

Gözetlenen Değil Gözetilen Veriler

Fatma Büşra FIRAT, 11 Nisan 2022

<https://www.hukukvebilisimdergisi.com/yapay-Zekâ-ve-kisisel-veriler/>

Giriş

Bugün, adını sıkça duyduğumuz, hemen her yerde karşılaştığımız; maruz bulunduğumuz yahut maruz bırakıldığımız **yapay Zekâ ve kişisel veriler**, bir bütünü besleyen parçalar gibidir. Öyle ki, yapay Zekâ bir insan olsa, en büyük besin kaynağı veriler olurdu. Bu kadar veri açlığı içinde olan bir teknolojiye tüketip saklaması, sindirip kullanması ve çıkarımlarda bulunması için birtakım veriler sunulurken, etik değerlerin göz ardı edilebileceği ve bazı hakların ihlal edilebileceği de bir gerçektir. Peki bir yapay Zekânın temel besin kaynağına veri derken tam olarak neyi kastediyoruz? Buna cevap vermeden önce gelin, yapay Zekânın ne anlama geldiğine bir bakalım.

Tanım

Yapay Zekâ, tanımı yapılması zor bir alan olsa da ACM tarafından; çevreyi algılayan, öğrenerek yeni bilgiler üreten, problem çözebilen, yazılım ve donanımları gerçekleyen bir bilim dalı olarak ifade edilebilir.

İlk kez bilgisayar bilimci John McCarthy tarafından 1950’de bir konferansta kullanılan yapay Zekâ terimi, bir anlamda makinelere, normalde insan Zekâsına ihtiyaç duyulan işleri yaptırma teknolojisidir.

Bir sistem veya makine düşünün. Anlama, iletişim, öğrenme gibi beyinsel aktiviteleri yerine getirmede insan Zekâsını taklit etsin. Hatta öyle ki bir habere göre siber dolandırıcılar tarafından bir CEO’nun sesini taklit ederek 1 milyonun üzerinde bir parayı çalabilecek kadar bu taklitte başarılı olsun. Microsoft gibi bazı teknoloji şirketleri tarafından performans ölçüm hizmeti adı altında çalışanlarının vücut hareketleri, mimikleri, ses tonları gibi detaylardan ölçüm yaparak çalışılan işte verim analizi ortaya koysun ve belki de çalışanları işten çıkarmada geçerli fesih sebeplerini işverenin imkanına sunsun.

İşte tüm bunlara imkân veren yapay Zekâ teknolojisinde algoritma yazılırken yapay Zekâya öğretilen, neyin kararını vereceği değil, nasıl bir karar vermesi gerektiği olacaktır. Buna, makine öğrenmesi denilmektedir.

Yapay Zekâyı da İçine Alan Big Data

Teknolojinin hızlı ilerleyişı ve verilerin öneminin artması ile big data denen; yapay Zekâ, veri bilimi ve nesnelerin interneti gibi birçok dijital dönüşüm uygulamasını içine alan bir itici güç ortaya çıkmış, bu kadar veri ile kendi yararımıza neler yapabileceğimizin sorusu gündeme gelmiştir.

Aslına bakarsanız big data şunu ilke edinmiştir: Ne kadar çok veri, geleceğe ilişkin o kadar güvenilir tahmin ve saptama demektir. Öte yandan geçmişten günümüze veri kavramı da epey anlam genişlemesine uğramıştır. Bugün bakıldığında elektronik kablolar veya veri tabanları ile sınırlı verilerin yerini fotoğraf, video, ses kayıtları, yazılı-sözlü metinler, sensör verilerine kadar pek çok şeyi içine alan bir veri anlayışı almıştır. Tüm bu dağınık verileri anlamlı bir hale getirebilmek için büyük veri projeleri; yapay Zekâ ve makine öğrenimini içeren bazı analizler kullanır. Bilgisayarlara da bu verilerin neyi temsil ettiğı öğretilir. Büyük veri projelerinin sağlık, eğitim, ekonomi, suç bilimi ve hatta doğa olaylarına varıncaya kadar pek çok konuya müdahalesi ile veriye dayalı analizler elde edilmektedir.

