BLG412 Bilişim Etiği

CRN:21896

Mahremiyet, Veri koruma ve Etik Üzerine Rapor

Yunus Güngör

No:150150701

1) Bilişim Çağı ve İnsanlığa Etkileri

Bilişim çağı, gelişmiş yarı-iletkenlerin keşfi sonucu bilgisayarların yaygınlaşması ve haberleşme teknolojilerindeki gelişmeler sonucu bu bilgisayarların birbirine bağlanması sonucu oluşmuştur aynı zamanda şuanda içinde yaşadığımız çağın ismidir. Tüm dünya çapında her türlü bilgiye anında ulaşabilme yetisinin insanlığa etkisi çok büyük olmuştur. Birçok insanın düşüncelerini paylaştığı bir bilgi ağı, birçok kişinin yararlı fikirlerinin işleme geçmesini sağlamış, kitlesel fonlama ile birçok yeni fikir ve ürünün insanlığın hizmetine sunulmasına yardımcı olmuştur. Kütlesel fonlama bu büyüklükte bir enformasyon ağının sağladığı faydalara sadece bir örnektir. Bu gelişmiş ağın yararları olduğu kadar zararları da bulunmaktadır. Yaşadığımız çağda bilginin çok değerli olması, insanları veri çalmaya ve insanlara karşı kullanmaya itmiş ve birçok ahlaki sorunu beraberinde getirmiştir.

2) Bilişim Çağında Bilgi

Bir kişiye ait olan bilgiler, o kişiye karşı kullanıldığında, kararlarını etkileyerek özgürlüğün kısıtlanmasına, maddi ve manevi zararlara sebep olabilir. Kötü niyetli insanlar sadece kişinin bilmesi gereken bilgileri, örneğin: kızlık soyadı, kullanarak kurum ve bireyleri kandırarak o kişi adına işlem yapabilirler veya aynı şekilde kişiyi kandırarak daha fazla bilgi çalabilir hatta maddi ve manevi zarar da verebilirler. Bu durumun fark edilmesi ve kötüye kullanılması sebebiyle her yerden erişebilen ve çok hızlı şekilde sınırsız defa kopyalanabilen verilerin ve bilgilerin korunması bilişim çağının en büyük sorunu haline gelmiştir. Sadece kişiler için geçerli olmayan bu durum devletlerin başta istihbarat teşkilatları olmak üzere tüm kurumlarında, şirketlerin gizli bilgileri, tescil ve şirket sırları için de geçerli olması bilginin değerini arttırmış ve verilerin korunması sorunun büyümesine sebebiyet vermiştir.

3) Bilginin Mahremiyeti

Bilişim çağının temel dayanağı olan, dünya çapındaki ağda yani internette kullanıcının isteğiyle veya isteği olmadan birçok veri toplanmaktadır. Kullanıcıların internete bağlandığı yer, yaşı, ismi vb. birçok veri kurumlar tarafından toplanmakta, kurumların isteğiyle veya isteği dışında üçüncü partilere aktarılmakta, veriler işlenerek yeni bilgiler ve varsayımlar türetilmekte, üretilen ve toplanan bu bilgiler kullanıcılara karşı veya onların yararına kullanılmaktadır. Genel olarak bu verilerin toplanma ve işlenme amaçları kullanıcı odaklı sistemlerin geliştirilmesi ve iyileştirilmesidir. Örneğin dünyanın en büyük arama motorlarından biri olan Google, yapılan arama ve diğer hizmetlerindeki verilerden yola çıkarak kişiye özel arama sonuçları oluşturmaktadır. Bu özelleştirme kişilere zaman kazandırmakta ve daha iyi bir internet deneyimi yaşamasını sağlamaktadır. Ancak aynı bilgiler Google'ın reklamlarında da kullanılmakta ve kişilerin özgür iradesini etkileyebilmektedir. Kullanıcıların verilerini kullanarak, almak istedikleri ürün veya hizmetin reklamlarını, kullanıcıya özel olarak

