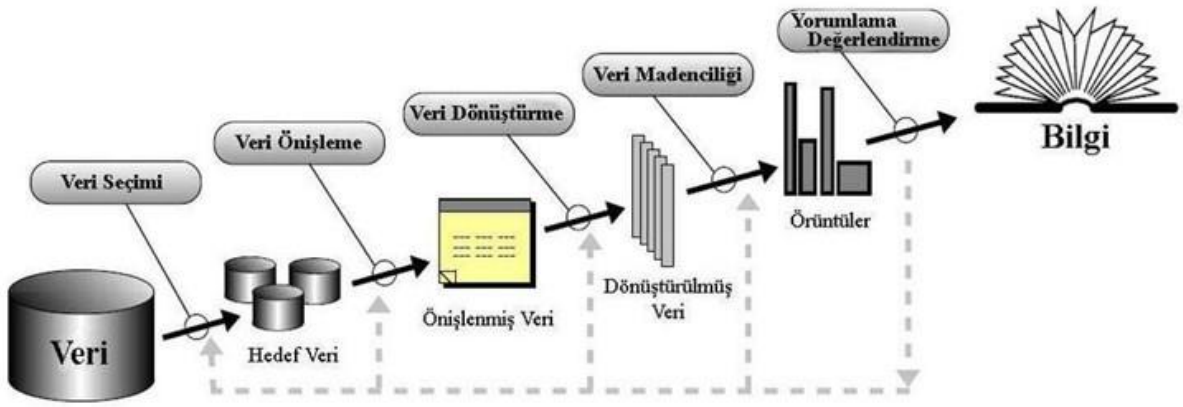
Hazırlanmış olan veriler üzerinden, amaca uygun olan veri madenciliği algoritmalarının uygulandığı süreçtir. Büyük veri setlerinde gizli veya önceden bilinmeyen desenleri ve ilişkileri keşfetme sürecidir. İstatistiksel ve matematiksel tekniklerle bu verilerden anlam çıkarılmasını sağlar.

1.1.7. Desenler (Pattern Evaluation)

Birtakım ölçümler yapılarak elde edilen bilgiyi temsil eden örüntüler tanımlanır. Desen değerlendirmesi, veri madenciliği sonuçlarını değerlendirme sürecini ifade eder. Elde edilen desenlerin anlamlılığı ve kullanılabilirliği üzerine yapılan analizlerle değerlendirme gerçekleştirilir.

1.1.8. Bilgi Sunumu (Knowledge Presentation)

Elde edilen bilginin kullanıcıya sunulmasıdır. Analiz edilen verilerden elde edilen önemli bilgilerin etkili bir şekilde iletilmesini içerir. Grafikler, raporlar veya interaktif araçlar kullanılarak elde edilen bulgular paylaşılır (5,6,7).



Şekil 1. Veri Madenciliği Adımları (8)

1.2.Veri Madenciliği Modelleri

Veri madenciliği modellerinden sınıflandırma (classification), kümeleme (clustering) ve birliktelik analizi (association analysis) (9,10) gibi modeller siber suçlarda sıklıkla kullanılabilmektedir (Şekil 2).

1.2.1. Sınıflandırma Yöntemi

Veri madenciliği alanında en çok kullanmakta olan yöntemlerden bir tanesidir ve veri tabanlarında bulunan gizli örüntülerin açığa çıkarılması amacıyla kullanılmaktadır. Bu açığa çıkarma noktasında eldeki veri veya verilerin sınıflandırılması konusunda belirli bir sürecin izlenmesi gerekir. Verileri sınıflandırabilmek için önce verilerin bir kısmını ayırmak ve bunu eğitim amacıyla kullanarak sınıflandırma kurallarını oluşturmak gerekmektedir. Bu kurallar uygulanarak yeni bir durum oluştuğunda modelin nasıl karar vereceği belirlenmelidir (8, 11).