Hastalıkların erken teşhisi, çok sayıda tıbbi kayıt ile yeni ilaçlar geliştirme yollarına gitme; birtakım sensör verileri ile olası depremlerin şiddetinin hayat kurtaracak bir zaman aralığında tespiti; bir suçun önlenmesinde ekiplerce veriye dayalı yöntemlerin geliştirilmesi gibi apayrı pek çok konuda hayatı kolaylaştırıcı bir etkisi olduğunu ve olacağını söylemek mümkünse de bu işin endişe veren boyutlarını da es geçmemek gerekir.

Covid Döneminde Arkamızda Bıraktığımız İzler, Kişisel Veriler

Gündelik yaşamımızda pandeminin de etkisi ile dışarı bile çıkmamız gerekmeden, evlerimizi adeta home office olarak kullandığımız şu günlerde alışverişlerimiz, yaptığımız çalışmalar, konuşmalar, sıkıldığımız bir anda çekip paylaştığımız fotoğraflar, sipariş ettiğimiz belki bir ayakkabı, bir yemek, uzun zamandır göremediğimiz bir arkadaşımıza yazdığımız özlem mesajına kadar yüzlerce veriyi sanal ortama bırakmaktayız. Ürettiğimiz bu kadar çok verinin pek çoğunu gizli tutma hakkına sahip olsak da bu veriler güvenilir ellere teslim midir, orasını pek bilemeyiz. İçimize kurt düşse de bazen, çoğu kez bu büyük veri destekli uygulama ve hizmetlerin sunduğı kolaylığı ve rahatlığı tercih eder, bu kolaylığın karşısında birkaç kişisel verimizi paylaşmaktan zarar gelmeyeceğini düşünürüz. Hatta çoğu kez kendimizi ve verilerimizi pek de önemli

görmez, kendimize ait bu bilgilerle en çok neyin yapılabileceğini düşünüp içimizi rahatlatırız. Oysa hep duymuşuzdur, hatta klişe bir hal de almaya başlamıştır artık: “Bir uygulama ücretsizse orada ürün, veri sahibidir.” Bu bile verilerimizin arka planda tedavül gücünü göstermektedir.

Verilerimizi Neden Korumalıyız?

Verileri korunmaya muhtaç kılan en önemli unsur, bizimle her yere gidiyor olması, mekanlarla ve kurumlarla sınırlı olmamasıdır. Veri akışı esnasında o verinin veri sahibine ait olduğunun bilincinde olunarak hareket edilmesi ve bu akış sırasında tabir yerinde ise “kötü adamlar” olarak nitelendirebileceğimiz kişilerce siber güvenliğin tehdit edilerek veri sahibinin alanına müdahale edilebilecek girişimlerden kaçınılması beklenir. Çünkü veriler, yapay Zekâ teknolojisi içinde çok büyük bir katma değere sahiptir ve bu sebeple kötü niyetli kullanımlara açık bir alan olabileceği de bir gerçektir.

Buraya kadar veri sahiplerinin rızaen paylaştığı verilerinin kullanımından bahsetmiş görünsek de işin hukuka aykırı boyutu, bizler nelere rıza gösterdiğimizi sanırken veri sorumlularınca bu rızanın içine daha başka nelerin de dahil edilebildiği kısmıdır. Özellikle kamuyu, tüm dünyayı ilgilendiren ve hakkında baştan beri pek de bütünsel bir bilgiye vakıf olunamayan pandemi sürecinde halkın yararına olduğu düşüncesi ile verilerin önemi artmış, bu kişisel verilerin kullanılması konusunda eskiye nazaran bir esnetme politikası uygulanmıştır. Örneğin daha sağlıklı bir toplum düşüncesi ile virüs barındıran bireylerin tespiti ve izlenmesine ilişkin devlet politikaları ortaya çıkmış ve garip bir şekilde süreç, veri sahibi olan bizleri, bu bilgilerimizin paylaşılmasına zorunlu bir rıza gösterir hale getirmiştir. Bu noktada insanlarda bireyin çıkarının toplumun çıkarına nazaran daha fazla bir öneme sahip olmadığı düşüncesi hâkim olmuştur. Böylece daha büyük bir amaç için belki de en önemli şeyden, verilerimizden biraz da olsa istifade ederken bulmuşuzdur kendimizi.