yayınlamak hem şirketler hem de kişiler için maddi kazanç sağlayabileceği gibi bazı yanlış anlaşılmalara yol açabilmekte, kullanıcının kararlarını etkileyebilmekte ve hatta kişilerin özel sırlarının başkası tarafından anlaşılmasına yol açabilmektedir. Bu duruma başka bir örnek ise Target firmasının genç bir kızın evine gönderdiği hamilelik ürünü kuponlarının, genç kızın babasının, kızının hamile olduğunu anlamasına sebebiyet vermesidir. Bu firma genç kızın yaptığı alışverişleri, genel olarak hamile bayanların yaptığı alışverişle eşleştirmiş ve adresine kampanya kuponları göndererek, kişiye ait bir sırrın açığa çıkmasına sebebiyet vermiştir; ayrıca firma, müşterilerinin alışverişlerini analiz ederek onlardan izinsiz bilgi toplamıştır (How Companies Learn Your Secrets,Duhigg,2012).

a. Verilerin Toplanması

Herhangi bir kurumun herhangi bir kişi hakkında veri toplamadan önce ilk olarak kullanıcıdan izin alması gerekmektedir. Kişilerin sahip olduğu bilgiler, bu kişiye ait mülkiyetidir ve bilgileri paylaşıp, paylaşmama özgürlüğü, özellikle kişisel olan bilgilerde, kullanıcıya ait olmalıdır. Fakat bilginin doğası gereği, kolaylıkla kopyalanabilir ve bilgi, bilişim çağının getirdiği yenilikler sayesinde anında başka bir yere aktarılabilir. Bu durum kurumların gözlem yaparak veya kullanıcının izni olmamasına rağmen direk kendisinden alarak birçok veriyi toplamasına sebebiyet vermektedir. Bilişim çağında her ne kadar bu bilgiler dijital ortamda, başka insanların gözlerinden uzakta bulunsa bile çeşitli durumlarda ortaya çıkması kötü sonuçlar oluşturmaktadır. Dolayısıyla kişilerin hangi bilgileri verip, hangi bilgileri vermeyeceğine karar verebilmesi gerekmektedir. Bu durumda kullanıcıdan izin istendiğinde, kullanıcılar sayfalarca süren hukuku anlaşmaları okumaya zaman ayırmak istemediklerinden, genel olarak bilgi toplamaya ve bu bilginin kullanımına iznin verirler. Her ne kadar hukuki olarak kurumun bu tutumu doğru olsa da, ahlaki olarak çok yanlış bir tutumdur. Kişilere hangi bilgilerin toplandığı kısa ve öz biçimde anlatılmalı ve kullanıcıların bu konuda bilinçlendirilmesi ve bilgilendirilmesi gerekmektedir.

Kuruluşların toplayabildiği her veriyi toplaması, hem hukuki hem de ahlaki bir sorun olmasıyla birlikte, bu verilerin depolanması ve işlenmesi kurumlara çok büyük iş yükü oluşturmaktadır. Toplanabilen her verinin toplanması yerine sadece kurumların ihtiyaç duyduğu, kuruma gerekli verilerin toplanması hem kullanıcı adına hem de iş yükü adına daha iyi bir seçenek olacaktır. Aynı şekilde kurumların sadece o anda ihtiyacı olduğu veriyi toplaması, daha sonra ihtiyaç duyabileceğini tahmin ettiği verileri toplamaması, ihtiyaç olabileceğini düşündüğü verileri yalnızca ihtiyaç duyulduğunda toplaması, kullanıcıya bilgi paylaşımında büyük bir kontrol verecek, ayrıca bilgilerin depolanması için gereken iş gücünü de azaltacaktır. Tüm bunların yanında hukuki ve ahlaki olarak uygulanması gereken sistem budur. Hatta mümkünse toplanan verilerin anonim hale getirilmesi bu bilgiler açığa çıktığında oluşabilecek

