Araştırma Makale | Research Article

KHM, Cilt:6 Sayı:2, 2026, s. 761-787.
Geliş Tarihi | Received: 30.06.2026
Kabul Tarihi | Accepted: 30.10.2026
Yayın Tarihi | Published: 30.10.2026
doi: 10.59909/khm.06.02.012

İntihal | Plagiarism: Bu makale, en az iki hakem tarafından incelendi ve intihal içermediği teyit edildi.
| This article has been reviewed by at least two referees and scanned via a plagiarism software.

BİRLEŞMİŞ MİLLETLER'İN KİŞİSEL VERİLERİN KORUNMASINA DAİR ÇALIŞMALARI

THE UNITED NATIONS' WORK ON THE PROTECTION OF PERSONAL DATA

Dr. Öğr. Üyesi Songül Atak*

Öz

Birleşmiş Milletler'in doğrudan kişisel verilerin korunması konusunu ele alan ve bu alanda önemli düzenlemeler içeren ilk belgesi 1990 yılında Genel Kurul tarafından kabul edilen "Bilgisayar Ortamında işlenen Kişisel Veri Dosyalarının Düzenlenmesine ilişkin Rehber İlkeler"dir. Ancak, Birleşmiş Milletler bu belgeden sonra çok uzun süre kişisel veriler konusunu doğrudan ele almamıştır. BM'nin konuyu tekrar ele almasında Edward Snowden tarafından 2013 yılında yapılan açıklamaların ve kişisel verilerin korunması alanında çalışan örgütlerin önemli bir rolü olmuştur. BM Genel Kurulu 2013 yılından itibaren belirli aralıklarla güncellenen "Dijital Çağda Mahremiyet Hakkı" başlığını taşıyan kararları kabul etmiştir. Bu kararlarda kişisel verilerin korunması konusu önemli bir yer tutmaktadır. BM Genel Kurulu bu kararlarında özellikle 2018 yılından sonra yapay zekâ teknolojilerinin kullanımının kişisel verilerin korunması açısından yarattığı sorunlar üzerinde yoğunlaşmıştır. Bu çalışmada, öncelikle BM Genel Kurulunun kişisel verilerin ve mahremiyet hakkının korunmasına ilişkin kararları değerlendirilmiştir. Ayrıca BM İnsan Hakları Konseyi, BM İnsan Hakları Komiserliği ve BM Özel Raportörlerinin bu alanda yaptığı çalışmalar incelenmiştir. Bu çalışmanın odak noktasını, Birleşmiş Milletlerin kişisel verilerin korunması alanında yapmış olduğu düzenlemeler oluşturmaktadır. Bu düzenlemelerin hazırlanmasında rol oynayan etkenler incelenmiş ve yapılan düzenlemelerin bu alandaki ihtiyaçlara ne ölçüde cevap verdiği değerlendirilmiştir. Söz konusu düzenlemelerde yer verilen yapa zekâ ve biyometrik teknolojilerin neler olduğu, büyük veri, algoritmik karar verme sistemleri ve belirli tahmin algoritmaları gibi kavramların ne anlama geldiği açıklanmıştır. Ayrıca bu teknolojilerin ve yöntemlerin kullanımının mahremiyet hakkı ve kişisel veriler alanında ne tür ihlallere yol açtığı incelenmiştir. Çalışmanın sonunda, uluslararası alanda kişisel verilerin daha güçlü bir şekilde korunabilmesi için BM'nin atması gereken adımlara ilişkin öneriler ortaya konulmuştur.

Anahtar Kelimeler Birleşmiş Milletler, Kişisel Veri, Mahremiyet Hakkı, Dijital Çağ, Yapay Zekâ

* Dicle Üniversitesi Hukuk Fakültesi Anayasa Hukuku Ana Bilim Dalı.
0000-0002-2573-7602 songulatak@hotmail.com

Bu eser Creative Commons Alıntı-GayriTicari-Türetilemez 4.0 Uluslararası Lisansı ile lisanslanmıştır.
This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