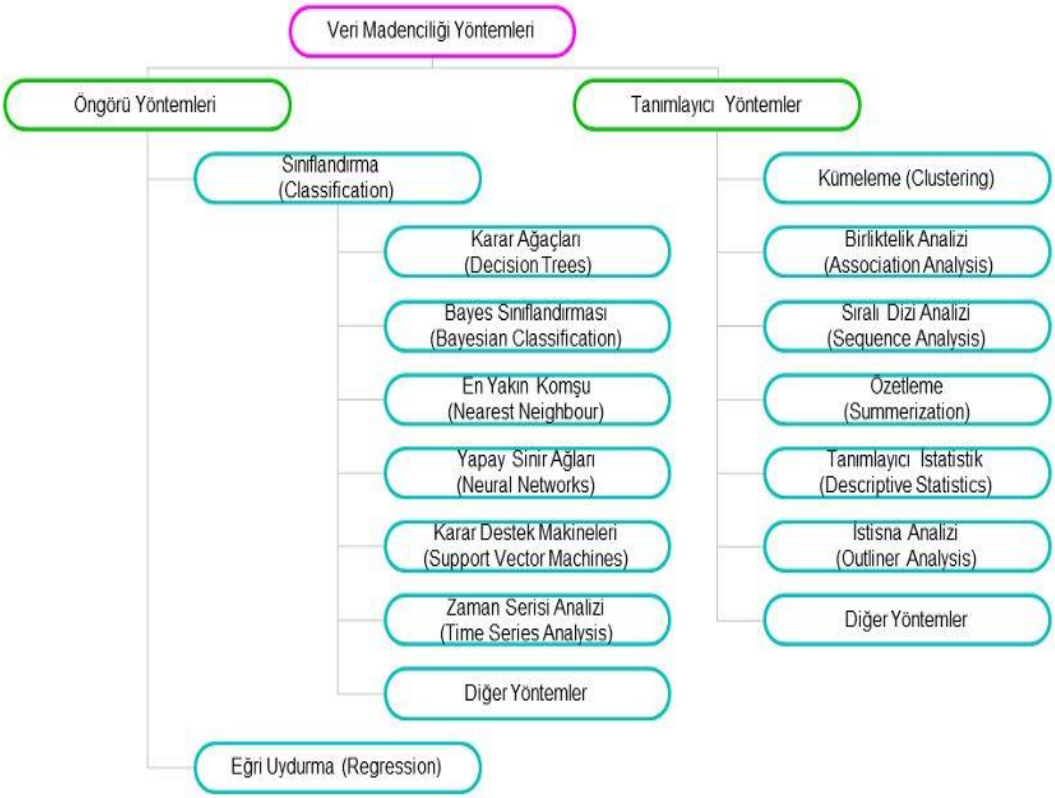
1.2.2.Kümeleme Yöntemi

Küçük veri setleri veya öznitelik setlerinden denetimsiz bir şekilde, yani doğal yollarla oluşan altsınıfların bulunduğu veya otomatik olarak oluştuğu sisteme denir (12). Ancak öznitelik sayısı arttığında, kümeleme problemi daha da zorlaşacak ve insan zihninin baş edemeyeceği bir seviyeye gelecektir. Günümüzdeki veri setleri, tipik olarak onlarca boyut içermekte ve öznitelikler arasındaki olası ilişkileri anlamayı ve gruplar oluşturmayı zorlaştırmaktadır (13).

1.2.3.Birliktelik Analizi Yöntemi

Çok büyük veri kümelerinin analiz edilerek birbirleri arasında olan ilginç birliktelik ilişkilerini veya korelasyonları bulabilmek için kullanılan yönteme denir. Korelasyon, temel anlamda iki ya da daha fazla değişken arasındaki ilişkiyi göstermek için kullanılmaktadır. Veri kümesinin içinde çok sık görülen birliktelikleri tespit etmek ve buna göre hareket etmek büyük verilerin analizinde zaman kazandıracaktır (14).