zararları azaltmakla birlikte verinin boyutunu da küçültecektir. Toplanan verilerin anonim hale getirilmesi, o verilerin herhangi bir kişiyle olan iletişimini keseceğinden bilginin kişinin kontrolünden çıkmasına sebep olmaktadır. Fakat her ne kadar bilgi kişiye ait olsa da, bu bilginin anonim hale getirilmesi verinin kullanıcıyla ilişkisini kestiği için kişinin kontrolünün bulunması gerekmemektedir. Anonim hale getirme işlemi düzgün ve kurallara uygun bir şekilde yapılmalıdır. Aksi durumunda arta kalan veri parçaları bilgi sahibinin kimliğini ele verebilir ve zaten bilgi üzerinde kontrolü bulunmayan kişi, verilerin anonim hale getirilmesinden zarar görebilir. Kişiyle bağlantı kurabilecek tüm veriler temizlenemediği durumlarda bilgi kesinlikle anonim hale getirilmemelidir ki bilgi sahibinin kontrolü sağlanabilsin. Ayrıca anonim bilgi toplanması, bilginin toplandığı kişiden izin alma yükümlülüğünü kaldırmaz. Hatta izin alınırken bilgilerin anonim olarak toplandığı belirtilmelidir.

Veri toplarken kurumların dikkat etmesi gereken başka bir husus ise verilerin sürekli güncel durumda tutulması veya güncel durumda tutulabilecek şekilde toplanmasıdır. Tarihi geçmiş veriler kullanıcılara zarar verebileceği gibi, bu veriyi kullanarak yapılan uygulamalarda da şaşırtmalara sebep olacaktır.

b. Verilerin Aktarılması veya Çalınması

Kurumlar tarafından izinli olarak toplanan veriler, başka bir kuruma aktarılırken veya aynı kurum içinde başka bir hizmette kullanılırken bilgi sahibinden tekrar izin alınmalıdır veya bilgi sahibinin daha önceden izin vermiş olması gerekir. Bazı durumlarda ise kurumların kontrolü dışında başka kurumlar daha önce toplanan bilgileri kullanabilir. Örneğin çerezler denen, web sitelerinin daha önce yapılan işlemleri ve sisteme giriş yapmış kullanıcıları tanımak için kullanılan küçük dosyalar, çerezleri oluşturan sitelerin dışındaki kurumlar tarafından öncelikle istatistik ve kullanıcı portföyü oluşturmak gibi çeşitli amaçlarla kullanılmaktadır. Bu tür bir durumda üçüncü parti olan kurumlar kullanıcıdan izin istemeli, mümkünse gerekli veriyi de anonim olarak toplamalıdır. Anonim bilgi toplarken dikkat edilmesi gereken ve yukarda belirtilen hususlar bu durumda da geçerlidir. Bir başka durum ise kurumun üzerinde depolanan bilgiye başka bir kurumun veya kişinin izinsiz olarak erişmesi ve bu bilgiyi başka bir konuma aktarması yani bilgi korsanlığı durumudur. Bu tür bir durumda bilgi güvenliğinin sağlanması bilgiyi toplayan kurumun sorumluluğundadır. Bilgi güvenliğini sağlayamayan kurum, veriyi çalan kişileri tespit etmeli ve anlık olarak kullanıcılarını bilgilendirmelidir. Daha sonrasında toplayacağı veriler için güvenlik sisteminin hatalarını düzeltmeli, gerekirse veri depolama ve işleme birimleri baştan sona yenilemeli, tüm testlerini tamamlamalı ve bilgi güvenliğini tekrar sağlayabileceği konuma geldikten sonra tekrar bilgi toplamaya başlamalıdır. Bilgileri çaldıran kurumun, etkilenen kişilerden özür dilemesi ve kullanıcılarından bilgi toplamak için tekrar izin istemesi ahlaki olarak uygun bir davranış olur. Bilgileri çalan kişi ve

kurumlara karşı hukuki bir mücadelenin başlatılması ise bir suçun cezasız kalmasını engelleyeceği gibi gelecekte olabilecek bilgi korsanlığı olaylarını da engelleyebilir.

