DEU FMD 26(76) (2024) 173-191

Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi
Dokuz Eylul University Faculty of Engineering Journal of Science and Engineering
Elektronik/Online ISSN: 2547-958X

ARAŞTIRMA MAKALESI / RESEARCH ARTICLE

KVKK Kavramlarının Modellenmesi için Ontoloji Tabanlı Bir Yaklaşım

An Ontology Based Approach for Modelling KVKK Concepts

Emre Atlıer Olca [1]*, Özgü Can [2]

[1] Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Yazılım Mühendisliği Bölümü, İstanbul, TÜRKİYE
[2] Ege Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İzmir, TÜRKİYE

Sorumlu Yazar / Corresponding Author *: emreolca@maltepe.edu.tr

Öz

Bilgi ve iletişim teknolojilerinin hızlı gelişimi kişisel verilerin paylaşılmasını ve daha kolay yayılmasını sağlamaktadır. Kişisel verilere olan erişim kolaylığı, kişisel mahremiyeti ve veri güvenliğini tehdit etmektedir. Veri gizliliğini ve güvenliğini sağlamak için 2016 yılında 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) kabul edilmiştir. Anayasa'nın 20. maddesi, Türk Ceza Kanunu, Türk Medeni Kanunu gibi bazı yasal çalışmalarda kişisel verinin korunmasına yönelik maddeler bulunsa da konuyu bütüncül olarak ele alan tek çalışma 6698 sayılı kanundur. Bu kanuna göre, kişisel verinin kullanımı kişinin onamına bağlıdır. Etkili bir onam yönetiminin sağlanabilmesi için veriye erişim bilgilerini ve erişim kurallarını tutan politikaların paylaşımı gereklidir. Bu çalışma kapsamında, Genel Veri Koruma Tüzüğü (General Data Protection Regulation - GDPR) ve KVKK kavramları karşılaştırılmakta ve KVKK metni analiz edilerek KVKK kavramları çıkarılmaktadır. Ayrıca, KVKK kavramlarını temel alan onam modeli ontoloji tabanlı bir yaklaşım ile geliştirilmekte ve Anlamsal Web teknolojileri tabanlı bir onam yönetim sistemi önerilmektedir.

Anahtar Kelimeler: *Mahremiyet, Onam, Gizlilik, Ontoloji, Anlamsal Web, KVKK*

Abstract

The rapid development of information and communication technologies enables the sharing and dissemination of personal data more easily. The ease of access to personal data threatens personal privacy and data security. In order to ensure data privacy and security, the Personal Data Protection Law No. 6698 (KVKK) was adopted in 2016. Although there are articles on the protection of personal data in some legal studies such as the 20th article of the Constitution, the Turkish Penal Code, the Turkish Civil Code, the only study that deals with the issue as a whole is the Law No. 6698. According to this law, the use of personal data depends on the consent of the person. In order to ensure an effective consent management, it is necessary to share the policies that hold data access information and access rules. Within the scope of this study, the General Data Protection Regulation (GDPR) and KVKK concepts are compared and the KVKK concepts are extracted by analyzing the KVKK text. In addition, the consent model based on KVKK concepts is developed with an ontology-based approach and a Semantic Web technologies-based consent management system is proposed.

Keywords: *Privacy, Consent, Confidentiality, Ontology, Semantic Web, KVKK*

EXTENDED ABSTRACT

Introduction

In our digitized world, the omnipresence of digital technologies has brought unprecedented efficiency to daily life. However, the flip side of this convenience is the growing concern surrounding the unregulated accumulation of personal data, especially in realms like health, education, and social media. This prompts a critical examination of privacy safeguards, leading us to the Turkish Personal Data Protection Law (KVKK).

This study delves into the intricacies of the KVKK, enacted in 2016, and its pivotal role in upholding individual privacy rights. The legislative journey, beginning in 1988 and aligning with European data protection standards, culminated in the establishment of a comprehensive legal framework.

Acknowledging that personal data extends beyond conventional identifiers to include a myriad of information, the study emphasizes the need for robust protection measures.

Recognizing the potential threats posed by uncontrolled data processing, the study advocates for awareness and knowledge dissemination to individuals and institutions. A cornerstone of the KVKK is the requirement for explicit consent before accessing personal data. The research takes a comparative stance, juxtaposing the KVKK with the General Data Protection Regulation (GDPR) to distill key insights.

In response to the challenges posed by evolving data landscapes, the study proposes a forward-looking solution: a Semantic Web-based consent management system. This innovative model, rooted in KVKK principles, seeks to empower individuals to make informed decisions about their personal data. Leveraging Semantic Web technologies and ontologies, the system is designed for flexibility and adaptability across diverse domains.

This introduction lays the groundwork for a holistic exploration of personal data protection, legislative frameworks, and a cutting-edge approach to consent management. The study not

DOI:10.21205/deufmd.2024267620

Atıf şekli / How to cite:
Olca, E., Can, O. (2024). KVKK Kavramlarının Modellenmesi için Ontoloji Tabanlı Bir Yaklaşım. DEUFMD, 26(76), 173-191

Geliş Tarihi / Received: 10.09.2022
Kabul Tarihi / Accepted: 08.10.2022

only aims to address current challenges but also aspires to contribute meaningfully to the ongoing discourse on information technology, privacy, and data security.

Materials and Methods

The content entails a meticulous exploration into the development of a Consent Management System, deeply rooted in compliance with both the Turkish Data Protection Law (KVKK) and the General Data Protection Regulation (GDPR). The initial phase involves an intricate analysis of the KVKK text using the Term Frequency-Inverse Document Frequency (TF-IDF) method, elucidating pivotal terms such as " Personal Data" and their weighted significance.

The architectural framework of the system is introduced, elucidating pivotal actors, entities, and procedural workflows. At the heart of the model lies the acquisition of explicit consent, with a particular emphasis on the concept of " Explicit Consent". The TF-IDF method is systematically applied to gauge the importance of identified terms, playing a decisive role in shaping the Consent Management System.

The document seamlessly transitions into a broader legal context, underscoring the critical role of consent in safeguarding personal data within the ambit of the KVKK. The operational sequence is visually represented through a System Sequence Diagram (SSD), offering a clear depiction of the stepwise procedures involved in responding to access requests for personal data.

Moreover, semantic solutions are introduced through ontologies, featuring the development of the KVKK Ontology, FOAF Ontology, and Relationship Ontology. These ontologies serve as foundational structures for expressing consent policies and ensuring seamless interoperability across diverse domains.

The proposal transcends the immediate KVKK framework, emphasizing the universal need for consent management across various sectors, including banking, healthcare, and energy. This underscores the adaptability and relevance of the system in diverse data processing environments. The integration of Semantic Web Rule Language (SWRL) rules further augments the system's capabilities by enabling rule-based reasoning, ensuring that consent-related decisions align meticulously with the specified regulations.

In essence, the content provides a comprehensive exploration of the Consent Management System's development, encompassing legal intricacies, architectural components, ontological solutions, and the broader ramifications of consent management across multifaceted domains.

Results and Discussion

The study unveils crucial insights derived from the term significance analysis, emphasizing the prominence of " Personal Data" in the analyzed KVKK context. The proposed Consent Management System architecture is delineated, featuring a System Sequence Diagram that illustrates the procedural flow in handling access requests. The development of ontologies, including KVKK Ontology, FOAF Ontology, and Relationship Ontology, is outlined as foundational structures for expressing consent policies, further strengthened by the integration of Semantic Web Rule Language (SWRL) rules. Noteworthy is the system's adaptability across diverse sectors, ensuring universal relevance in various data processing environments. The Discussion delves into legal compliance and ethical considerations, assessing the alignment with frameworks such as KVKK and GDPR. The study evaluates the effectiveness of ontologies in ensuring semantic interoperability and discusses practical implications, potential challenges, and future directions. Additionally, it explores the system's practical implications, potential challenges, and future research avenues, providing a comprehensive understanding of the proposed Consent Management System's implications and future prospects.

Conclusion

In conclusion, the text underscores the crucial need for a robust consent management system in ensuring the privacy and security of personal data, especially in the context of the comprehensive legal framework provided by the Personal Data Protection Law. The proposed Semantic Web-based solution emerges as a strategic response to the apparent lack of specific technical studies on consent management in Turkey. By analyzing the law using the TF-IDF method, the system's components are identified, and a layered MOF structure is presented, promising not only enhanced security but also semantic interoperability. Looking forward, the envisaged application for managing consents and the incorporation of an audit mechanism are pivotal steps in advancing the field of personal data protection in line with evolving legal and technological landscapes.

1. Giriş

Dijital teknolojiler günlük hayatın her alanına bütünleşmiş durumdadır. Bu durumun sonucunda, sistemlerin ve kişilerin erişilebilirliği artmakta ve kişiler bulundukları yerden işlerini yaparak zamandan tasarruf etmektedirler. Sağlık, eğitim, bankacılık sistemlerinin yanı sıra sosyal medya üzerinde kişi bilgilerinin tutulmasıyla kontrolsüzce toplanan büyük hacimli veri elektronik ortamda tutulmaktadır. Her geçen gün artan bu veri, sermayeleştirilerek kullanılmak istenmektedir. Kişiler zamandan tasarruf yaparken diğer yandan kişisel gizlilik ve siber korsanlık tehlikeleriyle karşılaşmaktadırlar. Bunun sonucu olarak, kişisel verilerin korunması önemli bir ihtiyaç haline gelmektedir.

Kişisel veri, gerçek kişiyle ilişkili olan bilgidir. Gerçek kişi tanımına bakıldığında ise kimliği belirli veya belirlenebilir olması gerekmektedir [1]. Bu kapsamda, kişisel veri kapsamında yalnızca kişinin adı, soyadı, kimlik numarası, doğum yeri bulunmamaktadır. Bunların yanında bu kişiyi doğrudan veya dolaylı olarak tanımlayabilen telefon numarası, adres gibi iletişim bilgileri, fotoğraf, video veya ses kayıtları gibi sosyal medya bilgileri, sosyal güvenlik numarası, pasaport numarası, genetik veri, hobileri, dernek / vakıf üyelikleri gibi veriler de kişisel veriler kapsamındadır [2].

Kişisel verilerin korunması temel bir haktır ve bu hak, temel kişisel hak ve özgürlükler arasında yer almaktadır. Kişinin mahremiyetinin korunması, demokrasinin güçlendirilmesi ve hukuk devleti ilkesi için önemlidir. Bu nedenle, kişisel veriler de dâhil olmak üzere, kişilerin özel hayatı Anayasa tarafından güvence altına alınmış durumdadır [1]. 2010 yılında Anayasa'ya 20/2 sayılı hüküm eklenmesi ile kişisel verilerin korunmasına ilişkin gerekli yasal dayanak oluşturulmuştur. Kişisel verilerin korunmasına yönelik çalışmalara, Adalet Bakanlığı tarafından 1988 yılında başlanmıştır. Kişisel Verilerin Korunması Kanun Tasarısı, 2003 yılında oluşturulan bir komisyon tarafından 2005 yılında Başbakanlık'a gönderilmiştir. Tasarı, 2008 yılında da TBMM'ne sevk edilmiştir. Bu tasarı, TBMM Adalet Komisyonu tarafından Şubat 2016'da kabul edilmiştir ve 6698 kanun

numarasıyla 26 Mart 2016 tarihinde yasalaşmıştır [1]. Bu kanun, 108 sayılı Avrupa Konseyi Sözleşmesi [3] ile 95/46/EC sayılı Veri Koruma Direktifine [4] paraleldir.

Kişisel verilerin kontrolsüz bir şekilde elde edilmesi ve işlenmesi, temel hak ve özgürlük ile birlikte özel hayatın gizliliğini de tehdit etmektedir. Buna göre, kişisel verilerin yasada belirtilen şartlara uygun olarak işlenmesi, veri sahiplerinin aydınlatılması, bu alanın denetlenmesi ve düzenlenmesi için bir otorite oluşturulması ve veri güvenliğine ilişkin gerekli önlemlerin alınması temel ilke olarak kabul edilmektedir. Bu konuyla ilgili olarak ortaya çıkabilecek sorunları en aza indirmek için bireyleri ve ilgili kurumları veri güvenliği konusunda bilgilendirmek ve bilinçlerini geliştirmek, farkındalığı arttırmak önemlidir.

6698 sayılı Kişisel Verilerin Korunması Kanunu'na (KVKK) göre kişisel veriye erişim için kişiden onam alınması gereklidir. Bu çalışma kapsamında, KVKK incelenmekte ve Avrupa Parlamentosu tarafından kabul edilen GDPR ile karşılaştırılmaktadır. Ayrıca kişinin mahremiyetini korumak amacıyla kişisel onam yönetimini gerçekleştirmesini sağlayan bir Anlamsal Web tabanlı çözüm önerilmektedir. Bu amaçla, KVKK'yı temel alan bir onam yönetim modeli sunulmaktadır. Anlamsal Web, ortak bir anlambilimi üzerine kurulu bir yapıdır ve makineler bu biçimsel anlambilimi kullanarak diğer makineler ile iletişim kurabilmektedir. Böylelikle, bilginin paylaşılması ve yeniden kullanımı sağlanmaktadır. Anlamsal Web, farklı terimleri açıklamak ve ortak tanımlamaları oluşturmak için ontolojileri kullanmaktadır. Bu çalışma kapsamında, ontolojiler kullanılarak mahremiyetin ve veri gizliliğinin korunması için alan (domain) bilgisinden bağımsız ve KVKK'yı temel alan bir onam yönetim sistemi önerilmektedir. Literatürde bilişim teknolojileri kapsamında, KVKK'yı temel alan benzer bir yaklaşım bulunmamaktadır. Bu nedenle, önerilen onam yönetim sistemi kişisel mahremiyeti korumak için 6698 sayılı KVKK'yı temel alan özgün bir çalışma niteliğindedir.

Onam yönetimi, kullanıcılar tarafından verilen izinleri dikkate alarak kişisel verilere erişim yönetimi ile ilgilenir. Veri koruma düzenlemeleri açısından, onam yönetimi, kullanıcıların gizliliğinin korunmasında önemli bir role sahiptir. Bu çalışma kapsamında ortak alanın paylaşılabilmesi için onam yönetimi sürecine anlamsal bir yaklaşım getirilmekte ve anlamsal onam yönetimi modeli önerilmektedir. Anlamsal Web, mevcut Web'in bir uzantısı olan Semantik Web'e dayanmaktadır. Semantik Web'de bilgi, bilgisayarların ve insanların işbirliği içinde çalışmasını sağlamak için iyi tanımlanmış bir anlamda verilir [5]. Anlamsal Web'in anlamlı verilerle ilişkilendirme hedefine ulaşmak için ontolojiler önemli bir rol oynamaktadır. Bir ontoloji, bir kavramsallaştırmanın açık bir belirtimi olarak tanımlanır [6]. Ontolojiler, ilgili alan içindeki kavramları ve bu kavramlar arasındaki ilişkileri tanımlayarak alan bilgisini temsil etmek için kullanılır.