Kısaca özetlemek gerekirse, elde edilen büyük miktardaki verileri aynı sınıf ve aynı kümede olacak şekilde gruplandırabilmek ve sonrasında birbiriyle ilişkili öğeleri tespit ederek verileri bilgiye dönüştürmek veya bu yöntemleri ayrı ayrı ele alarak sonuca gidebilmek mümkündür.



Şekil 2. Veri Madenciliği Yöntemleri (15)

1.3. Veri Madenciliğinin Siber Suçlarda Kullanımına İlişkin Bazı Örnekler ve Çözüm/ Önleme Önerileri

Bir şirkete ait verilerin, belirlenen hedefler kapsamında veri madenciliği yaptırılarak modelleme istenmesi neticesinde bu işi yapacak olan kişinin şirkete ait kritik bilgileri ele geçirme ihtimali çok yüksektir. Çıkardığı sonuç ve tahminleri rakip şirketlere veya kamuoyuna açıklamak ya da sızdırmak suretiyle şirkete büyük zararlar verebilir. Bu durumun önüne geçebilmek için güvenilir olmayan şahıs veya firmalar ile çalışılmamalı, gizlilik anlaşması yapılmalı ve verilerin içerisine belirli bir oranda gürültü eklenmelidir.

Kurumda yeni işe başladığını ve bir oturuma giriş yaparak güncelleme yapmak istediğini belirten birinden telefon veya e-posta yoluyla bir talep alındığında, şifre paylaşımı yapılması ciddi güvenlik risklerine yol açabilir. Bu durumda, yalnızca yetkilendirilmiş kişilerin erişebileceği bilgilere izinsiz erişim sağlanabilir ve bu bilgiler kötüye kullanılabilir. Bu tür risklerin önlenmesi için şifrelerin paylaşılmaması, yetkilendirme süreçlerinin bilmesi gereken prensibine uygun olarak yürütülmesi ve gizlilik derecesi yüksek belgelerin güvenli koşullarda (dijital ya da fiziksel) saklanması gereklidir. Ayrıca, sistem yöneticilerinin admin yetkileri sayesinde gerekli durumlarda erişim sağlayabilecekleri ve bu nedenle bireysel şifrelere ihtiyaç

duymayacakları unutulmamalıdır. Bu yaklaşımlar, bilgi güvenliğinin sağlanması ve olası ihlallerin önlenmesi açısından kritik önem taşımaktadır.

Dışarıda bulunulan bir zamanda kurumdan gelen acil bir e-posta kontrol edilmek istendiğinde, bulunulan ortamın ortak internet bağlantısının kullanılması durumunda bilgi ve belge güvenliğinin tehlikeye girmesi muhtemeldir. Bu tür bir durumda, birkaç parça dahi olsa veri sızıntısı yaşanması halinde, birey ya da kurumla ilgili önemli bilgi ve verilerin ele geçirilmesi mümkün olacaktır. Bu riskin önlenmesi için, acil durumlarda dahi ortak internet bağlantılarının kullanılmaması gerektiği unutulmamalıdır.

Tanımadık bir kişi tarafından cep telefonunun kısa bir arama yapmak veya mesaj göndermek amacıyla kullanılmasının talep edilmesi ve bu talebin kabul edilmesi durumunda, telefon içerisinde bulunan verilerin yalnızca birkaç saniye içinde çalınması mümkün hale gelebilir. Bu nedenle, her ne sebeple olursa olsun, cep telefonlarının tanınmayan kişilere verilmemesi gerektiği unutulmamalıdır.

Mesaj, e-posta veya sosyal medya üzerinden gönderilen bağlantılara tıklanması durumunda cihazlara zarar verilmesi ve kişisel ya da kurumsal bilgilere erişim sağlanması mümkün olabilir. Bu nedenle, kaynağı bilinmeyen ya da şüpheli bulunan bağlantıların kesinlikle açılmaması gerektiği unutulmamalıdır.

Bu konuda işlenen suçlara elbette daha fazla örnek mümkündür ve ne yazık ki yeni yöntemler de eklenmeye devam edecektir. Ancak bu çalışmada konu hakkında farkındalık oluşturmak amaçlanmıştır.