Birçok şirket şu an bu kadar veri ellerindeyken niçin kamu yararına bu verileri kullanmayacağını tartışıp olayı basite alsa da pandemi süreci bittikten sonra halihazırda bu verilerin imha edileceği bir ortam yaratılmadığı takdirde işin büyüyen bir tehlikeye doğru yol alması kaçınılmaz hale gelecektir. Zira yapay Zekânın beslendiği veriler, sektör için büyük bir ekonomik kaynak olma potansiyeline sahiptir ve her geçen gün ve her an veri üreten bizler için bu işin sınırını çizmek de gün geçtikçe zorlaşacaktır.

Şimdilerde söylenen aşı faaliyetlerinin zorunlu tutulmayacak olması, aslına bakılırsa veri paylaşma noktasındaki zorunlu tutulmayışa bir anlamda benzemektedir. İkisinin de zannımca şöyle tehlikeleri vardır, her ne kadar iradi de gösterilse, örneğin aşı olmayan birinin bazı işlere alınmayabilmesi, bazı alışveriş merkezlerine girememesi, bazı hizmetlerden yararlanamaması gibi ihtimaller olacaktır. Aynı şekilde veri paylaşımından kaçınan biri için de hizmet sağlayıcıları aynı iradeyi gösterebileceklerdir. Tüm bunlar, verilerimizi paylaşıırken ne kadar iradi davranabildiğimizi sorgulatır hale gelecektir.

İşin hukuka aykırı bir başka kısmı da lokal veri paylaşımının sınırlarının aşılmasıdır. Örneğin yalnızca konum bilgisinin gerektiği bir uygulama kullanılırken kullanım izninin, ayrıca veri sahibinin telefon rehberi bilgisine de ulaşma iznini kapsaması, tek bir izin sistemi ile aslında uygulamanın amacının dışına çıkan veri paylaşımının da önünün açılması, kişisel verilerin ihlali anlamına gelecektir.

Veri sorumlularının verileri paylaşmada denetim mekanizmalarına tabii tutulması beklenmektedir. Bu yolla, bir teknikler bütünü olan yapay Zekânın amacının insan ya da hayvan zekâsını makine kullanımı yoluyla taklit ederken o insanın yahut hayvanın yerine geçme amacı taşımaktansa bu canlıların hayatını kolaylaştırma noktasında bir araç olarak faaliyet göstermesi gerekir. Teknoloji, nihai bir çözüm değil, çözüme giden yolda bir araç olabilir ve sağlıklı bir işleyiş için sosyal değerlerden ödün verilmemelidir.

Siber Güvenlik Noktasında Zero Trust

Kişisel verilerin korunmasında siber güvenlik ve blockchain de önem arz etmektedir fakat yeterli değildir. Bu anlamda varsayımsal güven, sorun yaratabilmektedir. Bir uygulamayı tek başına güvenli kılmaktansa zero trust (sıfır güven) kapsamında güven duygusunu bütüne yaymak amaçlanmalıdır. Kimlerin verilerimize ulaştığı, ulaşma yetkilerinin olup olmadığı ve verilerimizin nerede durduğu/dolaştığı gibi soruların öncelikle cevaplanması gerekir. Bu sebeple veri sahipleri olarak “hemen güvenme, önce doğrula, sonra aksiyon al” şeklinde bir yöntem izlenmelidir.

Verilerin Korunmasına İlişkin Bazı Yasal Düzenlemeler

Veri ihlalinde asıl tehlike grupları, basit hackerlar olabileceği gibi politik organizasyonlar ve ticari yarar sağlayan dolandırıcılar da olabilmektedir. Bu noktada ülkemizde 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren KVKK, bizlere önemli ölçüde yol göstericidir. Anayasanın 20.maddesinde temel bir hak olarak

düzenlenen kişisel verilerin korunmasını isteme hakkı,2010 Anayasa değişikliği ile özel hayatın gizliliğini düzenleyen sınırlar çerçevesinde diğer hak ve özgürlükler lehine sınırlandırılabilir.