Bu çalışmada, kişisel verilerin korunması için elektronik bir onam yönetimi sistemi yerine onam yönetimi alan bilgisinin tekrar kullanılabilirliğinin sağlanması ve paylaşılabilmesi için Anlamsal Web teknolojilerini kullanan ontoloji temelli anlamsal onam yönetimi modeli sunulmaktadır. Anlamsal çözümlerin kullanıldığı sistemlerde uygulamaların başarısı temel olarak alan ontolojisinin ne kadar iyi tasarlandığına bağlıdır. Anlamsal model kapsamında bir alan ontolojisi oluşturmak, heterojen sistemler ile iş alanındaki katılımcıların bilgi paylaşımını ve birlikte çalışabilirliğini önemli ölçüde arttırmaktadır. Alan ontolojileri, gerçek dünyadaki uygulama alanını kavramsallaştırır. Ontolojiler, bilgi temelli yazılım uygulamalarında çok önemli bir rol oynamaktadır. Çeşitli bilgi kaynaklarından gelen verilerin otomatik olarak anlamsal yorumlanmasını ve birlikte çalışabilirliği kolaylaştırır. Bir ontoloji, bilgi sistemlerinde alan bilgisini almak, saklamak ve çalışmak için etkili ve güçlü bir araç olarak kullanılabilmektedir. Bu nedenlerle, kişinin onamının kontrol edilmesi için bir anlamsal bir model geliştirilmiştir. Önerilen model, bireylerin kişisel bilgilerine kimlerin, hangi amaçlarla ve hangi koşullarda erişebileceğini belirlemek için gizlilik tercihlerini belirlemelerine olanak tanımaktadır. Bu amaçla, onam yönetimi sistemi oluşturulmuş ve bu sistem için Anlamsal Web teknolojileri kullanılarak onam ontolojileri geliştirilmiştir. Geliştirilen ontolojilerin Meta-Object Facility - MOF (Üst Nesne Çerçevesi) [7] yapısına göre yerleştirildiği katmanlar sunulmuştur.

Bu çalışmanın organizasyonu şu şekildedir: ikinci bölümde kişisel verinin korunmasına yönelik yapılan ulusal ve uluslararası hukuki çalışmalar verilmekte, KVKK'nın Avrupa Birliği tarafından yürürlüğe konulan Genel Veri Koruma Tüzüğü [8] ile bir karşılaştırılması sunulmakta; üçüncü bölümde KVKK ve dördüncü bölümde Anlamsal Web teknolojileri açıklanmaktadır. Beşinci bölümde KVKK'yı temel alan bir onam yönetim sistemi önerilmektedir. Altıncı bölümde onam yönetimine getirilen anlamsal çözüm yaklaşımı sunulmaktadır. Son bölüm olan yedinci bölümde ise çalışmanın sonucu sunulmakta ve gelecek çalışmalar anlatılmaktadır.

2. Materyal ve Metot

Kişisel verinin korunmasına yönelik hem ulusal hem de uluslararası alanda birçok hukuki çalışma yapılmaktadır. Ülkemizde ilgili kanun 2016 yılında kabul edilmiş olmasına rağmen Avrupa ve Amerika Birleşik Devletleri'nde ilgili çalışmaların çok önceden yapıldığı görülmektedir. Bu çalışmalar aşağıda sunulmaktadır. Ayrıca Tablo 1'de kapsadıkları konuların karşılaştırması verilmektedir.

2.1. Ulusal Çalışmalar

Kişisel veri tanımı yasalarda, mevzuatlarda, alanyazında birbirine benzer anlamlarda yapılmaktadır. Bu tanımlamalara bakıldığında temel olarak şu tanım ortaya çıkmaktadır: Elde edilen veri ya da veri topluluğundan veri sahibi kişiye ulaşılabiliyorsa bu veri ya da veriler kişisel veridir.

Türkiye'deki kişisel veri tanımına bakıldığında; Anayasanın 20. Maddesi Özel Hayatın Gizliliği başlığı altında "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." tanımı yapılmaktadır. Bu tanım ile kişisel veri koruma altına alınmakta ve bir hak olarak tanımlanmaktadır [1]. Kişisel verinin erişimi ve kullanımı için ise özel hayatın gizliliğinin dokunulamaz olduğu belirtilmekte ve kişisel veriye erişim için hâkim kararı ve yetkili bir merciin izni olmadıkça kişisel eşyasının aranamayacağı, el konulamayacağı tanımı yapılmaktadır. Daha sonra yapılan düzenleme ile 'kişinin açık rızası' ifadesi eklenmiştir. Kişinin verisinin sadece kişinin izni ya da kanunda belirtilen hallerde erişilebileceği / işlenebileceği vurgulanmaktadır. 20. Maddeye 2010 yılında eklenen ek fıkrada kişilerin kişisel verilerinin güvenliğinin sağlanmasını isteme hakkının bulunduğu belirtilmektedir. Bu hak kapsamında kişi, kişisel verilerinin silinmeni, düzeltilmesini talep edebilir, kendi verilerine erişebilir ve kişisel verileri hakkında her türlü bilgilendirme isteyebilir. 5237 sayılı Türk Ceza Kanunu'nun 134. - 138. Maddelerinde izinsiz olarak kişisel verinin işlenmesi suç olarak kabul edilmektedir [9]. Ayrıca kişisel veriler, Türk Medeni Kanunu'nun 23. ve 24. maddelerince de korunmaktadır [10].

Kişisel veri tanımı KVKK'da şu şekilde verilmektedir: "Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu bağlamda sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini

sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir." [11]. Ayrıca, araç plakası, telefon numarası, pasaport numarası, ses ve görüntü kayıtları, sosyal güvenlik numarası, resim, parmak izi, genetik bilgiler kişiyi belirlenebilir kılması nedeniyle kişisel veri olarak kabul edilmektedir.

Veri saklayan her sistem tuttukları kişisel verinin gizliliğini sağlamak zorundadır. Kişisel verinin gizliliğinin sağlanmasında hem Kişisel Verilerin Korunması Kanuna göre hem de uluslararası antlaşmalara göre kişinin onamı şarttır. Veriyi tutan sistemler de veri gizliliğini ve güvenliğini sağlamak için onam kontrol mekanizmasını işletmek zorundadır. Türkiye'de onam yönetimi ile ilgili çalışmalar Kişisel Verilerin Korunması Kanunu'nun kabul edilmesiyle hız kazanmıştır. Kanunun kabulü öncesinde kanun tasarısının değerlendirilmesi çalışmaları mevcuttur. Bu çalışmalardan biri 2016 yılında Ekonomi ve Dış Politika Araştırmalar Merkezi tarafından yapılan bir çalışmadır [12]. Bu çalışmada veri gizliliğinin önemi vurgulanmaktadır. Amerika Birleşik Devletleri, Rusya, Çin ve İran'da ve birçok Avrupa ülkesinde veri gizliliği üzerine var olan yasal çalışmaları analiz etmektedir. Sonrasında ise kanun tasarını hukuki boyutu üzerine değerlendirmektedir.

Kütükçü [13] ve Henkoğlu [14] tarafından sunulan çalışmalarda; KVKK'nın kabul edilmesine kadar yapılan hukuki çalışmalar anlatılmaktadır. Kişisel verilerin korunması için son 40 yıl içinde imzalanan uluslararası antlaşmalar ve gizliliğin sağlanmasına yönelik yapılan çalışmalar incelenmektedir. Sunulan bu çalışmaların kişisel verilerin gizliliğini sağlamak için yeterliliği sorgulanmakta ve teknik çalışmalar önerilmektedir. Henkoğlu'nun sunduğu çalışma, 6698 Sayılı Veri Koruma Kanunu'nu içerik analizi yöntemiyle incelemekte ve bu kanunun farklılıkları belirtilmektedir. Kütükçü tarafından sunulan çalışma ise mevzuatı ve mevzuat temelinde yaşanan süreci değerlendirmektedir.

Yildiz [15], kanunu genel hatlarıyla değerlendirmekte, kişisel veri tanımını kanuna göre yapmakta, kişisel verinin işlenmesini, transferini, veri sorumlusunun görevlerini tanımlamaktadır. [16], kişisel verilerin korunmasını 1985-2016 yılları arasını gözden geçirerek değerlendirmektedir. Türkiye ve diğer bazı ülkeler bazında karşılaştırmalar yapmakta, ortaya çıkan eşitsizlikleri değerlendirmektedir.

Altınok ve arkadaşları [17], çalışmalarında kişisel verilerin korunmasına ilişkin Türk yasaları ve mevzuatı analiz edilmekte ve mevcut durum uluslararası mevzuatlara uygunluk açısından değerlendirilmektedir. Kişisel Verilerin Korunması Kanunu'nun artılarının ve eksilerinin sunulduğu bu çalışmada, kişisel verilerin korunması üzerine yapılan hukuki çalışmalar sunulmakta ve koruma politikaları önerilmektedir.

Kartal [18], Türk Bankacılık sektörü üzerinden ilgili kanunu incelemektedir. Her sektörde olduğu gibi bankacılık sektöründe de kişisel verilerin gizliliği ve güvenliği kritik bir öneme sahiptir. Bu çalışmada, kişisel verilerin güvenliği ve gizliliği için kurum içi kontrol sistemlerinin kurulması gerektiğini vurgulanmaktadır. Çalışmaya göre sadece bankacılık sektöründe değil eğitim ve sağlık başta olmak üzere verinin saklandığı tüm alanlarda kişisel verinin korunması için gereken sistemlerin kurulması gereklidir [19].

2.2. Uluslararası Çalışmalar

Avrupa ve Amerika Birleşik Devletleri'nde hukuki çalışmalar 1970'li yıllarda başlanmış ve sonrasında teknolojik düzenlemelerin geliştirilmesine başlanmıştır. Avrupa'da var olan mevzuatlardaki kişisel veri tanımına bakıldığında; [20]'nin Rehber İlkelerinde kişisel veri, "Belirli veya belirlenebilir bir gerçek kişiye ilişkin tüm bilgiler" olarak verilmektedir. 108 Numaralı Avrupa Konseyi Sözleşmesinde [21] ve 95/46/EC numaralı Avrupa Birliği direktifinde [22] kişisel verinin tanımı yapılmakta ve neredeyse tanımların aynı olduğu görülmektedir. Bu tanımlarda kişisel tanımının gerçek bir kişiye ait olan tüm bilgiler olduğu belirtilmektedir. Kişisel veri, tek bir bilgi de olabileceği gibi, birbiriyle ilişkili bilgiler de olabilmektedir. Kişinin isim – soysisim, kimlik numarası, doğum tarihi gibi demografik bilgileri, adres ve telefon numarası gibi iletişim bilgileri, banka hesap numarası, parmak izi, kişisel bilgisayarından internete bağlanmış olduğu internet protokolü adresi ve hatta almış olduğu sağlık raporları kişisel veriye verilebilecek örneklerdir. Amerika Birleşik Devletleri'nde kritik olarak işaretlenen kurumsal veriler arasında kabul edilmektedir. Özel Yaşamın Gizliliği Kanunu hassas veriler için özel bir koruma getirmektedir. Bilgi Edinme Hakkı Kanununda kişisel verilerin üçüncü kişilere açıklanması yasaklanmıştır [23] [24].

Onam üzerine yapılan alanyazındaki çalışmalara bakıldığında da özellikle sağlık alanında birçok alanda çalışma yapıldığı görülmektedir. 2013 yılında Luger ve Rodden çalışmasında [25], teknolojinin gelişimiyle birlikte artan akıllı cihazların akıllı çevreleri oluşturduğu belirtilmektedir.

Akıllı çevrelerden, özellikle sensörlerden elde edilen kişisel bilgilerin kullanımı için kişilerin onamının gerekliliği vurgulanmaktadır. Gelişen teknolojide onamın var olması ve kullanılabilirliği için bu çalışmada anahtar prensipler önerilmektedir. Çok disiplinli çalışma alanlarında gelişen teknolojide onam kullanılabilirliğinin zorlukları aktarılmıştır. Gerçek zamanlı çalışan sistemlerde onam yönetiminin de gerçek zamanlı gerçekleşmesi gerektiği belirtilmiş ve pratikteki uygulama zorluğu anlatılmaktadır. İlgili çalışmada, elektronik onam yönetimi geliştiricilerine yönelik olarak: sistemlerin kullanıcı beklentileri ve kabul görmüş standartlar dikkate alınarak geliştirilmesi, bu sistemlerin üçüncü-partilerle bilgi alışverişine açık olması gibi öneriler sunulmaktadır.

Yu ve arkadaşlarının çalışmalarında [26], sağlık hizmeti sunan kurumların kullandıkları Elektronik Sağlık Kayıtları (ESK) sisteminin de kişinin onamını göre kişinin sağlık kayıtlarına erişimi gerçekleştirmesi gerektiğini vurgulanmaktadır. Bu gerekliliği rağmen Amerika Birleşik Devletleri sağlık endüstrisinin tamamen dijital ortama geçmesinin yanında onam sürecinin hala çoğunlukla kâğıt tabanlı olarak tutulduğu bilgisi verilmektedir. Elektronik olarak tutulan onam kayıtlarının ise sadece yasal zorunluluğu karşılamak için olduğu, kayıtların basit tutulduğu ve onam kayıtlarını dijital ortamda tutan sistemin gelişmiş özellikleri desteklemekten uzak olduğu belirtilmektedir. Ayrıca, kişinin onamını doğru olarak elde etmedeki hata, sağlık pratiklerindeki şikâyetlerde ilk on içerisinde yer almaktadır. Bunların sonucu olarak da elektronik onam sisteminin gerekliliği vurgulanmakta ve Elektronik Sağlık Kayıtlarında onam-tabanlı bir iş akışı kontrolü sistemi sunulmaktadır.

2016 yılında Amerika Birleşik Devletleri'nde yapılan bir patent başvurusunda, şirketler arasında onam kontrollü veri erişimini sağlamak üzere bir metot geliştirilmiş, bu metodu temel alan bir sistem üzerine çalışılmıştır [27]. Bu sistem, onam yönetimi modülünü içermektedir. Veriye erişim, kontrol seviyeleri ile gerçekleşmektedir ve bu kontrol seviyeleri verinin sahibi kişi, veri ve veriye erişim talep eden operatör ile ilişkilidir.

Anlamsal Web tabanlı onam yönetimi çalışmaları kapsamında; 2014 yılında Amerika Birleşik Devletleri'nde yapılan bu çalışma, askeri personelin ve ailelerinin sık sık görevleri nedeniyle yer değiştirmesi gerekliliğinden yola çıkılmıştır [28]. Çalışmada, askeri personel ve ailelerinin aldıkları sağlık hizmeti için

Tablo 1. Alanyazında yapılan çalışmaların karşılaştırması.

Table 1. Comparison of studies in the literature.

Yayın	Yıl	Elektronik Onam Yönetimi Sistemi	Onam Modelleri	Alan	Denetleme Mekanizması (Audit)
[12]	2016	Yok	Yok	Genel	Yok
[13]	2017	Yok	Yok	Genel	Yok
[14]	2017	Yok	Yok	Genel	Yok
[15]	2017	Yok	Yok	Genel	Yok
[16]	2017	Yok	Yok	Genel	Yok
[17]	2018	Yok	Yok	Genel	Yok
[18]	2018	Yok	Yok	Bankacılık	Yok
[19]	2016	Yok	Yok	Genel	Yok
[25]	2013	Yok	Yok	Genel	Yok
[26]	2014	Var	Yok	Sağlık	Var
[27]	2016	Var	Yok	Genel	Yok
[71]	2019	Var	Yok	Genel	Yok

yasaların eyaletlere göre değiştiğine vurgu yapılmakta ve bu değişen yasalara göre onam yönetiminin zorluğu vurgulanmaktadır. Sağlık kayıtlarının Elektronik Medikal Kayıt (EMK) sistemi içinde tutulduğu ve bu sistem içinde onamın alınmasının, doğrulanmasının ve onama göre davranılmasının yasal olarak zorunlu olduğu belirtilmektedir. Tedaviye ve ilaç kullanımına yönelik yasal zorunlulukların da eyaletlere göre değişmesinin de onam sürecinde bir zorluk yarattığı belirtilmektedir. İlgili çalışmada, ontoloji tabanlı bir çerçeve ve açık kaynak bir EMK sistemini kullanan bir prototip sunulmaktadır.