1.4. Bilişim Hukuku Açısından İnceleme

Veri madenciliğinin kötüye kullanılması nedeniyle kişiye ait verilerin yasal olmayan yollar ile elde etmek, buradan haksız fayda sağlamak veya kişiyi maddi ve manevi zarara uğratmak mümkündür. Bu durumda işlenen suçlar Siber Suç kapsamında değerlendirilmektedir ve Türk Ceza Kanunu'nda bu tip suçlardan bazıları için doğrudan madde olsa da bazıları için de uyarlama yapılmıştır ve bu nedenle kaçış yolu bulmak mümkün olabilmektedir. İlgili maddeler 1.5'te verilmiştir.

1.5. Türk Ceza Kanunu İlgili Maddeleri

Madde 124- Haberleşmenin engellenmesi
Madde 132- Haberleşmenin gizliliğini ihlal
Madde 133- Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması
Madde 134- Özel hayatın gizliliğini ihlal

Madde 135- Kişisel verilerin kaydedilmesi

Madde 136- Verileri hukuka aykırı olarak verme veya ele geçirme

Madde 138- Verileri yok etmeme

Madde 142- Nitelikli hırsızlık

Madde 158- Nitelikli dolandırıcılık

Madde 226- Müstehcenlik

Madde 243- Bilişim sistemine girme

Madde 244- Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Madde 245 – Banka veya kredi kartlarının kötüye kullanılması

Madde 245/A- Yasak cihaz veya programlar (16).

1.6. Literatürde Veri Güvenliği

Veri güvenliği ve kişisel veri koruma konuları, dijital platformların ve teknolojinin hızlı gelişimiyle birlikte önemli bir tartışma konusu haline gelmiştir. Özellikle Cambridge Analytica olayı, kişisel verilerin etik dışı kullanımını vurgulayarak bu alandaki düzenlemelerin ve koruma mekanizmalarının eksikliklerini ortaya koymuştur. Bu bağlamda, mevcut yasal düzenlemelerin, hızla evrilen teknolojiye etkin bir şekilde adapte olamaması ve belirsizliklere yol açması önemli bir sorun teşkil etmektedir.

Avrupa'da Genel Veri Koruma Düzenlemesi (General Data Protection Regulation-GDPR) ve Türkiye'de Kişisel Verilerin Korunması Kanunu gibi mevzuatlar, kişisel verilerin korunması amacıyla adımlar atmıştır. Ancak, bu düzenlemelerin teknolojik değişimlere uyum sağlamada sınırlı kaldığı ve veri toplama işlemlerine yeterince nüfuz edemediği ifade edilmektedir. Yeni gelişen teknolojilerle birlikte ortaya çıkan belirsizlikler, mevcut yasal korumanın yetersiz olduğu ve kişisel veri güvenliğinin sağlanmasında daha etkin önlemlerin alınması gerektiği konusunda bir ihtiyaca işaret etmektedir (17). Ayrıca, bazı ülkelerde hükümetlerin sosyal medya platformlarına erişimi kısıtlaması, dijital özgürlük ve bilgi akışı konularında yeni bir tartışma açmıştır. Otoriter yönetimlerin kontrolündeki dijital araçlar, bilgi akışını yönetme ve sosyal kontrol mekanizması olarak kullanılarak dijital Çin Seddi gibi sistemler ortaya çıkmıştır (18, 19). Bu bağlamda, kişisel veri güvenliği ve dijital özgürlükler arasındaki denge, teknoloji ve hukuk alanında yeni yaklaşımları gerektiren karmaşık bir konu olarak karşımıza çıkmaktadır. Hukuki düzenlemelerin teknolojik gelişmelere uygunluğu, bilgi güvenliği politikalarının etkinliği ve dijital özgürlüklerin sınırları gibi konular detaylı bir şekilde ele alınması gerektiği değerlendirilmektedir.