Kanunu daha da işler kılabilme ve denetimler yapabilmek için Kişisel Verilerin Korunması Kurumu hayatımıza girmiştir.

Kanun; uluslararası belgeler, karşılaştırmalı hukuk uygulamaları ve ülke ihtiyaçlarımız göz önünde tutularak kişisel verilerin çağdaş standartlarda işlenip koruma altına alınmasını amaçlamaktadır.

Kişisel verilerin korunması kanunu, mahremiyetin korunup veri güvenliğinin sağlanmasını önceler. Bu yolla kişisel veriler sınırsız ve gelişigüzel toplanmayacak, yetkisiz kişilerin erişimine açılmayacak, amacının dışında ve kötüye kullanılmayacak, ifşa edilmeyecektir.

Kanun, veri sahibi gerçek kişiler ile bu verileri tamamen ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişileri kapsamına alır. Veriden ziyade veri sahibini korumaktadır.

Kimliği belirli yahut belirlenebilir gerçek kişiye ait her türlü bilgi, kişisel veridir. Bu açıdan bakıldığında bir şirketin ticaret unvanı ya da adresi, gerçek kişi ile ilişkilendirilemediği sürece kişisel veri sayılmamaktadır. Gerçek kişinin fatura bilgilerinden mektup ve davet yazılarına, ses veya görüntü kayıtlarından kredi kartı ekstrelerine kadar pek çok kayıt, kişisel veridir.

Bir de özel nitelikli kişisel veriler vardır ki bu veriler, başkalarınca öğrenildiğinde veri sahibinin mağduriyeti ve ayrımcılığa maruziyeti sonucunu doğurabilecektir. Kişilerin ırkı, dini, sağlığı, mezhebi, siyasi düşüncesi, cinsel hayatı, felsefi inancı, kılık ve kıyafeti, vakıf ve sendika üyeliği, ceza mahkumiyeti ve güvenlik tedbirleri ile ilgili biyometrik ve genetik veriler, bunlara örnektir. Özel nitelikli kişisel verilerin işlenmesi için mutlaka ilgilinin açık rızası aranır.

Kişisel verilerin işlenmesi; bu verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi demektir. Kanunun 6.maddesinin 3. fıkrasında, özel nitelikli kişisel veri olan sağlık ve cinsel hayata ilişkin verilerin ancak

kamu sađlıđının korunması, koruyucu hekimlik, tıbbi teřhis, tedavi ve bakım hizmetlerinin yrtlmesi, sađlık hizmetleri ve finansmanının planlanması ve ynetimi amacıyla sır saklama ykmllđ altında bulunan kiřiler veya yetkili kurum ve kuruluřlar tarafından aık rıza aranmadan iřlenebileceđi yer almaktadır. Fakat zel nitelikli verilerin iřlenmesinde ayrıca Kurulca belirlenen nlemlerin de alınması řarttır.

Hukuka uygun bir kiřisel veri iřleme faaliyeti gerekleřtirilebilmesi iin kiřisel verilerin ncelikle kanunun 5. Maddesindeki řartlardan birine dayanılarak iřlenmesi gerekir fakat her halkrda madde 4'te sayılan temel ilkelere uyulması da řarttır. Kanunun 7. Maddesine gre iřlenmesine rađmen, iřlenmeyi gerektiren sebeplerin ortadan kalkması halinde resen veya taleple kiřisel verilerin silinmesi, yok edilmesi veya deđiřtirilmesi gerekmektedir fakat kiřisel verilerin iřlenmesi, bařtan beri hukuka aykırı ise derhal silinmeli, hukuku uygunluk en kısa srede tesis edilmelidir.

Bazı zamanlarda anonimleřtirmeden bahsedilse de bu tek bařına yeterli olmayacak, eđer farklı st veriler ilgilinin kimliđini tespit imknı veriyorsa yine ihlaller kaınılmaz olacaktır.