[29]'da, bilgilendirilmiş onam formunu veya HIPAA formunu imzalayan kişilerden elde edilen izinleri tanımlamak için, tek bir formatta, makine-yorumlanabilir, uygulama-bağımsız bir yol ile süreci yönetebilmek için izin ontolojisi geliştirilmiştir. Çalışmada amaç; uygulama tercihlerinden bağımsız olarak klinik veri ambarları ve biyo-depoları arasında bilgilendirilmiş onam izinlerinin ve HIPAA kısıtlamalarının paylaşımını ve birlikte çalışabilirliğini etkinleştirmektir. Ayrıca gelen erişim isteklerinin, onam ve HIPAA kısıtlarıyla olan uygunluğu için ontoloji tabanlı muhakeme yapılmaktadır.

Avrupa'da yapılan kişisel verinin korunmasına yönelik en güncel çalışma Genel Veri Koruma Tüzüğüdür [30]. GDPR Avrupa Parlamentosu tarafından kabul edilen ve 95/46/EC sayılı Veri Koruma Direktifinin yerini alan bir düzenlemedir [31]. GDPR, 14 Nisan 2016 tarihinde Avrupa Parlamentosunda kabul edilmiştir. Bu kapsamda GDPR, yürürlüğe girme tarihinden itibaren iki yıl içerisinde Avrupa Birliğine üye ülkelerin GDPR'a uyum sürecini tamamlamaları gerekmiştir. Bu düzenleme kişisel verilerin nasıl kullanılacağını konu almaktadır. Avrupa Birliğine üye ülke vatandaşlarının gizliliğini korumaya yönelik oluşturulan bir yasadır. Avrupa Birliği üye ülkelerde bulunan ve kişisel veriyi tutan tüm işletmeler, vatandaşlarının kişisel verilerin gizliliğini düzenlemede belirtilen kurallar çerçevesinde sağlamak zorundadır. Bu düzenleme 95/46/EC sayılı Veri Koruma Direktifine göre çok daha kapsamlı bir düzenlemedir ve cezalar, yetki alanları gibi konularda ciddi farkları mevcuttur.

GDPR yeni bir düzenleme olarak görülse de aslında kişisel veri gizliliği üzerine yapılan çalışmalar çok eskiye dayanmaktadır. 1950 tarihli Avrupa İnsan Hakları Sözleşmesi 8. Maddesi, 108 sayılı Avrupa Konseyi Sözleşmesi, 95/46/EC sayılı Veri Koruma Direktifi kişisel verilerin korunmasına yönelik daha önce yapılan çalışmalardır. 95/46/EC numaralı Direktif Avrupa Birliğine üye ülkeler için genel bir çerçeve sunmakta, her ülkenin kendi düzenlemesini yapmasına imkân vermektedir. Fakat GDPR tüm üye ülkelerin bu kanuna uyumunu zorunlu kılmaktadır. Şirketlerin uyum yükümlüğünün bulunması ile de şirketlerin bu uyum sürecini tamamlamaları için ciddi bir yatırım gerektirdiğini vurgulayan çalışmalar bulunmaktadır [32].

Alanyazında, metin üzerinden terim listesi çıkarılması üzerine yapılmış olan çeşitli çalışmalar bulunmaktadır. [33] çalışmasında, Federal Düzenlemeler Kanunu'nun 12. Başlığı olan Yiyecek ve İlaçlar [34] için doğal dil çalışmalarından olan alttan – üste (bottom-up) yaklaşımı kullanılarak CFR SKOS (Temel Bilgi Organizasyon Sistemi - Simple Knowledge Organization System) [35] sözlüğü geliştirilmiştir. SKOS, sınıflandırma şemaları, taksonomi gibi bilgi organizasyon sistemlerinin (KOS) kullanımını desteklemek için standartlar geliştiren bir çalışma alanıdır. [36] çalışmasında, Amerika Birleşik Devletleri kanunları ve düzenlemeleri Finansal Regülasyon Ontolojisi'ne (Financial Regulation Ontology - FinRegOnt) aktarılmıştır.

2.3. KVKK ve GDPR Karşılaştırması

GDPR, 11 bölüm 99 maddeden, KVKK ise 7 bölüm 33 maddeden oluşmaktadır. GDPR, 95/46/EC ve 95/46 direktifleri temel alınarak hazırlanmış olan KVKK'da da bulunan Veri Sorumlusu (Controller) ve Veri İşleyen (Processor) gibi temel aktörleri içermektedir. İki terimin benzerlik gösterdiği GDPR'da Veri İşleyene veri kaybı sonrasında KVKK'ya göre çok daha ağır hukuki sorumluluk yüklenmektedir. Ayrıca GDPR'da Veri Sorumlusu, Veri İşleyenlerin GDPR'a uyumluluğunu denetlemek zorundadır. GDPR'ın KVKK'ya göre temel farklarından biri uyumluluk yükümü üzerinedir. Şirketlerin uyumluluk yükümünün doğması için gerekli kriterler şunlardır:

- Avrupa Birliği üye ülkeler içerinde bulunması,
- Avrupa Birliği üye ülkeler içerisinde değilse Avrupa'da ikamet eden kişilerin kişisel verilerini işlemesi,
- 250'den fazla çalışanı olması,
- 250'den az çalışanı olduğu durumda belli özel nitelikteki kişisel verileri içermesi.

GDPR'ın koruma alanı KVKK'da olduğu gibi kişisel veridir. Ancak, KVKK'ya göre kişisel veri örnekleri çok daha fazla detaylandırılmıştır. Kişisel veri tanımı verilirken kişisel verinin tutulduğu sektörlerin ayrı ayrı ele alınmaktadır. Örneğin, teknoloji bunlardan biri olup, IP adresi ve çerezler kişisel veri örneklerinden bazılarıdır. Bu doğrultuda GDPR, KVKK'ya göre çok daha geniş kapsamlıdır. KVKK'da bulunan Özel Nitelikli

Kişisel Veri tanımına karşılık GDPR'da Madde 9'da Hassas Kişisel Veri tanımı bulunmakta, genetik ve biyometrik veriler ayrıca belirtilmektedir.

GDPR'da KVKK'da olduğu gibi verinin işlenebilmesi için kişinin rızasını gerekli kılmaktadır. KVKK'ya göre kişinin verisinin işlenebilmesi için kişinin açık rızası gereklidir. Kişinin rızasının nasıl alınacağı ya da kişinin nasıl bilgilendirileceğinin detayı kanunda verilmemektedir. GDPR'da ise kişinin bilgilendirilmesi daha açık bir şekilde belirtilmektedir. Örneğin, işaretlenmeye hazır olarak kutucuklar sunulması, veri sahibinin sessiz ya da hareketsiz kalması gibi senaryolarla alınan rızanın geçersiz olacağı vurgulanmaktadır. Rızanın geçerli olması için onaylayıcı bir aksiyon ve olumlu bir onaylama gerekmektedir. GDPR'da özellikle veri sahibinin rızasını geri çekebilmesi için anlaşılır yöntemlerin sunulması gerektiği vurgulanmaktadır.

GDPR'ın KVKK'ya göre öne çıkan farklarından bir diğeri, çocukların kişisel verileri üzerine getirdiği düzenlemedir. GDPR, ilgili düzenlemeyi "Çocuğun bilgi toplumu hizmetlerine ilişkin rızası açısından geçerli koşullar" başlıklı 8. Madde'de belirtmektedir. Çocukların kişisel verilerinin, çocuğun kendi muhatap alınarak işlenebileceği yaş sınırı 16 olarak belirlenmektedir. Bu sınırın altında bulunan çocukların kişisel verilerinin işlenebilmesi için rıza alınacak merciinin çocuğun ebeveyn yükümlülüklerini üstlenen kişi ya da kurumların olduğu vurgulanmaktadır. Yaş sınırı düzenlemesi ayrıca üye ülkelerin kendi yasalarına bırakılmış olmasına rağmen, 13 yaş sınırı belirlenerek bu yaşın altına düşülmemesi gerektiği belirtilmektedir. GDPR ve KVKK arasındaki bir diğer fark, GDPR'da 17. Madde olan Unutulma Hakkı maddesidir. GDPR, bu kapsamda da çok açık kurallar getirmektedir.

GDPR düzenlemeleri içerisindeki öne çıkan yeniliklerden biri hesap verilebilirlik hükmüdür. Uyum yükümü altında olanların kararlarını belgelendirmesi gerekliliği buna verilebilecek bir örnektir. Uyum yükümü altında olanlar uygun ölçüde teknik önlemler alarak uyumluluğun sağlanmasını garantilemek zorundadırlar. Örneğin kişilerin veri işleme süreçlerinin izlenebilirliğini sağlamak zorundadırlar. Şirketler, GDPR'ın kabul edildiği tarihten itibaren iki yıl içerisinde uyumluluk yükümlülüklerini yerine getirmeleri gerekmektedir. Bu tarih sonunda uyum yükümlülüklerini yerine getirmemiş şirketlere ciddi yaptırımlar uygulanacak olması kişisel veriyi barındıran şirketleri sıkıntıya sokmaktadır. Örneğin, GDPR şirketlerin uyumluluk hükümlerine uymadığı durumlarda dünya çapında yıllık cirosunun %4′ üne kadar cezayı ya da 27 milyon Euro para cezasını öngörmektedir. Uyum yükümü altında olan firmaların uyumluluk süreçlerini tamamlaması ciddi bir bütçeyi gerektirdiğinin vurgulandığı [37] çalışmasında Amerikan menşeili şirketlerin %68′inin GDPR'a uyumlu hale gelmesi için 10 milyon $'a kadar harcama yapabilecekleri belirtilmektedir. %24'ü ise 1 milyon doların altında harcama yapacaklarını öngörmektedirler.

GDPR ve KVKK incelendiğinde, her iki metinde de ortak tanımların ve terimlerin kullanıldığı görülmektedir. İki düzenlemede de Madde 1'de kanunun amacı kişilerin temel hak ve özgürlüklerinin korunması olarak verilmektedir. GDPR'da ilk maddede özellikle kişisel verilerin serbest dolaşımına ilişkin kurallar belirtilmektedir. GDPR ve KVKK metinlerinde yer alan terimlerin ilgili maddeler kapsamında karşılaştırılması Tablo 2'de sunulmaktadır. GDPR, Avrupa Birliği üye ülkelerin uyum yükümlülüklerini kapsamaktadır. Avrupa Birliği sınırları içerisindeki vatandaşların ve müşterilerin verilerini toplayan ve saklayan tüm şirketler, Genel Veri Koruma Tüzüğüne tabidir. GDPR'da çeşitli ülkelerin kanunları göz önünde bulundurularak ortak bir düzenleme yapılmış ve kişisel verinin ortak dolaşımı üzerine tanımlar verilmiştir. KVKK ise sadece Türkiye için geliştirilmiştir ve GDPR'a göre kapsamı daha dardır.

3. Kişisel Verileri Koruma Kanunu (KVKK)

Türkiye'de, kişisel verilerin gizliliğinin sağlanması için ilişkin çalışmalar 1988 yılında başlamıştır. Kişisel verilerin korunması üzerine çalışacak olan komisyon 2003 yılında oluşturulmuştur. Komisyon tarafından hazırlanan çalışma, 2005 tarihinde Başbakanlığa sevk edilmiştir. Bir yıl sonra yenilenen bu çalışma 2008 yılında TBMM'ye gönderilmiştir. 2016 yılında kabul edilen bu tasarı 26 Mart 2016 tarihinde 6698 kanun numarasıyla yasalaşmıştır [38].

Kanunda kabul edilen temel ilkeler şunlardır;

- Kişisel verilerin işlenme şartları
- Bireylerin aydınlatılması
- Bu alanı kontrol edecek bir otoritenin oluşması
- Veri gizliliği ve güvenliği için gerekli önlemlerin alınması

KVKK, 7 bölümden ve 33 maddeden oluşmaktadır. 1. bölüm; Amaç, Kapsam ve Tanımları. 2. bölüm; Kişisel Verilerin İşlenmesinin Genel ilkelerini ve işlenme şartlarını belirlemektedir. 3. bölüm; Haklar ve Yükümlülükler, 4.bölüm; Başvuru, Şikâyet ve Veri Sorumluları Sicili, 5. bölüm; Suçlar ve Kabahatler, 6. bölüm; Kişisel Verileri Koruma Kurumu ve Teşkilat, 7. bölüm; Çeşitli Hükümler ile ilgili maddeleri kapsamaktadır.

KVKK'da denetim mekanizmasını gerçekleştirmek için Kişisel Verileri Koruma Kurumu kurulmuştur. Bu Kurum, Kurul ve Başkandan oluşmaktadır. Kurum, Kurul ve Başkanlık tanımları ilgili kanunda [38]; "Kurumun karar organı Kurul'dur. Kişisel Verileri Koruma Kurulu, bu Kanunla ve diğer mevzuatla verilen görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak yerine getirir ve kullanır. Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz. Başkan, Kurul ve Kurumun başkanı sıfatıyla Kurumun en üst amiri olup Kurum hizmetlerini mevzuata, Kurumun amaç ve politikalarına, stratejik planına, performans ölçütlerine ve hizmet kalite standartlarına uygun olarak düzenler, yürütür ve hizmet birimleri arasında koordinasyonu sağlar" olarak verilmektedir.

Kişisel veri, diğer ülkelere ve üçüncü kişilere aktarılabilmektedir. Kişisel verinin aktarılabilmesi için verinin işlenebilmesinde geçerli olan işlenme şartları geçerli olmaktadır. Özellikle kişisel verinin yurtdışına aktarılmasında Kurul'un izni gerekmektedir. Ayrıca verinin aktarılacağı ülkede yeterli korumanın bulunması da verinin aktarılabilmesi için gerekli olan kriterlerden biridir.

KVKK'da Veri Sorumluları Sicili ve Özel Nitelikli Kişisel Veriler terimleri mevcuttur. Kanuna göre; "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler" özel nitelikli kişisel veridir. Özel Nitelikli Kişisel Verilerin işlenme şartları, Kişisel Verilerin İşlenme Şartları ile benzerlik göstermektedir. Ek bir kriter olarak Kurul tarafından belirlenen tedbirlerin alınması gerekmektedir.

Veri Sorumluları Sicili, kamuya açık olarak tutulan bir listedir. Veri Sorumluları Sicilinden Kurul sorumludur ve Kurul gerekli denetimler gerçekleştirir. Kişisel verileri işlemek isteyen tüm gerçek ve tüzel kişiler bu sicile kaydolmak zorundadırlar. Bazı özel durumlarda Kurul'un denetiminde olmak şartıyla bu sicile kayıt zorunluluğuna istisna getirilebilmektedir.

Tablo 2. GDPR ve KVKK'da bulunan terimlerin karşılaştırılması.

Table 2. Comparison of terms in GDPR and KVKK.

Terim	KVKK	GDPR
Gerçek Kişi	2. Madde	1. Madde
Tüzel Kişi	2. Madde	4. Madde
Açık Rıza	3. Madde 1. Fıkra (a) Bendi	4. Madde 11.Fıkra
Anonim Hale Getirilmesi	3. Madde 1. Fıkra (b) Bendi, 7. Madde	-
Başkan	3. Madde 1. Fıkra (c) Bendi	-
İlgili Kişi	3. Madde 1. Fıkra (ç) Bendi	5. Madde
Kişisel Veri	3. Madde 1. Fıkra (d) Bendi	4. Madde 1. Fıkra
Veri İşleyen	3. Madde 1. Fıkra (ğ) Bendi	4. Madde 8. Fıkra
İşlenme Şartları	5. Madde	5. Madde
Kaydetme, İşleme, Değiştirme gibi Veri İşleme Çeşitleri	3. Madde 1. Fıkra (e) Bendi	4. Madde 2. Fıkra
Veri Sorumlusu	3. Madde 1. Fıkra (ı) Bendi	4. Madde 7. Fıkra
Kişisel Verileri Koruma Kurulu	3. Madde 1. Fıkra (f) Bendi	4. Madde 17. Fıkra
Veri Kayıt Sistemi	3. Madde 1. Fıkra (h) Bendi	-
Kişisel Verileri Koruma Kurumu	3. Madde 1. Fıkra (g) Bendi	4. Madde 16. Fıkra
Özel Nitelikli Kişisel Veriler	6. Madde	9.Madde

KVKK, kişisel verinin gizliliğinin sağlanması için bütüncül bir süreç sağlamaktadır. Bu kanuna göre kişisel verilerin işlenmesi için kişinin onamı şarttır. Kişisel veri için güvenlik ve gizlilik kavramlarından sonra onam kavramı da böylelikle literatürde yer bulmaktadır. Bu kavramların tanımları aşağıda verilmektedir.