Of ve Kılıçaslan (2023) çalışmasında günümüzde işletmelerin giderek dijitalleşen ortamlarda faaliyet göstermeleri nedeniyle veri güvenliğinin kritik bir önem arz ettiğini ele almakta, bu bağlamda işletmelerin karşılaştığı güvenlik risklerine vurgu yaparak alınması gereken tedbirleri tartışmaktadır. Gelişmiş güvenlik yazılımları ile güvenlik duvarları ve veri şifreleme teknolojilerinin kullanılmasının, işletmelerin ağlarını koruma konusunda etkili olduğunu belirtmişlerdir. Ayrıca düzenli güvenlik denetimlerinin yapılmasının, siber tehditlere karşı direnci artırabileceğini vurgulamışlardır (20).

Ateş (2019) dijital dönüşüm süreçlerinin suç alanında yarattığı etkileri ve ortaya çıkan güvenlik zorluklarını ele almıştır. Ayrıca, dijitalleşen dünyanın getirdiği yeni suç türlerini ve bu suçlarla mücadelede kullanılan güvenlik stratejilerine dikkat çekmiştir. Dijitalleşme ile siber saldırılar, kimlik hırsızlığı, veri manipülasyonu ve diğer dijital yöntemlerle gerçekleştirilen suçlar öne çıkmaktadır. Bu suç türlerinin teknolojik gelişmelerle birlikte nasıl evrildiği ve gelişen savunma mekanizmalarına karşı nasıl adapte oldukları detaylı bir şekilde ele alınmıştır (21). Efe (2016) çalışmasında, bilişim hukuku alanındaki sorunlara odaklanarak, yapılan literatür taraması sonuçlarına dayanarak bir dizi temel sorunu tanımlamıştır. Bu sorunlar arasında; elektronik verilerin ticarileştirilmesinde yaşanan zorluklar, arama motorlarının sorumluluğu ve internet hukukundaki problemler, internet sansür ağının oluşumu, sosyal medya aracılığıyla işlenen suçların artışı, siber zorbalık, kişisel bilgilerin korunamaması, mahremiyet ihlali, siber suç tanımının eksikliği, klasik ceza hukukunun yetersizliği, ulusal sınırların belirlediği hukuk anlayışının yetersiz kalması, bilgi kaynaklarına uzaktan erişim, fikri mülkiyet, kullanıcı gizliliği, bilgi bütünlüğünün sağlanması, e-imza altyapısının yetersizliği, bulut bilişim güvenliği eksikliği, adli bilişimin gelişim eksikliği, internet sitesi erişim engelleme kararlarının etkinliğinin sorgulanması, teknoloji aracılığıyla suç işlenmesindeki zorluklar ve kara para aklama ile terörizmin finansmanında kullanılan sistemlerin etkili bir şekilde kontrol edilememesi gibi konular yer almaktadır (22). Bu belirlenen temel sorunların özü, ulusal, kurumsal ve kişisel düzeyde çeşitli risklerle bağlantılıdır. Bulut bilişimin yaygınlaşması, ulusal egemenlik, hukuki ve etik yaklaşım, siber istihbarat, paralel yapılanma ve siber kapitalizm gibi riskler, bilişim hukukunun karşılaştığı geniş bir risk yelpazesini temsil etmektedir. Bu risklerin aşılabilmesi için güçlü bir siber mücadele alt yapısının, derin farkındalığın, etkin koordinasyonun, güvenlik ve güvenilirliği sağlayacak araçların entegrasyonunun ve mevzuatın sürekli güncellenmesinin önemine vurgu yapılmıştır.

2. SONUÇ VE ÖNERİLER

Gelişen teknoloji ve sistemler doğrultusunda ortaya çıkan yenilikler ve hızla çoğalan yeni suç yöntemleri göz önünde bulundurularak, özellikle internet ortamında atılacak adımların dikkatle planlanması gerekmektedir. Kişisel verilerin veya bu verilere ulaşılmasını sağlayabilecek bilgilerin paylaşılmaması konusunda özen gösterilmelidir. İyi niyetle yapılan bir paylaşımın ya da veri aktarımının bireylere, kurumlara veya topluma zarar verebileceği her zaman dikkate alınmalıdır. Kötü niyetli veri madenciliği yapan kişilerin, en küçük verilere dayanarak tüme varım yoluyla daha büyük bilgilere ulaşabilecekleri unutulmamalıdır.