Bilgiyi toplayan kurumun kontrolü dışında, kullanıcının sahip olduğu şifre, kullanıcı adı gibi özel erişim için gerekli olan anahtarların, kullanıcının bilgisayarından veya kişiye ait başka bir eşya aracılığı ile çalınması ise kullanıcının sorumluluğundadır. Kullanıcı sürekli kullanmadığı başka bir bilgisayardan erişim izni verdikten sonra, kurum tarafından kişiye bu bilgisayarın sahip olduğu erişim iznini kaldırması hatırlatılmalı ve normal olmayan erişim izinleri ve aktiviteler kullanıcılara bildirilmelidir. Kullanıcı gerekirse bir bilgisayarın iznini uzaktan kaldırabilmelidir. Böylece kullanıcının bilgilere erişim iznine sahip olan bilgisayarlar, sadece kişinin sahip olduğu bilgisayar ile sınırlandırılabilir. Ayrıca çalınma vb. gibi olaylarda, kullanıcının erişim iznini kaldırmasıyla; bilgisayarla birlikte kullanıcının verilerinin çalınması da önlenebilir. Tüm bu önlemlerden sonra erişim iznini yanlışlıkla vermiş veya hesabını açık unutmuş kullanıcıların bilgilerinin çalınması veya kullanıcının hesabı üzerinden aktarılmasından kurum değil kullanıcı sorumludur. Örneğin: Amazon adlı firmadan alışveriş yapan birçok kullanıcı, hediye almak istediği kişinin hesabındaki öneriler kısmını inceleyerek; hediyenin, alıcısı tarafından beğenilmesini garanti altına almaktadır. Hediyeyi alan kişinin Amazon hesabının bunun için kullanılması bu kişinin haklarını ve mahremiyetini ihlal etmektir. Fakat hesabının erişim iznini düzenlenmek kullanıcının sorumluluğundadır.

c. Bilginin Sentezlenmesi

Kuruluşlar tarafından toplanan tüm verilerin kullanılması için anlam kazandırmak gerekir. Verinin anlamdırılması ve düzenlenmesiyle bilgi sentezlenir. Birden fazla bilgi birleştirilerek başka bilgiler de sentezlenebilir. Bilgi sentezlenme işleminde bir takım çıkarımlar ve varsayımlar yapmak gerekir. Gerek istatistik yöntemler ile gerek mantıksal yöntemler ile işlenen verilerin nasıl işlendiği kullanıcı tarafından bilinmesi gerekmez. Hatta birçok durumda bu bilgilerin nasıl işlendiği ticari sır veya telif hakları kapsamına girebilir. Fakat sentezlenen bilgilerin ilgili kısımlarına kullanıcının erişim izni olmalıdır. Böylece kişi kendisiyle ilgili yanlış varsayım ve sentezlerin oluşmasını engelleyebilir, veri işleme sistemine katkıda bulunabilir. Kendisiyle ilgili oluşabilecek bilgi karmaşasının engellenmesi, herhangi bir hata sebebiyle kullanıcının zarar görmesini de engelleyecektir. Kullanıcının her zaman güvenilir olması, özellikle güvenlikle ilgili sistemlerde, tabi ki beklenemez; dolayısıyla kullanıcı tarafından yapılmak istenen düzeltmenin yetkili biri tarafından incelenmesi ve onaylanması gerekmektedir.

Kullanıcıların ilgili bilgilere ve verilere istediği zaman erişim sağlayabilmesi ya da bu verileri kendi bilgisayarına indirip inceleyebilmesi, bilgilerin doğruluğunu sağlayacak ve verilerin güncelliğini koruyacaktır. Kullanıcıların, kurumların elindeki yalnızca ilgili verileri elde edebilmesi hukuken ve ahlaki olarak doğru bir uygulamadır.