Güvenlik: Türk Dili Kurumu Büyük Türkçe Sözlükte güvenlik, "toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" anlamına gelmektedir [39]. Bilgi Güvenliği anlamı; "bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek" şeklinde verilmektedir [40]. Bilgi Güvenliği, gizlilik, bütünlük ve erişilebilirlik olmak üzere üç temel güvenlik öğesinden meydana gelir ve bu güvenlik öğelerinden birinin risk altında bulunması bilgi güvenlik zafiyetini oluşturur. Veri, bilginin ham, işlenmemiş halidir. Veri Güvenliği, Bilgi Güvenliği altında bulunan Ağ Güvenliği, Uygulama Güvenliği gibi temel kategorilerden biridir [41] ve veritabanı Güvenliği, Veri Kaybı/Sızıntısı Önleme, Şifreleme ve Erişim Yönetimi olmak üzere alt başlıklara ayrılmaktadır.

Gizlilik: Türk Dili Kurumu Büyük Türkçe Sözlükte gizlilik tanımı, "Gizli olma durumu, mahremiyet" şeklinde verilmektedir [39]. 2014 yılında yapılan bir çalışmada Gizlilik "bilginin yetkisiz kişilerin eline geçmeme ve yetkisiz erişime karşı korunmasıdır" olarak tanımlanmaktadır [42]. KVKK Genel Gerekçesinde Veri Gizliliği tanımı şu şekildedir: "Veri Gizliliği, verilerin yetkisiz kişiler tarafından elde edilmemesi, kullanılmaması ve ifşa edilmemesidir" [43]. Veri gizliliğinin sağlanması yöntemleri arasında biyometrik yöntemler [44], parola ile kimlik doğrulama [45], veriye erişimde standartların kullanımı [46] gibi çeşitli çalışmalar bulunmaktadır. Onam Yönetimi çalışmaları da kişisel verinin gizliliğini sağlamak üzere yapılan çalışmalardandır.

Onam: Türk Dili Kurumu Büyük Türkçe Sözlükte onam, "rıza, muvafakat" olarak tanımlanmaktadır [39]. KVKK'da onam yerine açık rıza kelimesi kullanılmaktadır. KVKK'nın 3. maddesinin 1. fıkrasının (a) bendine göre açık rıza "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" anlamına gelmektedir. KVKK'nın 5. maddesinin 1. fıkrasında belirtildiği üzere, kişisel verilerin işlenmesi ancak kişinin onamı yani açık rızası var ise gerçekleşebilir. Bu sebeple, kişisel verilerin işlenebilmesi için kişinin onamını tutan, veriye erişim sırasında onam kontrolünü gerçekleştiren ve erişime izin veren ya da vermeyen onam yönetimi çalışmaları da verinin gizliliğini sağlamak için yapılacak çalışmalar arasındadır. KVKK'ya göre onam süreci yasal olarak zorunlu kılınmaktadır.

Yukarıda verilen güvenlik, gizlilik ve onam tanımlarına bakıldığında gizlilik kavramı bilgi güvenliği kavramı altındaki üç temel unsurdan biri olarak görülmesine rağmen günümüzde veri gizliliği ve veri güvenliği iki ayrı temel çalışma alanı olarak görülmektedir. Veri güvenliği de yine bilgi güvenliği altında yer almaktadır. KVKK'da da belirtildiği üzere kişisel verinin gizliliğinin sağlanması için kişinin onamı yani açık rızası şarttır. Ekonomik Kalkınma ve İşbirliği Örgütü'nün [19] kişisel verinin gizliliğinin sağlanması için rehber ilkelerinde kişisel verilerin yasal mevzuatlara uygun ve meşru yollarla işlenmesi ve kişilerin izninin alınması gerektiği vurgulanmaktadır. Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin 2. fıkrasında [47], Avrupa Birliği Temel Haklar Sözleşmesi'nin 8. maddesinde [48] ve 108 Numaralı Avrupa Konseyi Sözleşmesi'nde [3] kişisel verinin mahremiyetinin sağlanması için kişinin vermiş olduğu onamın gerektiği belirtilmektedir. Onam kavramı, hassas bilgilerin ortaya çıkarılmasını bilginin sahibi kişinin isteklerine göre sınırlandırmak üzere ulusal ve uluslararası gizlilik mevzuatlarında, yasalarda ve antlaşmalarda geniş olarak yer bulmaktadır.

4. Anlamsal Web ve Teknolojileri

4.1. Anlamsal Web

World Wide Web - WWW, sadece insanların anlayabileceği bir ağ olarak değil, aynı zamanda makinelerin de bu ağa katılıp bilgi alabileceği bir alan olarak tasarlanmıştır [49]. Ancak, ağın mevcut halinde, çoğu bilgi insanların faydalanabileceği bir yapıda tutulmaktadır. Bilgilerin tutuldukları yapıdan dolayı internette gezinti yapan bir robotun bu bilgilere ulaşması ve bilgileri anlamlandırması kısıtlıdır. Anlamsal Web, bilgileri makine

işleyebilir formda (machine-processable form) tutan bir yapı sunmaktadır.

Anlamsal Web çalışması, daha akıllı ve sezgisel bir ağ oluşturmak isteyen Tim Berners-Lee tarafından başlatılmıştır. Berners-Lee'nin amacı, bilgisayarların otonom olarak bilgileri daha iyi manipüle etmelerini sağlamaktır [50]. Berners-Lee'nin tanımına göre Anlamsal Web, yeni ve ayrı bir ağ olmayıp, bilgilere iyi tanımlanmış anlamların verildiği, bilgisayarların ve insanların birlikte çalışmalarına imkân veren bugünkü ağın bir uzantısıdır. W3C (World Wide Web Consortium) tarafından uluslararası bir standart olarak geliştirilmiştir [51]. Anlamsal Web'de, bilgilerin ve verilerin makine tarafından erişilebilmesi ve yorumlanabilmesi (machine-interpretable) için var olan verilere üst veriler eklenmektedir. Böylelikle bilgisayarlar, internetteki verileri insanların bilgileri işleme biçimine benzer olarak anlamlı yorumlayabilmektedir.

Günümüzde, internette bir bilgi arandığında, kullanıcıya anahtar kelime ile eşleşen sayfalar veya belgeler sunulmaktadır. Gerçekleşen arama sonucu, kullanıcının almak istediği bir sonuç olmayabilir. Bunun nedeni, biçimlendirme dilinin, bir metine anlam kazandırmayan, sadece metnin internette görünmesini sağlayan bir işaretleme dili olmasıdır. Anlamsal Web, makinelerin web sayfası verilerini anlamalarına yardımcı olacak bir format veya yapı sağlamaktadır. Bu yapı kapsamında RDF (Resource Description Framework), OWL (Web Onlotolgy Language), XML (Extensible Markeup Language) ve SPARQL (Simple Protocol and Rdf Query Language) gibi teknolojiler bulunmaktadır. Bu teknolojiler ile ağda yer alan veri, makine-okunabilir bir formata dönüştürülmektedir. Böylelikle bilgisayarlar, internette bilgi arayabilmekte ve bu bilgiyi yorumlayabilmektedir.

Anlamsal Web, belgelerden ziyade bir veri ağını tanımlar [52]. Bu veri ağında, verilerin ortak gösterimi, entegrasyonu ve paylaşımı için ortak formatlar ve standartlar bulunmaktadır. Ayrıca, verilerin gerçek dünyadaki nesnelerle ilişkisini tanımlayan diller mevcuttur. Tim Berners-Lee tarafından önerilen Anlamsal Web katmanlı yapısında [53] bu formatlar, standartlar ve diller yer almaktadır. Yapının en alt katmanında URI tanımlamaları yer almaktadır. URI katmanının üstünde XML ve XML Schema bulunmaktadır. RDF temelli bir model, XML sözdiziminde ifade edilebilmektedir. Bu nedenle, XML katmanının üstünde RDF katmanı yer almaktadır. RDF katmanın üstünde ontoloji sözlüğü katmanı bulunmaktadır. Anlamsal Web katmanlarının en üst 3 katmanı Mantık, Kanıt ve Güven katmanlarıdır. Mantık katmanı, bir alt katmanında yer alan OWL'yi güçlendirmek için farklı ontoloji dilleri bulundurmaktadır. Bunlar: OWL Lite, OWL DL ve OWL Full. Kanıt katmanı gerçek tümdengelim işlemini, kanıtların temsilini ve kanıt doğrulamasını içermektedir. Uygulamaların neden belirli bir sonuca varıldığını sorgulamasına olanak tanımaktadır. Güven katmanı, dijital imzaların kullanımı, güvenilir acentelerin önerileri, sertifika acentelerinin derecelendirmeleri ile desteklenmektedir. Bu katman, kimlik doğrulanması ile veri ve servislerin güvenilirliğini sağlamaktadır.

4.2. Resource Description Framework (RDF)

RDF [54], bir W3C standardıdır. Nesnelere ("web kaynakları") ve bunların ilişkilerine atıfta bulunan veri modellerini ifade etmek için kullanılan basit bir dildir. RDF tabanlı bir model, RDF/XML, N3, Turtle ve RDFa gibi çeşitli sözdizimlerinde gösterilebilir. Anlamsal Web'in temel bir standardı olan RDF ifadeleri özne, yüklem ve nesne (subject, predicate,object) şeklinde üçlü olarak yazılmaktadır.

Şekil 1'de örnek bir RDF üçlüsü verilmektedir.

Örnek Cümle: Ece Aydın'ın yaşı 36'dır.

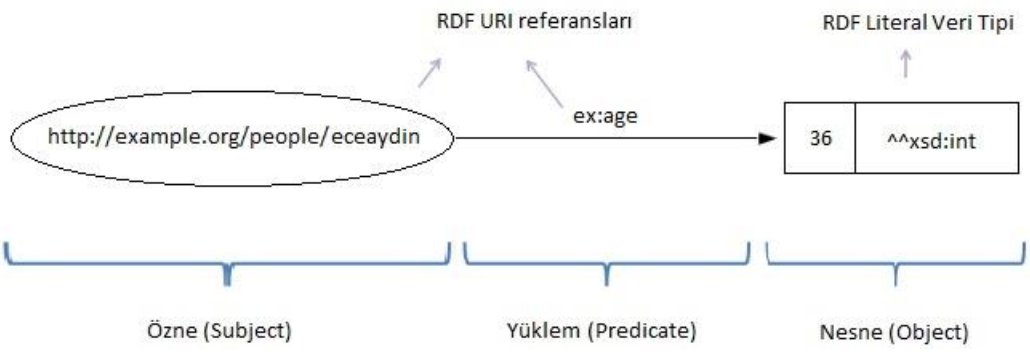
RDF, nesnelere işaret eden ve bu nesnelerin birbirleriyle nasıl ilişkili olduğunu tanımlayan bir veri modelidir. RDF temelli bir model XML sözdiziminde ifade edilebilmektedir. RDF, bir dil değil, bir veri modelidir. Bir nesnenin özelliklerini veya başka bir nesne ile olan ilişkisini tanımlamaktadır. Tablo 3'de öğrenci bilgilerini belirten bir RDF örneği verilmiştir.

4.3. RDF Schema (RDFs)

RDF Şeması [55], RDF nesnelerinin özelliklerini ve sınıflarını tanımlayan sözcükler bütünüdür. RDF Şeması, RDF'yi anlamsal olarak genişletmekte ve RDF tabanlı kaynakların özelliklerini ve sınıflarını tanımlamak için bir çerçeve sağlamaktadır. RDF Şeması'ndaki sınıflar, nesne yönelimli programlama dillerindeki sınıflara benzemektedir. Bu, kaynakların sınıf örnekleri ve sınıfların alt sınıfları olarak tanımlanmasını sağlamaktadır. RDF şemaları URI'lere sahip olan internet kaynaklarıdır. Tablo 3 ve Tablo 4'de öğrenci ve akademisyen için RDF şema örneği verilmiştir.

4.4. Ontology

RDF ve RDFS, bir alanın özelliklerinin tanımlanmasına izin vermektedir. Ancak, modelleme ilkelleri genel kullanım için çok kısıtlayıcıdır. Alanın taksonomik yapısının tanımlanması, alanın kısıtlamalarının modellenmesi ve alanla ilgili bir dizi çıkarım kuralının belirtilmesi gerekmektedir. Bu işlemler de ontolojiler sayesinde gerçekleştirilmektedir. Gruber'e göre ontoloji, kavramsallaştırmanın açık ve resmi bir tanımıdır [56]. Ontoloji, etki alanı hakkında ortak bir anlam sağlamaktadır. Ortak anlam da belirtimlerin biçimsel tanımlanması ile gerçekleşmektedir. Biçimsel tanımlama ile çıkarsama da sağlanmaktadır.



Şekil 1. RDF üçlü gösterimi.

Figure 1. RDF triple notation.

Tablo 3. Öğrenci bilgisini tutan RDF örneği.

Table 3. RDF example holding student information.

```
<?xml version="1.0"?>
  <rdf:RDF xmlns:rdf=http://www.w3.org/1999/02/22-rdf-syntax-ns#
           xmlns:student="http://www.w3.org/2000/10/swap/pim/student#">
           <student:Person rdf:about="http://www.w3.org/Students/EA/student#me">
           <student:name>Ece</student:name>
           <student:surname>Aydın</student:surname>
           <student:universtiy>Ege University</student:universtiy>
             <student:departmant>Computer Engineering</student:department>
            <student:number>Ege University</student:number>
             </student:Person>
  </rdf:RDF>
```

Tablo 4. Öğrenci ve akademisyen bilgisini tutan RDF örneği.

Table 4. RDF example that holds student and academician information.

```
<?xml version="1.0"?>
   <rdf:RDF xmlns:rdf=”http://www.w3.org/1999/02/22-rdf-syntax-ns#”
   xmlns:rdf=”http://www.w3.org/2000/01/rdf-schema#”
   xml:base=http://www.w3.org/2000/10/swap/pim/student#
         <rdfs:Class rdf:ID=”person”/>
      <rdfs:Class rdf:ID=”student”>
            <rdfs:subClassOf rdf:resource=”#person”/>
      </rdfs:Class>
      <rdfs:Class rdf:ID=”academician”>
          <rdfs:subClassOf rdf:resource=”#person”/>
     </rdfs:Class>
   </rdf:RDF>
```

Bir ontoloji dili, XML ve RDF/S gibi mevcut standartları genişletmekte ve muhakeme yeteneği sağlamaktadır. En yaygın kullanılan ontoloji dili OWL kısaltmasına sahip olan Web Ontoloji Dilidir. OWL bir W3C standardıdır. Sınıflar arası ilişkiler (disjointness), kardinalite (exactly-one), alan ve aralık kısıtlamaları, varlık kısıtlamaları, geçişli, ters ve simetrik özellikler gibi ek kısıtlamaları içeren RDFS'yi genişletmektedir.