Sanal bir dünyada kişinin hareketlerini analiz eden ve kişinin kendisi gibi düşünen dijital bir model oluşturmanın mümkün olduğu ve bu yüzden de kişinin sonraki hamlelerinin tahmin edilebileceği artık hayal olmaktan öte kaçınılmaz bir gerçeklik olarak karşımıza çıkmaktadır.

Türk Ceza Kanunu'nda siber suçlar konusunda maddeler bulunsa da yeni ve dinamik bir alan olması sebebiyle bu konular üzerine daha fazla düşünülmeli, önleyici ve caydırıcı tedbirler konusunda çözümler üretilmelidir. Çeşitlenen suç ve suç yöntemleri için daha ayrıntılı ve suça özel maddeler, siber suçlarla ilgili kanun maddelerini hayata geçirmiş olan farklı ülkelerin yasaları ve ülkemizde yapılmış olan akademik çalışmalar ışığında yeni maddeler eklenmesi düşünülmelidir. Yine diğer ülkelerin siber suçlara karşı uyguladıkları önleyici politikalarının incelenmesinin faydalı olacağı değerlendirilmektedir.

Önemsiz gibi görünen küçük ayrıntılardan, veri madenciliği konusunda uzman kişiler tarafından bilgi üretilme ihtimalinin bulunması, istenmeyen sonuçların ortaya çıkmasına neden olabilmektedir. Bu durumun önlenmesi için gerekli dikkat gösterilmeli ve tedbirler elden bırakılmamalıdır. Güvenliği merkezine alan bir savunma anlayışının benimsenmesi, bu anlayışın siber suçluların suça yaklaşımına paralel bir yapıda olması gerektiği göz önünde bulundurulmalıdır. Ayrıca, belirlenen stratejinin sabit bir yapıya sahip olmaması ve yeni ortaya çıkabilecek tehditlere karşı koyabilecek şekilde dinamik bir yapıda tasarlanması gerektiği unutulmamalıdır.

Örneklerden de anlaşılacağı üzere, en zayıf halkanın insan olduğu göz önünde bulundurularak, güvenlik açısından bazı basit ancak önemli tedbirlerin alınması gerekmektedir. Bu bağlamda, güçlü parolaların kullanılması ve kimseyle paylaşılmaması, parolaların belirli periyotlarla tahmin edilmesi zor olacak şekilde değiştirilmesi, kaynağı bilinmeyen ya da şüpheli görülen uygulama ve bağlantılardan uzak durulması, kurum içinden sosyal medya paylaşımı yapılmaması ve konum bilgisinin kullanılmaması, özellikle gizlilik derecesine sahip evrak ve belgelerle ilgili gerekli güvenlik önlemlerinin alınması, Bilmesi Gereken Prensibi'ne uygun

şekilde hareket edilmesi ve kurum ya da şirket tarafından belirlenen güvenlik önlemlerinin ihlal edilmemesi gerektiği unutulmamalıdır.

Gelişen teknoloji ve suç metodlarındaki değişim, güvenlik güçlerinin mücadele stratejilerini revize etme ihtiyacını ortaya koymaktadır. Bu bağlamda, mevcut yasal çerçevelerin değiştirilmesi, güvenlik güçlerinin sadece mevcut suçlara reaktif değil, aynı zamanda potansiyel suçları proaktif bir şekilde önlemeyi amaçlayan bir anlayışla eğitilmesini gerektirmektedir. Günümüzde, geçmişte etkili olan güvenlik stratejilerinin artık yetersiz kaldığı kabul edilmelidir.

Dijital platformda ortaya çıkan suçlar, sürekli olarak evrilen bir risk oluşturmakta ve bu suçlara etkili bir müdahale proaktif yöntemlerle sağlanmadığı takdirde, maddi ve manevi zararlara yol açmaktadır. Bu noktada, güvenlik güçlerinin yeni teknolojik gelişmelere uyum sağlayarak, bu gelişmelerin temelindeki sorunlara karşı uzmanlaşması büyük önem taşımaktadır.