Kamuya aık alanlarda inřaat iřisinin baretini takip takmadıđı gibi alıřılan ortamı, alıřanların davranıřsal yapısını, izleyip denetleyen yapılar, sanılanın aksine iř verimini de dřrebilecektir, yine bu tarz durumlar iin nceden hukuki nlemler alınmalıdır.

Trk Ceza Kanunu 135-140 ve 243-246 maddeleri kiřisel veriler ve biliřim sistemleri zerine iřlenebilen suları ve yaptırımlarını dzenlemektedir.

Peki Ne Yapmak Gerekir?

Kiřisel verilerin korunması noktasında karřı olunan unsur, verilerden deđer elde edilmesi deđer; bu verilerin kullanımının hakkın ihlaline yol aacak řekilde yapılmasıdır. Mahremiyet korunmadıka, siber gvenliđe iliřkin riskler hep devam edecektir. İřverenlerin, iřilerinin alıřmalarında kendi internetlerini kullanmalarına iliřkin teřvikleri ve bu konuda bilgilendirici eđitim faaliyetleri dzenlemeleri, bu konuya olan hassasiyetlerini belli edecektir. Baskıdan uzak bir ortamda kiřisel verilerin paylařılmasına iliřkin izin istenmeli, veri sahiplerinin rızalarının olabildiđince geređi yansıtması amalanmalıdır. İnsan kontrolnde yapay Zek sistemleri geliřtirilmelidir. Minimum veri ile alıřan sistemler retilmeli, sre ve yazılımlar veri koruma amacıyla tasarlanmalıdır. Elde edilen veriler bařka verilerin elde edilmesinde kullanılmamalıdır.

Veri işlerken risk değerlendirmeleri yapılmalı ve bu esnada yapay Zekâ ile big data özellikleri göz önünde tutulmalıdır. Verilerin korunması ilkesi (data protection by design) gözetilmeli, zaten her yanımızı sarmış olan önyargıların yapay Zekâ teknolojisinden arındırılması gerekmektedir. Veri açıklığını giderme noktasında gerçek kişisel verileri modelleyen temsilci veriler kullanılabilir. Yapay Zekâ geliştiricileri, satıcıları ve kullanıcıları hesap verilebilir bir algoritma kurmalı ve olası bir sorunda muhatap bulma açısından veri sorumlularının kim olacağı aydınlatma metni ile belirlenebilmelidir. Veriler toplanırken Avrupa Veri Koruma Tüzüğü ve KVKK dikkate alınmalı, yapılması gereken bir değişiklik olacaksa bu, KVKK madde 28 deki istisnalar kapsamına sokularak değil, ayrı bir kanun maddesi düzenlenerek yapılmalıdır. Mahremiyet olmadan güvenliğin olmayacağı unutulmamalı; gizlilik, güvenlik ve doğruluk endişeleri bir an evvel giderilmelidir.

Son olarak...

Bu kadar kapsamlı bir konuyu ele alırken yazımı Denzel Washington'un bir sözüyle noktalamak isterim: "Hayatını yaşa ve bunu gizli tut. Mahremiyet her şeydir."

Yapay Zekâ Hukuku alanındaki tüm Blog yazılarımızı [bağlantıdan](#) okuyabilirsiniz.

Kaynakça

https://www.academia.edu/42073914/Algoritmik_Karar_Verme_ve_Veri_Korumas%C4%B1

<http://www.diken.com.tr/yapay-Zekâyla-ceonun-sesini-taklit-edip-243-bin-dolar-caldilar/>

<https://www.mynet.com/amp/microsoft-yapay-Zekâ-ile-enerjisi-dusen-calisanibulacak-110106666850>

<https://elifbabanhukuk.com.tr/yapay-Zekâli-sistemlerde-etik-kurallar/>

<https://www.istanbulbarosu.org.tr/HaberDetay.aspx?ID=15738&Desc=Yapay-Zekâ-%C3%87a%C4%9F%C4%B1nda-Hukuk>

<https://berqnet.com/blog/kvkk-nedir>

TCK ilgili maddeler

KVKK ilgili maddeler