OWL, belirli geliştirici ve kullanıcı toplulukları tarafından kullanılmak üzere tasarlanan, üç alt dilin sunmaktadır. Bu alt diller:

- OWL Lite: Sınırlı bir OWL yapısı alt kümesini desteklemektedir. Sınıflandırma hiyerarşisine ve basit kısıtlamalara ihtiyaç duyan kullanıcılar için önerilmektedir. Owl Lite, OWL DL'den daha düşük bir resmi karmaşıklığa sahiptir. Hesaplama açısından verimlidir.
- OWL DL: Tanım Mantığı (Description Logic) adı verilen birinci dereceden bir mantığa dayanır. OWL DL, bütün OWL dil yapılarını içermektedir. Ancak, bunlar yalnızca belirli kısıtlamalar altında kullanılabilmektedir (örneğin, bir sınıf birçok sınıfın alt sınıfı olsa da başka bir sınıfın örneği olamaz). OWL Full'un bir alt dilidir.

- OWL Full: OWL Full, RDFS ile tam uyumluluk sunmaktadır. OWL-Full, en geniş tanımlama ifadelerine sahip OWL alt dilidir. Yüksek anlamlılığın daha önemli olduğu durumlarda kullanılmak üzere tasarlanmıştır. Bu nedenle, OWL-Full ontolojileri üzerinde otomatik bir akıl yürütme yapmak mümkün değildir

4.5. Anlamsal Web Kuralı Dili (Semantic Web Rule Language – SWRL)

Kural tabanlı sistemler günümüzde neredeyse her alanda mevcuttur. Örneğin, mühendislikte tanımlama kuralları, ticarette iş kuralları, hukukta yasal kurallar, internette erişim kuralları bulunmaktadır. Kural İşaretlemesi (RuleML) Girişimi [57], kuralların tanımlanmasında bir standart oluşturulması için çalışmalar yürütmektedir. Kural Tanımlama Dili (Rule Markup Language – RuleML), Kural İşaretlemesi Girişimi tarafından World Wide Web'de kural tabanlarını yayınlamak ve paylaşmak için geliştirilen bir işaretleme dilidir. RuleML, endüstri standartları arasındaki kural işbirliğini sağlamak için geliştirilmiştir. SWRL ise, Anlamsal Web için geliştirilmiş olan bir kural dilidir ve Anlamsal Web katmanlı yapısında Ontoloji Sözlüğü katmanında yer almaktadır [58].

SWRL, Web Ontolojisi Dilleri'nden OWL DL ve OWL Lite dilleri ile Kural İşaretleme Dilinin (Rule Markup Language) alt dillerinden olan Unary/Binary Datalog RuleML'nin kombinasyonu temeline dayanmaktadır [59]. SWRL, OWL'nin hem OWL DL hem de OWL Lite alt dillerinde üst düzey bir soyut sözdizimi içermektedir. Tüm kurallar OWL kavramları (sınıflar, özellikler, bireyler) cinsinden ifade edilmektedir. SWRL için W3C tarafından verilen örnekte [59], bu kuralların basit bir kullanımı, hasParent, hasBrother ve hasUncle özellikleri ile verilmektedir. Bu kural şu şekilde sunulmaktadır:

$$hasParent(?x1,?x2) \land hasBrother(?x2,?x3) \Rightarrow hasUncle(?x1,?x3)$$

Bu kural örneklenirse;

$$hasParent(Arda,Ali) \land hasBrother(Ali,Mehmet) \Rightarrow hasUncle(Arda,Mehmet)$$

Bu kurala göre, Ali, Arda'nın ebeveyni ise ve Mehmet, Ali'nin kardeşi ise, o zaman Mehmet, Arda'nın amcasıdır.

5. Kişisel Verilerin Korunması için Onam Yönetimi Sistemi

KVKK'ya göre kişisel verilerin işlenmesi için kişinin onamı şarttır. Kişisel veriye erişilmesi ve bu verinin kullanılması için onam yönetimi sürecinin gerçekleşmesi gerekmektedir. Kanun, Onam Yönetimi Sistemi için sistem aktörlerini ve ilişkilerini vermektedir.

Bu aktörler ve ilişkiler kanun metininin analiz edilerek terminolojinin çıkartılmasıyla elde edilmektedir. Terminolojinin manuel veya otomatik olarak çıkartılmaktadır. Otomatik terim çıkarma sürecinde TerMine [60] ve Text2Onto [61] gibi terim çıkarma uygulamalarından ve Doğal Dil İşleme metotlarından yararlanılmaktadır. Manuel terim belirlemede ise alan uzmanları bilgilerine ve tecrübelerine dayanarak terimleri çıkartmaktadır. Terimler, çıkartıldıkları alandaki gerçek dünya kavramlarına benzemektedir. Çıkartılan terimler içerisinden sınıflar ve özellikler belirlenmektedir. Sınıfları temsil eden terimler, grup halinde ve aynı zamanda hiyerarşik bir biçimde düzenlenmelidir. Terimlerin belirlenmesinde önerilen dört yaklaşım vardır: Top-down, Bottom-up, Middle-out, Hybrid [62] [63]. Top-down yaklaşımında, alandaki en genel kavramlar ve sonrasında bu kavramların özelleşmiş alt kavramları belirlenmektedir. Örneğin, hayvan sınıfı belirlendikten sonra köpek, kedi gibi alt sınıflar oluşturulmaktadır. Bottom-up yaklaşımında, öncelikle en özellikli sınıflar (hiyerarşinin yaprakları) ve bu sınıfların üst kavramları tanımlanmaktadır. Örneğin, kaplan, aslan gibi alt sınıflar belirlendikten sonra bu sınıfların bir üst sınıfı olan kedi sınıfı sonradan tanımlanmaktadır. Middle-out yaklaşımında, tüm sınıflar rastgele alınarak birbirleri ile ilişkilerine göre ontoloji içerisinde tanımlanmaktadır. Hybrid yaklaşımı, Top-down ve Bottom-up yaklaşımlarının bir birleşimidir. Öncelikle, daha genel kavramlar tanımlanmakta, sonrasında bu kavramlar uygun şekilde genelleştirilmekte ve özelleştirilmektedir.

Metinden terminoloji çıkarılmasında aşağıdaki teknikler kullanılmaktadır:

- C-değeri (C-value) [64],
- TF-IDF (Term Frequency—Inverse Document Frequency) [65],
- Mevcut alan sözlüklerinin veya ontolojilerinin kullanımı [65],
- Varlık ismi çıkarımı (Named Entity Recognition - NER) [67],
- Chunking [68],
- Hearst patterns tasarım tabanlı ayrıştırma [61]

Bu teknikleri kullanarak geliştirilen TerMine, Text2Onto ve KIM Platform gibi araçlar bulunmaktadır. Protégé üzerinde eklenti olarak da çalışan TerMine, C-değeri metodunu kullanmaktadır. Bu araç sayesinde bir metin kitaplığından terim çıkartılabilmektedir. Çıkarılan aday terimler uzman bir kişi tarafından değerlendirilerek kullanım alanına göre sınıflandırılır ve hiyerarşik yapı oluşturulur [60]. Text2Onto, TextToOnto projesinin geliştirilmiş halidir. Text2Onto, metinden ontoloji öğrenmesi için geliştirilen bir çatıdır ve sadece İngilizce, İspanyolca ve kısmen Almanca dillerinde yazılmış metinler üzerinde çalışmaktadır. Üzerinde çalışılan metinden gerekli terimlerin seçilmesi alan bilgisine sahip bir uzman tarafından yapılabilmektedir [69]. KIM Platformu, metinleri analiz eden ve yapısal olmayan veriyi anlamlı hale getirmeyi hedefleyen bir araçtır. Metinleri analiz ederek otomatik olarak anlamsal bağlantıları, varlıkları ve ilişkileri oluşturmaktadır. Tespit edilen ve sunulan yapı RDF'de saklanır. Çeşitli RDF serileştirme formatlarında dışa aktarılabilir. Varlık ismi çıkarma (Named Entity Recognition - NER), bir bilgi çıkarımı yöntemidir [70] ve daha çok İngilizce dokümanlar üzerinde çalışmaktadır. NER, metni alır, analiz eder ve önemli varlık elamanlarını kendi belirlemiş olduğu kişi, organizasyon gibi kategorilere göre belirler.

Yukarıda sunulan araçlar İngilizce dokümanlar üzerinde çalışmakta olup Türkçe metinler üzerinde anlamlı sonuçlar üretmemektedir. TF-IDF metodu ise dil bağımsız olarak tüm metinler üzerinde çalışabilmektedir. İstatistiksel hesaplamalar yapan TF-IDF metodu, metin madenciliği ve doğal dil işleme çalışmalarında kullanılan yöntemlerden biridir. Bu yöntemde, kelimelerin yer aldıkları metinlerdeki kullanım sıklığı hesaplanmaktadır. Bu nedenle, analiz metodu olarak TF-IDF (Term Frequency—Inverse Document Frequency) [65] metodu seçilmiştir.

TF-IDF metodu ile sistemin olası elemanlarının hepsi ilgili kanundan çıkartılmaktadır. Öncelikle TF-IDF ile kanun metninin hangi bölümlerinin analiz edileceği belirlenmiştir. Sonrasında bu bölümler üzerinde ön işlemler yapılmıştır. Örneğin, kişisel kelimesi Kişisel Veri terimi dışında kullanılmaktadır. Onam yönetimi sürecinde kişisel kelimesinin herhangi bir etkisi yoktur. Aksine, Kişisel Veri tanımı bu işleyişteki temel kavramlardandır. Bu nedenle, tamlama grupları tek bir kelime haline getirilmiştir. Kişisel Veri ikili kelime grubu KişiselVeri olarak birleştirilmiştir. Buna ek olarak kanunun madde numaraları, bazı noktalama işaretleri ve bağlaçlar da işlenecek metinden çıkarılmıştır. Sonraki aşama olarak ön işlem yapılan kanun metninden kelime

bulutu oluşturulmuştur. Oluşturulan kelime bulutu ve kelime sıklığı Şekil 2 ve Şekil 3'de sunulmaktadır.

Kanun metninden kelime bulutu çıkartıldıktan sonra elde edilen kelimelerin ağırlıkları alanyazında kabul görmüş TF-IDF metodu ile hesaplanmaktadır. TF-IDF formülü, Formül 1'de verilmektedir.

$$w_{i,j} = tf_{i,j} \times \log \frac{N}{df_j} \text{ (Formül 1 TF-IDF formülü)}$$

TF-IDF ile terimlerin ağırlıklarının bulunması ve aday terimlerin çıkartılması [71]'de detaylı bir şekilde sunulmaktadır.

Üzerinde çalışılan kanun metninin ilk iki bölümünde en fazla geçen terim Kişisel Veri olmuştur. Bu terimin TF-IDF değeri 0.041'dir. Sonrasında gelen terimler şunlardır: İlgili Kişi, Açık Rıza, Veri Sorumlusu, Gerçek Kişi, Kişisel Veri İşlenmesi, Tüzel Kişi, Veri Kayıt Sistemi.

KVKK, kişisel verinin korunması için onam yönetimini zorunlu kılmakta ve bir senaryo sunmaktadır. Senaryo yukarıda da öne çıktığı görülen Açık Rıza yani Onam üzerinedir. İlgili Kişi'nin Onam'ı üzerinden işleyen bu süreçteki aday terimler kelime bulutu ve kelime frekanslarıyla bulunmuş, ağırlıkları da TF-IDF metodu ile analiz edilmiştir. Tüm bu işlemlerin sonunda ortaya çıkan terimler halen aday terimler olup bir uzman görüşü ile Onam Yönetimi Modelinde kullanılacak terimler belirlenmektedir. Sistem içinde yer alacak aktörler, nesneler ve işlemler şunlardır: Kişisel Veri, İlgili Kişi, Açık Rıza, Başkan, Kişisel Verilerin İşlenmesi (elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi), Kişisel Verileri Koruma Kurulu, Kişisel Verileri Koruma Kurumu, Veri İşleyen, Veri Kayıt Sistemi, Veri Sorumlusu, Gerçek Kişi, Tüzel Kişi, İşlenme Şartları, Özel Nitelikli Kişisel Veriler, Kişisel Verilerin Silinmesi, Yok Edilmesi, Anonim Hale Getirilmesi, Verilerin Aktarılması, Veri Sorumluları Sicili.

Kişisel Verilerin Korunması Kanununa göre sunulan sistemdeki aktörler ve sistem üyeleri için tanımlar aşağıda verilmektedir.

- İlgili Kişi: Kişisel verisi işlenen gerçek kişi.
- Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
- Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.
- Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
- Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
- İşleme Şartları: Kişisel verinin işlenme şartlarını ifade eder.
- Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
- Diğer Haller: İlgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi bazı koşulların sağlanması ile mümkündür. Bu koşullar; kanunlarda açıkça öngörülmesi, ilgili kişinin kendisi tarafından alenileştirilmiş olması gibi koşullar.

Geliştirilen onam yönetimi sisteminde, Veri Kayıt Sistemi, Kişisel Veriyi tutmaktadır. Veri Sorumlusu, Veri Kayıt Sisteminden sorumludur ve Veri Kayıt Sisteminin tuttuğu Kişisel Veriyi anonimleştirebilir, yok edebilir ve/veya silebilir. Veri Sorumlusu, aynı zamanda Kişisel Veriyi Yurt Dışı/Üçüncü Kişilere, Kişisel Verinin işlenme şartlarına bağlı kalarak aktarabilir. Veri Sorumlusu, Veri İşleyeni yetkilendirmektedir. Yetkilendirilmiş Veri İşleyen, Kişisel Veriyi İşlenme Şartlarına bağlık kalarak işlemektedir. İşlenme Şartları, İlgili Kişinin onamı ya da yasal onamdan oluşan şartlardır. İlgili Kişi, Kişisel Veriye sahiptir ve kendi Kişisel Verisini anonimleştirebilir.

Kanuna göre belirlenmiş sistemin genel işleyiş modeli Şekil 4'de sunulmaktadır. Bu modelde, Veri Sorumlusu ve Veri İşleyen aktörlerinin ilişkileri sunulmaktadır. Veri Sorumlusu aktörü, KVKK'nın 3. maddesi 1. fıkrası (ı) bendine göre Veri Kayıt Sisteminin kurulmasından ve yönetilmesinden sorumludur. Kanunun 3. maddesi 1. fıkrası (ğ) bendine göre Veri Sorumlusu, Kişisel Veriyi işleyebilmesi için Veri İşleyeni yetkilendirir. Veri Kayıt Sistemi, kanunun 3. maddesi 1. fıkrası (h) bendine göre Kişisel Verinin tutulduğu kayıt sistemidir. Veri İşleyen, kanunun 3. maddesi 1. fıkrası (ğ) bendine göre Kişisel Veriyi işler. Kişisel Verinin işlenmesinde kanunun 3. maddesi 1. fıkrasına göre kişinin Açık Rızası (Onamı) aranır. Kanunun 3. maddesi 2. fıkrasına göre kişinin Açık Rızası aranmaksızın belli şartların varlığı halinde Kişisel Veri işlenebilir.

Şekil 5'de onam yönetim sistemi için bir etkinlik diyagramı verilmektedir. Etkinlik diyagramında, kişisel veriye erişim talebinin gelmesi ve bu talep için cevap alınması arasındaki süreç verilmektedir. Buna göre, Kişisel Veri'ye Veri İşleyen'den bir erişim talebi gelmektedir. Öncelikle, bu erişim talebinin amacı belirlenmekte, sonrasında veri sahibi İlgili Kişinin erişilmek istenen veri için onamının olup olmadığı ile ilgili kontrol gerçekleştirilmektedir. Eğer kişinin onamı varsa, erişim talebi onaylanır. Eğer kişinin onamı yoksa diğer hukuki izinlerin varlığı kontrol edilir. Hukuki izin bulunursa erişim talebi onaylanır. Eğer izin bulunamazsa, erişim reddedilir. Onam yönetimi sistemine gelen erişim talebi, sürecin sonunda bir cevap üretmektedir.