Ancak bu durumda erişilen verilerin güvenliğinde kullanıcılara büyük yük düşmektedir. Kişiler verileri görüntülemeden veya indirmeden önce kendi bilgisayarlarının güvenirliliğini sağlamalıdır.

d. Bilginin Kullanılması

Tüm verilerin toplanmasının ve sentezlenmesinin asıl amacı bu bilgilerin belirli bir yerde kullanılabilmesidir. Sitelerin reklam algoritmaları, alışveriş sitelerinin sizin için öneriler bölümü, sosyal medya sitelerinin fotoğraflarınızı otomatik olarak tanıması, oyunların kişinin tarzına göre şekillenmesi vb. birçok alanda üretilen ve toplanan bilgiler kullanılmaktadır. Bu bilgilerin kişiye karşı ve amacının dışında kullanılması kişiyi maddi ve manevi olarak etkileyebilir.

i. Özgür İradenin Kısıtlanması

Kullanıcıya verilen öneriler, kişiye fayda sağlayabileceği gibi, kişinin iyi veya kötü yönlendirilmesine de sebebiyet verebilir. Özellikle alışveriş sitelerinde kullanıcıların yanlış yönlendirilmesi sonucu, etkilenip alabileceği birçok ürün bulunmaktadır. Başka bir örnek ise: Andreas Lubitz adlı Germanwings adlı havayolu şirketinde çalışan bir pilot, son uçuşunda uçağı Alp dağlarına düşürürek, uçaktaki herkesin ölümüne sebep olmuştur. Olaydan günler önce ise arama motorlarında "kokpit kapıları" ve "intihar" kelimelerini aradığı tespit edilmiştir (Andreas Lubitz: Everything we know about Germanwings plane crash co-pilot, Sawer, 2015). Arama motorları Andreas'ın aramasındaki verileri kullanarak intihar yardım hatlarını veya psikolojik danışmanlık hizmetlerini sonuç olarak verilebilir ve birçok hayat kurtulabilirdi. Fakat bu yönlendirmenin her konuya yayılması ve aşırı olacak duruma gelmesi insanların özgür iradesini etkileyeceğinden ahlaki olarak doğru olmazdı.

ii. Verilerin Önemi ve Hassaslığı

Kullanılan verilerin kişinin hayatını ne kadar etkilediği, hangi verilerin toplanıp işleneceğini belirlemek için önemli bir etken olmalıdır. Kişinin din, dil, ırk, siyasi görüşü, sağlık ve cinsel yaşamıyla ilgili bilgiler hassas bilgilerdir. Hassas bilgilerin kullanılmaması, kullanılması gerekiyorsa mümkün olduğunca anonim hale getirilerek kullanılması gerekmektedir. Değerli olan veriler ise kişiden kişiye değişebilmektedir. Bir bilgi tek başına değerli olmasa bile, başka bilgilerle birleştirildiğinde ve sentez yapıldığında değerli bir bilgi üretilebilir. Kişilerin kurumların elindeki ilgili verilerin tümüne erişebilmesi bu sebepten ötürü de çok önemlidir. Sadece yanlış verilerin düzeltilmesi değil, kişiye göre değerli olan verilerin kurumdan silinebilmesi için de kullanıcılar, kurumların elindeki ilgili bilgileri görüntüleyebilmelidir.

4) Bilginin Korunması

Bu bilgilere erişebilecek programların ve personellerin kısıtlanması, güvenliği arttırır ve bilgi korsanlığının önüne geçebilir. Ayrıca verilerin toplanma amacı dışında

kullanılması, kişilere zarar verebilir. Dolayısıyla verilerin erişiminin çok dikkatli düzenlenmesi ve toplanma amacı dışında kullanımının engellenmesi gerekir. Bunu yapmanın basit bir yolu olmadığı gibi veri setine görüne değişik çözümler uygulanabilir. Teknik olarak gelişmiş ve güncel sistemlerin kullanılması, gerekirse bir danışman şirket veya kişiden yardım alınması bilgi korsanlığının önüne geçebilir.