Geleceğin güvenlik stratejilerini inşa etmek adına geçmişteki yaklaşımları değiştirmek, cesaret gerektiren bir adımdır. Bu nedenle, uluslararası ve ulusal düzenleyici kuruluşlar, akademik kurumlar ve ticari kuruluşlarla iş birliği yaparak kolektif bir çaba harcamak, güvenlik güçlerinin bu yeni paradigma içinde etkili olmalarını sağlamak açısından hayati bir gerekliliktir.

Dijital dönüşüm ve bilgi teknolojilerindeki hızlı ilerleme, veri madenciliği gibi tekniklerin yaygın olarak kullanılmasına yol açmıştır. Veri madenciliğinin kötüye kullanımı, bireylerin gizliliğini ve güvenliğini tehdit eden bir dizi sorunu beraberinde getirmektedir. Veri madenciliği, bireylerin çevrimiçi davranışlarını, tercihlerini ve alışkanlıklarını analiz etmek için kullanıldığında, bu verilerin izinsiz bir şekilde toplanması, gizlilik ihlallerine neden olabilir. Bu durum, bireylerin kişisel ve hassas bilgilerinin yetkisiz kişiler tarafından ele geçirilmesi riskini artırabilir. Kullanıcı davranışlarına dayalı olarak profil oluşturabilir. Bu profillemeler, kişilere özel hedefleme, ayrımcılık ve manipülasyon için kullanılabilir. Özellikle, etnik köken, cinsiyet, dini inançlar gibi hassas özellikler üzerinden yapılan profillemeler, toplumsal sorunlara neden olabilir. Veri madenciliği algoritmaları, kullanılan veri setlerinin yanlılık içermesi durumunda adaletsiz sonuçlara yol açabilir. Eğitim verilerindeki önyargılar, algoritmaların kararlarında yanlılıklara neden olabilir ve bu durum, toplumsal adaleti zedeleyebilir.

Veri madenciliğinin kötüye kullanımının yanı sıra, mevcut bilişim hukuku çerçevesindeki yetersizlikler de endişe vericidir. Hukuki düzenlemeler, teknolojik gelişmelere

ve veri madenciliği uygulamalarındaki yeniliklere etkin bir şekilde ayak uyduramamaktadır. Bu noktada, aşağıdaki temel gerekçeler makale konusunu desteklemektedir:

Bilişim hukukunda, özellikle veri madenciliği alanında, mevcut yasal düzenlemelerin teknolojik gelişmelere paralel olarak güncellenme eksikliği mevcuttur. Bu durum, hukuki boşlukları ve uygulamada belirsizlikleri beraberinde getirmektedir. Bilişim hukukundaki mevcut çerçeve, bireylerin temel hak ve özgürlüklerini yeterince korumamaktadır. Veri madenciliği uygulamalarının bireylerin özel yaşamlarına müdahalesi karşısında, bu hakların etkin bir şekilde korunması adına hukuki mekanizmaların eksik olduğu söylenebilir. Veri madenciliği, sınır ötesi etkileşimler içerdiğinden, uluslararası düzeyde standartlar ve iş birliği eksikliği, bu faaliyetlerin kötüye kullanımını önlemeyi ve düzenlemeyi zorlaştırmaktadır.

Bu gerekçeler ve mevcut eksiklikler, veri madenciliğinin kötüye kullanımının yanı sıra bilişim hukukundaki yetersizliklerin önemli bir sorun teşkil ettiğini ortaya koymaktadır. Bu bağlamda, akademisyenlerin ve konu uzmanlarının, sistemdeki eksikliklerin tespitine yönelik daha kapsamlı araştırmalar yapmaları, bu doğrultuda tespit, çözüm ve önerilerini ortaya koymaları önemli bir katkı sağlayacaktır.