Filter	Size	Color	Angle	Font
Kisiselveri	29	Default	Default	Default
Ilgilikisi	14	Default	Default	Default
Acıkrıza	10	Default	Default	Default
Iliskin	9	Default	Default	Default
Gercekkisi	8	Default	Default	Default
Ilgili	8	Default	Default	Default
Kisiselveriislenmesi	7	Default	Default	Default
Verisorumlusu	7	Default	Default	Default

Şekil 2. Kelime bulutu oluşturucu tarafından çıkartılan kelime sıklıkları.

Figure 2. Word frequencies extracted by the word cloud generator.

Şekil 3. Kanun metninden oluşturulan kelime bulutu.

Figure 3. Word cloud created from the text of the law.

Sistem ardıl-işlem diyagramı (system sequence diagram - SSD), UML'de bir tür dizi şemasıdır. Bu diyagramlar, aktörler tarafından sistemin dışından üretilen olayların ayrıntılarını göstermektedir [72]. Onam Yönetimi için sistem ardıl-işlem diyagramında, kişisel veriye erişim talebinin gelmesi ve bu talep için cevap alınması arasındaki sürecin işleyişi verilmektedir. Şekil 6'de Onam Yönetimi için bir sistem ardıl-işlem diyagramı verilmektedir.

Şekil 6'da sunulan SSD'de, Kişisel Veri, Veri İşleyen tarafından erişilmek istenmektedir. Veriye erişim için amaç ve işlem gibi bilgiler *kisiselVeriyeErisim()* metodu ile erisimBilgisi parametresi içinde gönderilmektedir. Erişim ve amaç verileri erisimBilgisi parametresi içinden alınmakta ve kişinin onamı *onamKontrol()* metodu ile kontrol edilmektedir. Sonuç, sırayla *onamSonucu(), erisimSonucu()* metotları ile kullanıcıya döndürülmektedir.

Onam Yönetimi sürecinde onam kontrolünü gerçekleştiren metot için sözde kod Tablo 5'de verilmektedir.

Sistem ardıl-işlem diyagramı (system sequence diagram - SSD), UML'de bir tür dizi şemasıdır. Bu diyagramlar, aktörler tarafından sistemin dışından üretilen olayların ayrıntılarını göstermektedir [72]. Onam Yönetimi için sistem ardıl-işlem diyagramında, kişisel veriye erişim talebinin gelmesi ve bu talep için cevap alınması arasındaki sürecin işleyişi verilmektedir. Şekil 6'de Onam Yönetimi için bir sistem ardıl-işlem diyagramı verilmektedir.

Şekil 6'da sunulan SSD'de, Kişisel Veri, Veri İşleyen tarafından erişilmek istenmektedir. Veriye erişim için amaç ve işlem gibi bilgiler *kisiselVeriyeErisim()* metodu ile erisimBilgisi parametresi içinde gönderilmektedir. Erişim ve amaç verileri erisimBilgisi parametresi içinden alınmakta ve kişinin onamı *onamKontrol()* metodu ile kontrol edilmektedir. Sonuç, sırayla *onamSonucu(), erisimSonucu()* metotları ile kullanıcıya döndürülmektedir.

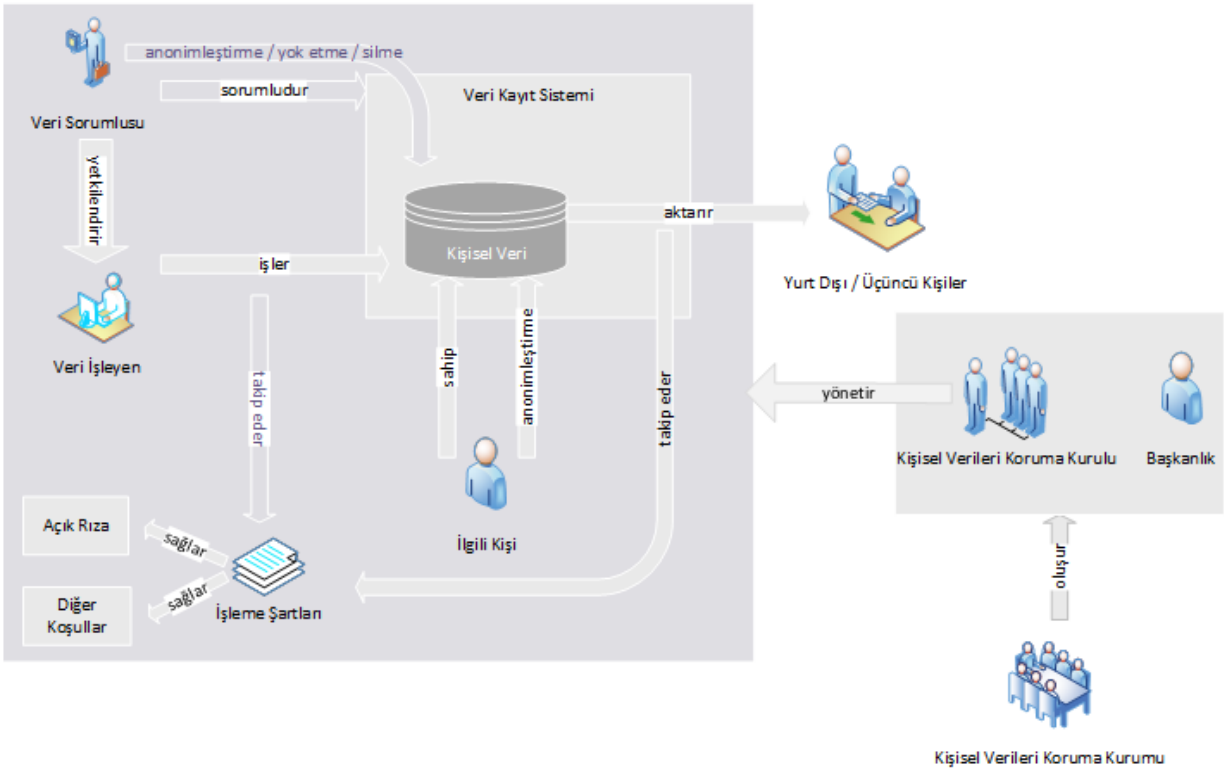
Onam Yönetimi sürecinde onam kontrolünü gerçekleştiren metot için sözde kod Tablo 5'de verilmektedir.

6. Onam Yönetimi Sistemi için Geliştirilen Anlamsal Çözüm

Hem KVKK hem GDPR'a göre kişinin verisinin erişilip işlenebilmesi için kişinin vermiş olduğu onam gereklidir. Kişinin onamına göre kişisel verinin işlenme sürecinin yönetiminde onam yönetimi önemli ve gerekli bir süreç haline gelmektedir. Beşinci bölümde KVKK metni TF-IDF metodu ile analiz edilerek sistemin aktörleri ve ilişkileri çıkartılmıştır. Çıkartılan sistem elemanlarının Onam Yönetimi Sistemi için işleyiş modeli sunulmuş ve Etkinlik Diyagramı çizilmiştir. Bu bölümde ise sunulan Onam Yönetimi Sistemine, onam bilgilerinin paylaşımın yapılabilmesi, aktörler ve kurumlar arasında birlikte çalışabilirliği sağlanması ve çıkarsamaların yapılabilmesi için anlamsal bir çözüm sunulmaktadır.

Anlamsal çözümlerin kullanıldığı sistemlerde, uygulamaların başarısı alan ontolojisinin ne kadar iyi tasarlandığına bağlıdır. Bunun nedeni, alan ontolojilerinin gerçek dünyadaki belirli bir uygulama alanının kavramsallaştırılmasını belirtmeyi amaçlamasıdır. Alan ontolojileri, ilgili alandaki kavramları ve bu kavramların aralarındaki ilişkileri tanımlamaktadır. Bu kavramlar ve ilişkiler kullanılarak onam yönetimine anlamsallık getirilmek için ilgili ontolojiler oluşturulmaktadır.

Anlamsal Onam Yönetimi için Onam Ontolojisi ve durum çalışması kapsamında geliştirilen Nabız Ontolojisi Protege ontoloji editörü kullanılarak geliştirilen iki yeni ontolojidir [71]. FOAF Ontolojisi, ihtiyacı karşılamadığı için genişletilmiştir. Alan Bağımsız Onam Yönetimi Ontolojisi ve E-Alan Ontolojisi, yeni geliştirilen ontolojilerin bir araya gelmesi ile oluşmuş yeni ontolojilerdir.



Şekil 4. KVKK'yı temel alan sistemin işleyiş modeli.

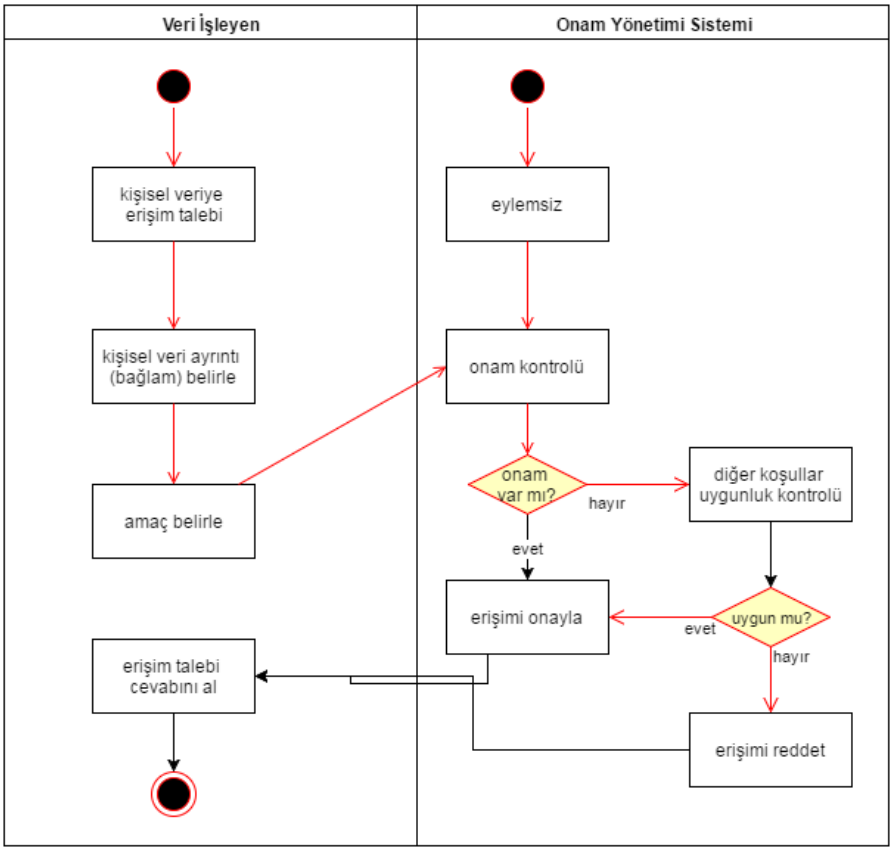
Figure 4. Operating model of the system based on KVKK

Tablo 5. Onam yönetimi algoritması için sözde kod.

Table 5. Pseudocode for consent management algorithm.

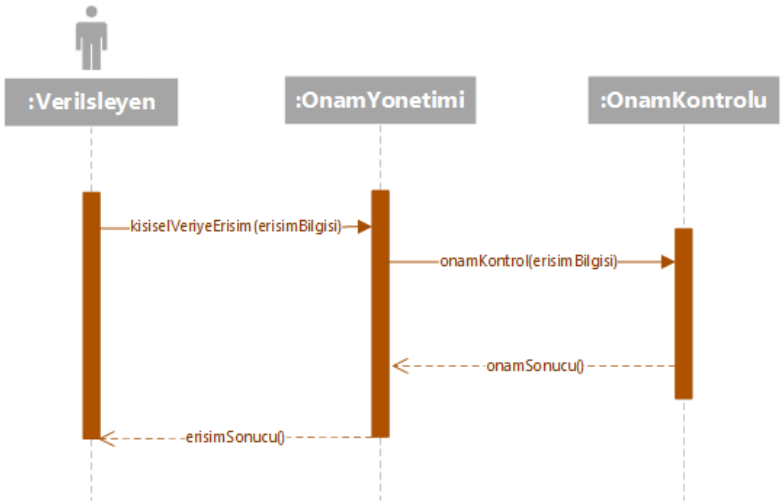
Algoritma: Onam yönetimi algoritması için sözde kod

```
Boolean consent = false;
foreach consentRequest in requestPool do
    purpose = restriction.getPurpose();
    process = restriction.getProcess();
    sensitivityLevel = restriction.getSensitivityLevel ();
    personalData = restriction. getPersonalData ();
    relevantPerson = restriction.getrelevantPerson ();
    consentData = createConsentData(purpose,porcess,sensitivityLevel,personalData,relevantPerson);
    consent  = consentControl(consentData);
end
if (consent)
    return true;
else
    return false;
end
```



Şekil 5. Onam Yönetimi Sistemi Etkinlik Diyagramı.

Figure 5. Consent Management System Activity Diagram.



Şekil 6. Onam yönetimi sistem ardıl-işlem diyagramı.

Figure 6. Consent management system post-process diagram.

Onam Ontolojisini oluştururken Ontology 101 [63] dokümanı temel alınmakta ve ontolojide yer alacak kavramların çalışıldığı alandaki nesnelere ve ilişkilere yakın olması gerektiğinden dolayı kanun metninden çıkartılan terimler kullanılmaktadır. Ontoloji içindeki nesneler TF-IDF metodu ile belirlenen terimlerdir. Yine bu terimler arasında fiil olarak cümlelerde bulunan kelimeler ise ilişkileri vermektedir. Çıkartılan ilişkiler şunlardır: Tutar, Sorumludur, Yetkilendirir, Anonimleştirir / yok eder / siler, İşler, Sahiptir, Aktarır.

Sınıflar tek başlarına yetkinlik sorularını cevaplama için yeterli bilgi sağlamamaktadır [63]. Yetkinlik sorularını cevaplayabilmek için bazı sınıfların veri nitelikleri tanımlanmalıdır. Bu nedenle, ontoloji sınıflarının belirlenmesinden sonra bu sınıfların veri nitelikleri belirlenmektedir. Tanımlanan veri nitelikleri şunlardır:

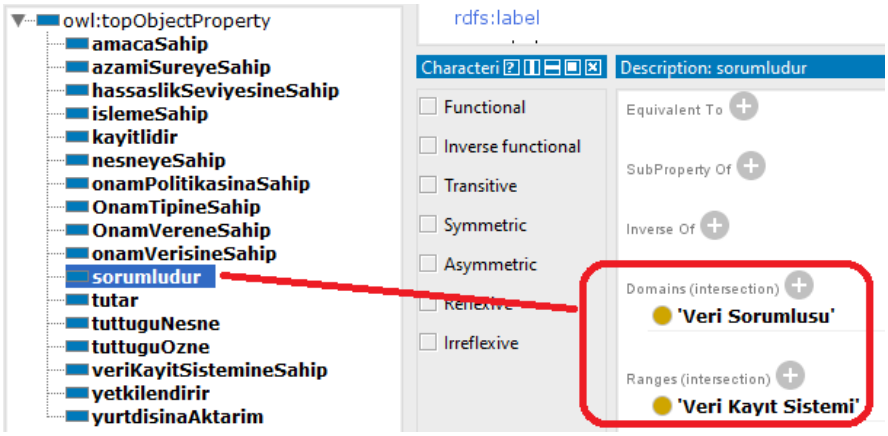
- ismeSahip: İlgili Kişi'nin ismi için tanımlanmış bir özelliktir.
- soyismeSahip: İlgili Kişi'nin soyismi için tanımlanmış bir özelliktir.