5) Alınan Yasal Önlemler
    a. Türkiye'deki yasal önlemler

Dijital ortamda bulunan kişisel bilgilerin korunması için gerekli olan yasalar Türkiye'de 6698 nolu Kişisel Verilerin Korunması Kanunu ile korunmaktadır. Bu kanun tasarısı 24 Mart 2016 tarihinde TBMM Genel Kurulu'nda kabul edilerek yasalaşmıştır. Bu kanunun öncesinde Türkiye'de kişisel bilgileri koruyan özel bir kanun bulunmamaktaydı.

i. 6698 nolu kanun

6698 nolu Kişisel Verilerin Korunması Kanunu ile kişisel veriler, yasalar tarafından gerektirmediği veya kişilerin meşru menfaatlerine aykırı olmadığı durumlarda, kişinin açık rızası bulunmadan toplanamaz, düzenlenemez veya depolanamaz. Fakat birçok sistemin internet üzerinden çalışması sebebiyle, kişinin açık rızasının alınması ve bu rızanın geçerli olduğunu doğrulamak çok zor olabilir. Aynı zamanda bu yasa veri işlenmesini gerektiren sebeplerin ortadan kalktığı veya geçerliliğini yitirdiği veriler için yok edilmesini veya anonim hale getirilmesi gerektiğini öngörür. Kişisel Verilerin Korunması Kanunu, veri sorumlusuna, veri üstünde yapılan her işlem hakkında ilgili kişileri bilgilendirme sorumluluğunu yükler; ilgili kişiler ise kendisiyle ilgili olan bilgilerin işlenmesiyle ilgili bilgi talep edebilir. Verilerin işlenmesi, verilerin elde edilmesi, depolanması, değiştirilmesi, başka bir tarafa aktarılması veya açık hale getirilmesini kapsar. Kendi verileriyle ilgili bilgi alan kişi hataların düzeltilmesini de talep edebilir. Verilerin güvenliğini sağlamak ise veri sorumlusunun görevidir.

6698 nolu yasa, bağımsız bir Kişisel Verileri Koruma Kurulu kurulmasını da öngörür. Verilerin işlenmesiyle ilgili sıkıntılar, şikâyetler veya güvenlik açıkları kuruma bildirilerek yayınlanması veya çözümlenmesi sağlanabilir. Bu kurul, şikâyetleri karara bağlamakla yükümlüyken, hukuki anlamda bilirkişi gibi görev yapmaktadır.

Kişisel Verilerin Korunması Kanunu her ne kadar birçok durum için eskiden olmayan düzenlemeler getirmiş ve Türkiye'de kişisel veriler ve mahremiyet konusunun hukuk ile bağlantısını kurmuş olsa da, kanundaki birçok madde yorumlamaya çok açık durumdadır. Diğer maddelerin çoğu ise kurul ve yönergelere bağlanmıştır. Bu esnek ve hızlı değişen bir yapı oluşturmak için doğru bir hamle olsa da, kurul ve yönergelerin kanun üzerindeki etkilerinin azaltılması ve kanunun daha kesin bir hale getirilmesi gerekmektedir.

b. Dünya’daki önlemler

Dünya çapında alınan önlemlerde iki öncü kuruluş bulunmaktadır: Amerika Birleşik Devletleri ve Avrupa Birliği. Türkiye’de yeni kanunlaşan 6698 nolu yasa, Avrupa Birliği tarafından oluşturulan ilke ve yasalara benzemektedir. Avrupa Birliği tarafından oluşturulan yasalarda, kanunlarla belirtilen durumlar dışında kullanıcının rızasını almak gerekmektedir. Ayrıca amacı yerine getirmek için gerekenden daha fazla bilgi toplanması kanun ile yasaklanmış ve bilgilerin güncel ve doğru olması, yasalar tarafından zorunlu kılınmıştır. Türkiye’den farklı olarak, verilerin kayba uğramaması için alınması gereken önlemler de yasalarca zorunlu hale getirilmiştir. Amerika Birleşik Devletlerinde ise soruna yönelik özel çözümler üretilmişken, yasalar genel olarak aynı esaslar üstüne kuruludur. Kişiler, kendileriyle ilgili tutulan bilgileri öğrenebilir ve düzeltebilirler, bu bilgilerin tutulma ve kullanılma amaçlarını da öğrenebilirler. Veri kaydını tutan kuruluş, verilerin güvenliğinden ve bilgilerin doğruluğunun sağlanmasından sorumludur. Bu esaslara ek olarak varlığı gizli bir veri kaydı sisteminin olamayacağı da belirtilmiştir.