KAYNAKLAR

1. Shafiulla, S. M., & Gopinath, V. (2020). Role of data mining in malware detection., *Journal of Information and Computational Science*., 10 (7).

2. İşür, Ş. (2021). Bilişim hukuku, unutulma hakkı ve bilgi asimetrisi üzerine. *Türkiye Medya Akademisi Dergisi*, 1 (2), 82-111.

3. Dalaz, S. (2021) Kişisel verilerin dijital yöntemler ile hukuka aykırı elde edilmesi, *Ahkâm Aktüel Hukuk Dergisi*, 1, 60-68.

4. Oğuz, H. (2013). Elektronik ortamda kişisel verilerin korunması, bazı ülke uygulamaları ve ülkemizdeki durum. *Uyuşmazlık Mahkemesi Dergisi*, 0 (3) , 1-38.

5. Lei-da Chen, T. S., & Frolick, M. N. (2000). Data mining methods, applications, and tools. *Information Systems Management*, 17 (1), 67-68.

6. Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI Magazine*, 17 (3), 37-37.

7. Çelik, D. (2015). Veri Madenciliği Kullanarak Akıllı Reklam/Anket Uygulaması. Yayınlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi.

8. Özcan, C. (2014). Veri Madenciliğinin Güvenlik Uygulama Alanları ve Veri Madenciliği ile Sahtekarlık Analizi. Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi.

9. Savaş, S., Topaloğlu, N., & Yılmaz, M. (2012). Veri madenciliği ve Türkiye'deki uygulama örnekleri. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 11 (21), 1-23.

10. Han J., Kamber M., Pei J., (2012), *Data mining concepts and techniques*, 3rd Edition, Morgan Kaufmann Publishers, Waltham. Syf. 108.

11. Özekes, S. (2003). Veri madenciliği modelleri ve uygulama alanları. *İstanbul Ticaret Üniversitesi Dergisi*, 67-67.

12. Irmak, S. (2009). Veri Madenciliği Yöntemleri ve Sağlık Sektörü Veritabanlarında Bilgi Keşfi: Tanımlayıcı ve Kestirimci Model Uygulamaları. Yayınlanmamış Doktora Tezi, Akdeniz Üniversitesi.

13. Tang, Z., & Maclennan, J. (2005). *Data mining with SQL Server 2005*. John Wiley & Sons. Syf. 6.

14. Şen, F. (2008). Veri Madenciliği ile Birliktelik Kurallarının Bulunması. Yayınlanmamış Yüksek Lisans Tezi, Sakarya Üniversitesi.

15. Demir, B. (2021). Veri madenciliği yöntemleri. Erişim Tarihi: 21.10.2023 https://mektebiendustri.com/index.php/2021/07/17/veri-madenciligi-yontemleri/

16. Türk Ceza Kanunu (2023). Türk Ceza Kanunu. Seçkin Yayıncılık, Ankara.

17. Wachter, S. (2019). Data protection in the age of big data. *Nature Electronics*, 2 (1), 6.

18. Bolsover, G., & Howard, P. (2018). Propaganda in Europe, The US, and China. *Drums: Distortions, Rumours, Untruths, Misinformation, and Smears*, 61-81.

19. Sanovich, S. (2017). *Computational propaganda in Russia: The origins of digital misinformation* (S. Woolley & P. Howard, Eds.; Computational Propaganda Worldwide, pp. 1–25). Computational Propaganda Project.

20. Of, M., & Kılıçaslan, İ. (2023). İşletmelerde veri güvenliğinin önemi: Alınması gerekli tedbirler. *International Journal of Social and Humanities Sciences Research (JSHSR)*, 10(101), 3219-3227.

21. Ateş, E. C. (2019). Suç 4.0: Dijital suç ve güvenlik. *Dijital Dönüşüm Trendleri*, 258-284.

22. Efe A (2016) Bilişim hukuku alanındaki sorunlar ve risklerin mevzuat boyutuyla analiz ve çözümlemesi. *Türk Noterler Birliği Hukuk Dergisi* 3(1):175–209