- adreseSahip: İlgili Kişi'nin ve Organizasyon'un adres bilgisini tutmak için tanımlanmış bir özelliktir.
- organizasyonIsmineSahip: Organizasyon'un ismi için tanımlanmış bir özelliktir.
- azamiSure: Kişisel Veri'nin saklanması gereken azami süreyi belirtmektedir.
- yurtdisi: Kişisel Veri'nin yurtdışına aktarılıp aktarılamayacağını tutan özelliktir.

Sonraki adım olarak niteliklerin veri tipi, izin verilen değer aralıkları ve niteliğin alabileceği değerler belirlenmektedir. Ayrıca, niteliklerin domain ve range değerleri girilmektedir. Geliştirilen Onam Ontolojisinde Şekil 7'de sunulan nitelikler için yine aynı şekilde yer alan domain ve range değerleri tanımlanmaktadır. Sorumludur niteliği için yapılan tanımlama Şekil 8'de sunulmaktadır.

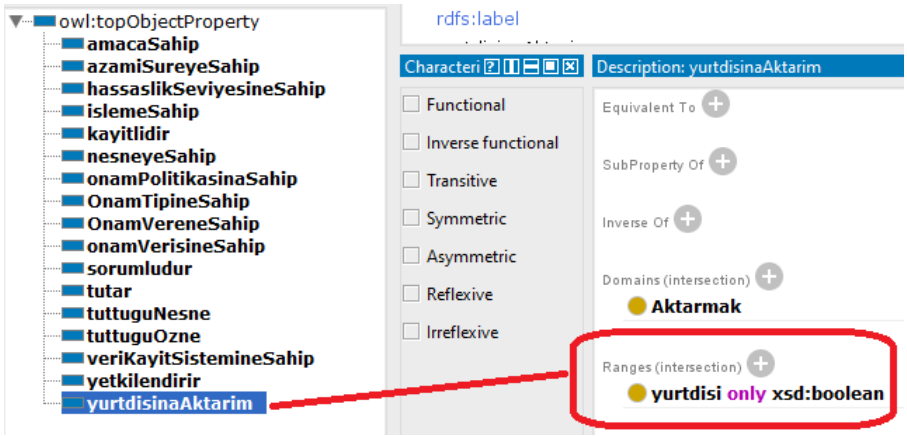
Nitelik kısıtı tanımlamada boolean, byte, string gibi veri tipi de tanımlanabilmektedir. Şekil 8'de boolean veri tipi tanımlaması sunulmaktadır.

Onam kontrolü mekanizmasını sadece bir alan için düşünmek ve planlamak hatalı olacaktır. Çünkü tüm bilgi sistemlerinde kişisel veriler tutulmaktadır. Bu nedenle geliştirilen onam yönetim sisteminde, onam kontrolünü gerçekleştirmek için bir üst (meta) onam ontolojisi geliştirilmektedir. Alan bilgisinden bağımsız olan bu üst ontolojinin, onam kontrolüne ihtiyaç duyan her sistemde kullanılabilmesi hedeflenmektedir. Alandan bağımsız olan bu onam ontolojisi, kullanılmak istenen alana ait ontoloji ile entegre edilerek ilgili alanda onam yönetiminin gerçekleştirilebilmesini sağlayacaktır. Böylelikle, önerilen onam yönetim sistemi kişisel verinin tutulduğu her alanda kullanılabilecektir.



Şekil 7. Nitelik kısıtı tanımlama.

Figure 7. Defining an attribute constraint.



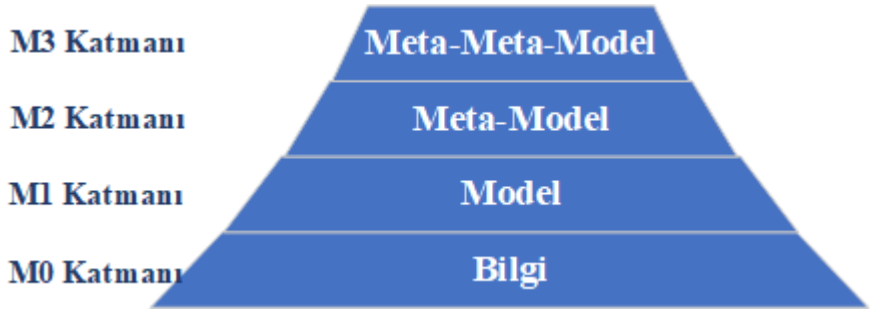
Şekil 8. Veri tipi ile nitelik kısıtı tanımlama.

Figure 8. Defining attribute constraint with data type.

Anlamsal Onam Yönetimi Sistemi için geliştirilen ontolojiler MOF yapısına göre katmanlara yerleştirilmiştir. MOF, model tabanlı mühendislik için Object Management Group [7] tarafından geliştirilmiş bir standarttır. MOF tabanlı standartlar, araçları, uygulamaları ve verileri entegre etmek için kullanılmaktadır. [73]'e göre, MOF, meta verileri ve verileri platformdan bağımsız bir şekilde tanımlamak, işlemek ve birleştirmek için genişletilebilir bir modele dayalı entegrasyon çerçevesidir. MOF, bilgi modellerini tanımlamak için bir model olarak kullanılabilir. Bu bağlamda, MOF Modeli bir meta-metamodel olarak adlandırılır, çünkü UML gibi metamodelleri tanımlamak için kullanılmaktadır. MOF, dört katmandan oluşan meta veri mimarisi tanımlamaktadır. Bu mimari Şekil 9'de verilmektedir.

MOF, teknoloji bağımsız meta-modelleri tanımlamak, oluşturmak ve yönetmek için soyut bir dil ve çerçeve tanımlamaktadır [74]. Şekil 9'de sunulan meta-model hiyerarşisindeki katmanlar şunlardır: (i) M3; meta-metamodel katmanı, (ii) M2; meta-model katmanı (iii) M1; model katmanı, (iv) M0; bilgi katmanı. Modellerin belirlenmesinde meta modeller kullanılır. Bu nedenle

katmanlı yapıda, her modelin üst katmanında o modeli tanımlayan üst-modeller bulunmaktadır.

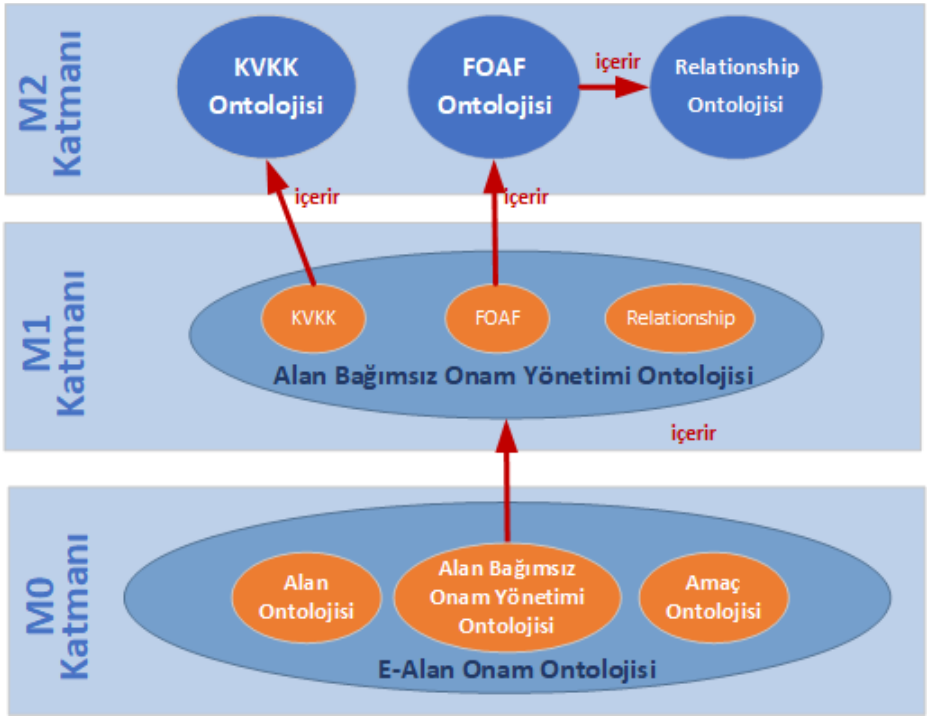


Şekil 9. MOF katmanları.

Figure 9. MOF layers.

Önerilen Onam Yönetim Sistemine ait bu ontoloji yapısı, MOF kapsamında Şekil 10'de gösterilmektedir.

M2 katmanında, KVKK Ontolojisi, FOAF Ontolojisi ve Relationship Ontolojisi almaktadır. KVKK Ontolojisi, KVKK temel alınarak çıkartılmış onam ontolojisidir. KVKK Ontolojisi bir üst ontolojidir ve bir alt seviyede bulunan Alan Bağımsız Onam Yönetimi Ontolojisi için üst sınıfları ve üst özellikleri tanımlamaktadır. Alan Bağımsız Onam Yönetimi Ontolojisi KVKK, FOAF ve Relationship Ontolojilerini içermektedir. FOAF Ontolojisi, kişileri ve bilgileri interneti kullanarak birbirine bağlayan bir [75]. Relationship Ontolojisi, aile, eş, meslektaş gibi kişiler arasındaki ilişkileri açıklayan bir ontolojidir [76]. FOAF ve Relationship ontolojileri alanyazında yer alan ontolojilerdir. Ancak, onam yönetimi gereksinimleri kapsamında bu ontolojiler genişletilmektedir [77]. Kişisel bilgileri tutan FOAF ontolojisi ve ilişkileri tutan Relationship ontolojisi, Consent ontolojisi ile entegre edilmiştir. Bu amaçla, FOAF, Relationship Ontolojisini ve Consent Ontolojisi, FOAF'ı içe aktarır. FOAF, yaş sınırlaması, kişinin rıza verme yeterliliği ve kişinin rıza bilgilerinin tutulması için genişletilmiştir. Relationship Ontolojisi, ebeveyn ilişkisini ve yasal temsilciyi tutmak için FOAF'ta genişletilmiştir. Consent Ontolojisinde, Kişi varlığına karşılık gelen Kişi sınıfı vardır. Bu Kişi sınıfı, FOAF ontolojisindeki Person sınıfıyla eşlenir. Böylece, FOAF ontolojisindeki Person sınıfının özellikleri, Consent ontolojisinde de kullanılabilir.



Şekil 10. Ontolojilerin MOF Bağlamında Yerleşimi.

Figure 10. Placement of Ontologies in MOF Context.

Onam Ontolojisi altında onam, *Prefix_Onam:izin* ve *Prefix_Onam:yasak* şeklinde tutulmaktadır. *Prefix_Onam:OnamPolitika* sınıfı *onamp:izin ve onamp:yasak* sınıfları ile *Prefix_Onam:onamTipineSahip* nesne özelliği aracılığıyla ilişkilendirilmektedir. Onam'ın verilmesi durumu örnek tanımlama seviyesinde *Prefix_Onam:izin* alt sınıfının değerinin true olmasıyla, onamın verilmemesi durumu *Prefix_Onam:yasak* alt sınıfının true olmasıyla gerçekleştirilir.

Prefix_Onam:izin ve *Prefix_Onam:yasak* alt sınıflarının veri tipi boolean olup, değerler baştan false olarak verilmekte ve istenen değer örnek oluşturmada true atanmaktadır.

Bu yapıda, *p* kişisi *f* FOAF profili ile tanımlanmaktadır. *p*'nin onam tipi *otp*, *ot £ {izin, yasak}* onam tipi setinin bir örneğidir. Kişinin yaşı page olarak tanımlanmaktadır. *p, otp | Person(p), OnamTipi(ot), onamTipineSahip(p, otp), yaş bilgisi yaşı(p, page)* tanımlamaları *p* kişisinin *f* FOAF profiliyle ilişkili olan onam tipi örneklerini oluşturmaktadır.

M1 seviyesinde yer alan Alan Bağımsız Onam Yönetimi Ontolojisi, M2'den gelen Onam ve genişletilmiş FOAF Ontolojisini kendi yapısına aktarmaktadır. Bir alt seviyede ise bu ontoloji bir alan ontolojisi ve alana özgü bir amaç ontolojisiyle E-Alan Ontolojisi içerisinde bir araya gelir ve onam yönetimi sürecini gerçekleştirir. Şekil 10'da sunulan ontoloji uzayında da görüldüğü gibi onam yönetimini gerçekleştirecek temel ontoloji olan Onam Ontolojisi bir üst ontoloji olarak geliştirilmiştir. Birlikte çalıştığı diğer üst ontolojiler ile onam yönetimine alan bağımsız olarak anlamsal bir çözüm sunulmuş olmaktadır.

KVKK ile banka, havayolu, sağlık, enerji, finans alanları başta olmak üzere kişisel verilerin tutulduğu her sistemde kişinin onamı gereklidir ve onam yönetimi süreci uygulanmak zorundadır. Kurala dayalı akıl yürütmenin yapılabilmesi için kural tanımlamalarının yapılması gerekmektedir. Yüksek seviye bağlamı, düşük seviye bağlam verilerinden muhakeme ile elde edilmektedir. Yazılan SWRL kural tanımlamaları etki alanları için ortaktır. Bu tanımlamalar oluşturulan E-Alan Onam Ontolojisi içerisinde yapılmaktadır. SWRL kural tanımlamaları Tablo 6'de verilmektedir. Tablo 6'de verilen kurallar sağlık alanı için yapılan tanımlamalardır. Farklı bir alan için tanımlamalar yapılacağında eegitim gibi prefix tanımı esaglik gibi ilgili etki alanının prefix tanımı ile değiştirilecektir.

Tablo 6. SWRL Kural Tanımlamaları

Table 6. SWRL Rule Definitions.

Kural Tanımı	SWRL Kuralı
Onam Verebilir	OnamOntolojisi:IlgiliKisi(?p) ^ eegitim:yas(?p, ?age) ^ swrlb:greaterThanOrEqual (?age, 18) -> foaf:canGiveConsent(?p, true)
Onam Veremez	OnamOntolojisi:IlgiliKisi(?p) ^ eegitim:yas(?p, ?age) ^ swrlb:lessThan(?age, 18) -> foaf:canGiveConsent(?p, false)
Ebeveyn İzni Alınır	OnamOntolojisi:IlgiliKisi(?p) ^ eegitim:yas(?p, ?age) ^ swrlb:greaterThanOrEqual (?age, 18) -> OnamOntolojisi:ebeveynKontrolu(?p, "Ebeveyn izni alınmalı")
Ebeveyn İzni Alınmaz	OnamOntolojisi:IlgiliKisi(?p) ^ eegitim:yas(?p, ?age) ^ swrlb:lessThan(?age, 18) -> OnamOntolojisi:ebeveynKontrolu (?p, "Ebeveyn izni alınmalı")
Kurumun yurtdışına izin vermemesi	OnamOntolojisi:islemeSahip(?policy, ?i) ^ OnamOntolojisi:yurtdisi(?i, false) -> OnamOntolojisi:onamTipineSahip(?policy, eegitim:onamYok)

7. Sonuç

Kişilik haklarından biri olan kişisel verilerin gizliliğinin ve güvenliğinin sağlanması için ulusal ve uluslararası alanda pek çok yasal düzenleme yapılmıştır. Kişisel Verilerin Korunması Kanunu, uluslararası antlaşmalar ve mevzuatlara paralel olarak hazırlanmış en geniş kapsamlı kanundur. Alanı bütüncül olarak kapsayan, sadece kişisel verinin korunmasına yönelik hazırlanmış bir kanundur. Kişisel verinin korunmasında güvenlik ve gizlilik yeterli değildir. Kişisel verinin işlenmesi için ülkemizde yapılan yasal çalışmalara ve uluslararası antlaşmalara göre kişinin onamı gereklidir. Kişinin onamına göre kişisel verinin işlenme sürecinin yönetiminde onam yönetimi gerekli bir kontrol sistemi haline gelmektedir. Türkiye'de 2016 yılının mart ayında kabul edilen Kişisel Verilerin Korunması Kanuna göre onam yönetimi üzerine herhangi teknik bir çalışmanın yapılmadığı görülmektedir. Bu çalışmada, KVKK'yı temel alan onam yönetimi sürecinin işlemesi için Anlamsal Web tabanlı bir onam yönetim sistemi önerilmektedir. Bu amaçla, öncelikle KVKK TF-IDF metodu ile analiz edilerek önerilen sistemin elemanları belirlenmektedir. Bu sistem elemanları ile genel bir sistem işleyişi sunulmakta, birlikte çalışabilirliğin ve çıkarsamaların desteklenmesi için anlamsal bir çözüm getirilerek geliştirilen ontolojiler anlatılmakta ve ontolojilerin yer aldığı katmanlı MOF yapısı sunulmaktadır.

Gelecek çalışma olarak, kişilerin onamlarının girilmesi, bu onamların güncellenmesi ve silinmesi, onamların yönetilmesi için bir uygulama geliştirilecektir. Onam çakışmasının tespiti gerçekleştirilecek. Kişisel veriye gelen erişim talebi, bu talebe karşılık yapılan onam kontrolü ve kontrol sonucu gibi işlemlerin denetlendiği ve kayıt altına alındığı bir denetim mekanizması eklenecektir.

Etik kurul onayı ve çıkar çatışması beyanı

Hazırlanan makalede etik kurul izni alınmasına gerek yoktur.

Hazırlanan makalede herhangi bir kişi/kurum ile çıkar çatışması bulunmamaktadır.

Kaynakça

[1] Anayasa. (1982). Türkiye Cumhuriyeti Anayasası. https://www.tbmm.gov.tr/anayasa/anayasa82.htm (Erişim Tarihi: 10.07.2022)

[2] Kişisel Verilerin Korunması Kanunu No 6698. (2016). Türkiye. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (Erişim Tarihi: 10.07.2022)

[3] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data - CETS No.108. (1985). Council of Europe.

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (Son Erişim Tarihi: 04.08.2022).

[5] Berners-Lee, T., Hendler, J., Lassila, O. 2001. The Semantic Web. Scientific American.

[6] Gruber R. T. 1993, Translation Approach to Portable Ontologies. Knowledge Acquisition, 5(2):199-220. doi:10.1006/knac.1993.1008.

[7] Object Management Group. 1997. "Meta-Object Facility (MOF)". http://www.omg.org/mof/ (Erişim Tarihi: 04.08.2022)

[8] https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/GDPR-Türkçe-Çeviri-AB-Bakanlığı.pdf (Son Erişim Tarihi: 04.01.2022).

[9] Türk Ceza Kanunu. 2004. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf (Erişim Tarihi: 04.08.2022)

[10] Türk Medeni Kanunu. 2001. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf (Erişim Tarihi: 04.08.2022)

[11] Türkiye Büyük Millet Meclisi. 2008. "Kişisel Verilerin Korunması Kanunu Tasarısı". 2008. http://www2.tbmm.gov.tr/d24/1/1-1009.pdf (Erişim tarihi: 04.08.2022)

[12] Ünver, H. A., Grace, K. 2016. Türkiye'de Veri Gizliliği ve Gözetimi: Kişisel Verilerin Korunması Kanunu Tasarısının Değerlendirmesi. Ekonomi ve Dış Politika Araştırma Merkezi.

[13] Kütükçü, A. 2017. Kişisel Verilerin Korunmasına İlişkin Mevzuat İncelemesi.

[14] Henkoğlu, T. (2017). Veri Koruma Kanununun Getirdikleri.

[15] Yildiz, S. 2017. Protection of Personal Data in Turkish Law. 22nd International Scientific Conference on Economic and Social Development, , 206–12.

[16] Kutlu, Ö. & Kahraman, S. (2017). Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi. Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi.

[17] Altınok Çalışkan, E. ve Öztürk, B. 2018. "Kişisel Verilerin Korunması Kanunu Hakkında Genel Değerlendirmeler ve Anayasaya Aykırılık Sorunu." http://openaccess.iku.edu.tr/handle/11413/3177 (Erişim Tarihi: 04.08.2022)

[18] Kartal, M. T. 2018. Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme. Uluslararası Ekonomi ve Yenilik Dergisi 4 (1) 2018: 1–18.

[19] Çekin, M. 2016. 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Bıg Data (Büyük Veri) Ve İrade Serbestisi Açısından Değerlendirilmesi. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 74(2): 629–44.

[20] OECD Home. 1980. "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data". http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Erişim Tarihi: 04.08.2022).

[21] Council of Europe. 1985. "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data - CETS No.108." http://www.coe.int/tr/web/conventions/full-list/-/conventions/treaty/108 (Erişim Tarihi: 04.08.2022)

[22] Official Journal of the European Communities. 1995. "Directive 95/46/EC of The European Parliement and of The Council". http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=CEL X:31995L0046:en:HTML (Erişim Tarihi: 04.08.2022)

[23] The Freedom of Information Act. 1966. https://www.gpo.gov/fdsys/pkg/STATUTE-80/pdf/STATUTE-80-Pg250.pdf (Erişim Tarihi: 04.08.2022)

[24] The Privacy Act. 1974. https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf (Erişim tarihi: 04.08.2022)

[25] Luger, E., Rodden, T. 2013. Terms of Agreement: Rethinking Consent for Pervasive Computing. Interacting with Computers 25(3): 229–41.

[26] Yu, B., Wijesekera, D., Costa. P. 2014. An Ontology for Medical Treatment Consent. CEUR Workshop Proceedings 1304: 72–79.

[27] Williams, J. B., Figley, T. 2016. System and Method for Providing Consent Management.

[28] Yu, B., Wijesekera, D., Costa. P. 2014. Consent-Based Workflow Control in EMRs. Procedia Technology 16(0): 1434–45.

[29] Grando, M. A., Boxwala, A., Schwab, R., Alipanah, N. 2012. Ontological Approach for the Management of Informed Consent Permissions. 2012 IEEE Second International Conference on Healthcare Informatics, Imaging and Systems Biology: 51–60.

[30] The EU GDPR.org. 2018. "The EU General Data Protection Regulation (GDPR)." https://eugdpr.org/ (Erişim Tarihi: 10.08.2022).

[31] The EU General Data Protection Regulation (GDPR). 2016. EU. https://gdpr-info.eu (Erişim Tarihi: 10.08.2022).

[32] Akyüzlü, M. 2017. "General Data Protectıon Regulatıon Nedir, Neler Getirmektedir?" https://www.peakup.org/blog/general-data-protection-regulation-nedir-neler-getirmektedir/ (Erişim Tarihi: 10.08.2022).

[33] Casellas, N., Bruce, T.R., Frug, S. S., Bouwman, S., Dias, S., Lin, J., Marathe, s., Rai, K., Singh, A., Sinha, D. and Venkataraman, S., 2012, Linked Legal Data: Improving Access to Regulations, In Proceedings of the 13th Annual International Conference on Digital Government Research, New York, 280–281.

[34] Casellas, N., 2012, Linked Legal Data: A SKOS Vocabulary for the Code of Federal Regulations, SemanticWeb-Journal.Org 0(0).

[35] SKOS Simple Knowledge Organization System. 1994. http://www.w3.org/2004/02/skos (Erişim Tarihi: 10.08.2022).

[36] Ziemer, J. 2016. "Loading Law & Regulations". https://finregont.com/loading-law-regulations/ (Erişim tarihi: 10.08.2022).

[37] Pwc. 2016. "Pulse Survey: US Companies Ramping up General Data Protection Regulation (GDPR) Budgets." https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-gdpr-series-pulsesurvey.pdf (Erişim Tarihi: 17.08.2022)

[38] TBMM. 2016. "Kişisel Verilerin Korunması Kanunu". http://www.kgm.adalet.gov.tr/DUYURULAR/6698KVKK.pdf (Erişim tarihi: 10.08.2022)

[39] Türk Dil Kurumu. "Büyük Türkçe Sözlük." http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.592558742166c2.96282838 (Erişim Tarihi: 10.08.2020)

[40] Tübitak Bilgem. 2011. TÜBİTAK – BİLGEM- Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü. http://www.bilgimikoruyorum.org.tr/?b121_bilgi-guvenligi-ne-demektir (Erişim tarihi: 10.08.2022)

[41] Pesen, M. M.. 2015. "Bilgi Güvenliği Nedir ve Nasıl Sınıflandırılır". https://www.sibergah.com/genel/bilgiguvenligi-nedir-ve-nasil-siniflandirilir/ (Erişim Tarihi: 10.08.2022)

[42] Şeremet, Ö. 2014. "BİT'in Gizlilik ve Güvenlik Boyutları." http://ozgurseremet.com/bitin-gizlilik-ve-guvenlikboyutlari/ (Erişim tarihi: 10.08.2022)

[43] Türkiye Büyük Millet Meclisi. 2008. "Kişisel Verilerin Korunması Kanunu Tasarısı". 2008. http://www2.tbmm.gov.tr/d24/1/1-1009.pdf (Erişim tarihi: 10.08.2022)

[44] Khomatov, A., 2008, Kişisel Gizliliği Sağlayan Biyometrik Doğrulama Sistemleri.

[45] Aladağ, C. E., Kurtarangil, E., Bahtiyar, Ş., 2014, Medikal Bilgi Sistemlerinde Güvenlik, Mahremiyet ve Kimlik Doğrulama, Akademik Bilişim, Mersin.

[46] Berber, L. K., 2010, Kişisel Sağlık Verilerinin Elektronik İletişim Yöntemleriyle İletimi, Standartları ve Çözüm Yolları, İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama Ve Araştırma Merkezi.

[47] Council of Europe. 1950. "Avrupa İnsan Hakları Sözleşmesi". http://www.echr.coe.int/Documents/Convention_T17R.pdf (Erişim tarihi: 25 Aralık 2019)

[48] Official Journal of the European Communities. 2000. "Avrupa Birliği Temel Haklar Sözleşmesi". http://www.europarl.europa.eu/charter/pdf/text_en.pdf (Erişim Tarihi: 10.08.2022)

[49] Berners-Lee, T., 1998, Semantic Web Road Map

[50] Berners-Lee, T., Hendler, J., Lassila, O., 2001. The Semantic Web. Scientific American

[51] W3C Semantic Web Activity. 2013. https://www.w3.org/2001/sw/ (Erişim Tarihi: 10.08.2022)

[52] Cardiff, J., 2009. The Evolution of the Semantic Web, Proc. of 2nd Workshop on Semantic Web and New Technologies (SemWeb09), Mexico, CEUR Workshop Proceedings vol. 534

[53] W3C Architecture. 2000. "Semantic Web - XML2000". http://www.w3.org/2000/Talks/1206-xml2ktbl/slide10-0.html (Erişim Tarihi: 10.08.2022)

[54] Resource Description Framework (RDF). 2004. RDF Working Group. http://www.w3.org/RDF/ (Erişim tarihi: 10.08.2022)

[55] RDF Schema. 2004. RDF Schema 1.1. https://www.w3.org/TR/rdf-schema/ (Erişim tarihi: 10.08.2022)

[56] Gruber, R. T. 1993. A Translation Approach to Portable Ontology Specifications, Knowledge Acquisition 5(2), 199–220 pp

[57] The Rule Markup Initiative. 2004. http://ruleml.org/index.html (Erişim Tarihi: 10.08.2022)

[58] O'Connor, M., 2009, The Semantic Web Rule Language, Protege Conference

[59] SWRL: A Semantic Web Rule Language Combining OWL and RuleML. 2004. https://www.w3.org/Submission/SWRL/#2 (Erişim Tarihi: 10.08.2022)
[60] Jupp, S., Horridge, M. 2008. "TerMine Plugin." https://Protégéwiki.stanford.edu/wiki/TerMine_Plugin (Erişim Tarihi: 17.08.2022)
[61] Cimiano, P., Völker, J. 2005. Text2Onto: A Framework for Ontology Learning and Data-Driven Change Discovery. Natural Language Processing and Information Systems: 227–238 pp.
[62] Trokanas, N., Koo, L. and Cecelja, F., 2018. Towards a Methodology for Reusable Ontology Engineering:
Application to the Process Engineering Domain, Computer Aided Chemical Engineering.
[63] Noy, N. F., McGuinness, D. L. 2001. Ontology Development 101: A Guide to Creating Your First
Ontology, Stanford Knowledge Systems Laboratory: 25 s.
[64] Frantzi K.T., Ananiadou S., Tsujii J. 1998, The C-Value/Nc-Value Method of Automatic Recognition for Multi-Word Terms, In Proceedings of the Second European Conference on Research and Advanced
Technology for Digital Libraries, ECDL, 585–604 pp.
[65] Wu, H., Luk, R., Wong, K., Kwok, K., 2008, Interpreting TF-IDF Term Weights as Making Relevance Decisions-Idf Mean?, ACM Transactions on Information Systems 26
[66] Navigli, R., Velardi, P., 2008, From Glossaries to Ontologies: Extracting Semantic Structure from Textual Definitions, Ontology Learning and Population 167: 71–87 ss.
[67] Kiryakov, A., Popov, B., Ognyanoff, D., Manov, D., Kirilov, A. and Goranov, M., 2003, Semantic Annotation, Indexing, and Retrieval, International Semantic Web Conference, 484-499 pp.
[68] Jurafsky, D., Martin, J. H. 2017. "Syntactic Parsing." In Speech and Language Processing,
https://web.stanford.edu/~jurafsky/slp3/12.pdf (Erişim Tarihi: 17.08.2022)
[69] Völker, J. 2008. Text2Onto.Neon-Toolkit. http://neon-toolkit.org/wiki/1.x/Text2Onto.html (Erişim Tarihi: 17.08.2022)
[70] Techopedia. 2012. "Named-Entity Recognition (NER)". https://www.techopedia.com/definition/13825/namedentity-recognition-ner (Erişim Tarihi: 17.08.2022)
[71] Can, Ö., Olca, E. 2019. Kişisel Verilerin Korunması Kanunu için Onam Ontolojisi Geliştirimi. Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi, 21 (62) , 559-575. DOI: 10.21205/deufmd.2019216220
[72] Hilsbos, M., Song, I. 2009. Use of Tabular Analysis Method to Construct UML Sequence Diagrams, Internation Conference on Conceptual Modeling
[73] Tang, W. 2009. Meta Object Facility, Encyclopedia of Database Systems, Springer, Boston.
[74] Fensel, D., Lausen, H., Polleres, A., Bruijn J. D., , Stollberg, M., Roman, D. and Domingue, J. 2010,
Enabling Semantic Web Services: The Web Service Modeling Ontology (1st ed.). Springer Publishing
Company, Incorporated.
[75] FOAF Vocabulary Specification 0.99. 2014. http://xmlns.com/foaf/spec/#sec-intro (Erişim Tarihi: 17.08.2022)
[76] http://vocab.org/relationship/ (Erişim Tarihi: 10.01.2022)
[77] Olca, E., Can, Ö. 2018. Extending FOAF and Relationship Ontologies with Consent Ontology, 2018 3rd International Conference on Computer Science and Engineering (UBMK), pp. 542-546, doi: 10.1109/UBMK.2018.8566297