ABSTRACT

The first United Nations document directly addressing the protection of personal data and containing significant regulations in this area was "Guidelines for the Regulation of Computerized Personal Data Files" adopted by the General Assembly in 1990. However, the UN did not directly address the issue of personal data for a long time after this document. Edward Snowden's revelations in 2013 and the efforts of organizations working in the field of personal data protection played a significant role in the UN's reconsideration of the issue. Since 2013, the UN General Assembly has adopted resolutions titled "The Right to Privacy in the Digital Age" updated periodically. The protection of personal data occupies a significant place in these resolutions. In these resolutions, the UN General Assembly has particularly focused on the problems created by the use of artificial intelligence technologies in terms of personal data protection since 2018. In this study, the resolutions of the UN General Assembly regarding the protection of personal data and the right to privacy are primarily evaluated. Furthermore, the work conducted in this field by the UN Human Rights Council, the Office of the UN High Commissioner for Human Rights, and various UN Special Rapporteurs is examined. The study focuses on the regulations established by the United Nations concerning the protection of personal data. It investigates the factors that contributed to the development of these regulations and assesses the extent to which they address the needs in this field. The study clarifies the nature of the artificial intelligence and biometric technologies addressed in these regulations, as well as concepts such as big data, algorithmic decision-making systems, and specific predictive algorithms. Additionally, it explores how the use of these technologies and methods can lead to violations of the right to privacy and the protection of personal data. Finally, the study offers recommendations on the steps the UN should take to ensure more powerful protection of personal data at the international level.

Keywords United Nations, Personal Data, Privacy, Digital Age, Artificial Intelligence.

GİRİŞ

Kişisel veriler bireylerin mahremiyet alanı içinde yer alan ve içerdiği bilgilerin öneminden dolayı güçlü bir şekilde korunması gereken verilerdir. Bu verilerin öneminden dolayı hem ulusal hukuklarda hem de uluslararası hukukta bu alanda özel düzenlemeler yapılması zorunludur. Ancak bu gerekliliğe rağmen, Birleşmiş Milletler örgütü kişisel verilerin korunmasına ilişkin gerekli düzenlemeleri yapma konusunda geç hareket etmiştir.

BM ilk olarak 1988 yılında kişisel verilerin korunması sorunu ile ilgilenmeye başlamış olmakla beraber, bu konuyu doğrudan ele alan ilk kararı 1990 yılında kabul etmiştir. Bu karar Genel Kurul tarafından kabul edilen "Bilgisayar Ortamında işlenen Kişisel Veri Dosyalarının Düzenlenmesine ilişkin Rehber İlkeler"dir. Bu karar ile BM üyesi devletlerin ulusal mevzuatlarında bu alanda kabul edilmesi gerekli olan minimum ilkeler belirlenmiştir.

BM'nin kişisel verilerin korunması alanında asıl çalışmaları 2013 yılından sonra başlamıştır. Edward Snowden tarafından yapılan açıklamaların dünya genelinde yarattığı olağanüstü tepki BM'nin kişisel verilerin korunması alanında adımlar atmasında çok etkili olmuştur. Bu olaydan kısa bir süre sonra BM "Dijital Çağda Mahremiyet Hakkı" başlıklı kararı kabul etmiş ve daha sonra da her iki yılda bir yeni gelişmeler doğrultusunda bu kararı güncellemiştir. Bu kararlarda kişisel verilerin korunması konusu oldukça önemli bir yer tutmaktadır.

Teknolojik gelişmelerin hızlı temposu, dünyanın her yerinde devletlerin ve özel sektörün izleme, dinleme ve veri toplama kapasitesini her geçen gün artırmaktadır. Bu açıdan, BM'nin bu alanda almış olduğu kararlar son derece önemlidir. Söz konusu kararlar, bağlayıcı olmasa dahi, mahremiyet hakkının ve kişisel verilerin korunabilmesi için devletlerin almaları gereken önlemler konusunda önemli bir rol oynamaktadır.

I. KİŞİSEL VERİLERİN KORUNMASI ALANINDA BİRLEŞMİŞ MİLLETLER'İN YAPTIĞI İLK DÜZENLEMELER

Birleşmiş Milletler örgütü kurulduğu tarihten itibaren başta İnsan Hakları Evrensel Bildirgesi olmak üzere çok sayıda insan hakları belgesi kabul etmiştir. BM tarafından kabul edilen genel insan hakları belgeleri içinde kişisel verilerin korunması konusunda açık bir düzenleme yer almamakla beraber, bu belgelerin bazılarında mahremiyet hakkını güvence altına alan düzenlemeler yer almaktadır. Söz konusu belgelerin ilki İnsan Hakları Evrensel Bildirgesidir.[1] Bildirge uluslararası alanda mahremiyet hakkını düzenleyen ilk önemli belgedir. Bu konu Bildirgenin 12. maddesinde düzenlenmiştir.

Mahremiyet hakkına ilişkin düzenleme daha sonraları kabul edilen bazı insan hakları belgelerinde de yer almıştır. Bu hak, Çocuk Hakları Sözleşmesinin[2] 16. maddesinde, Tüm Göçmen İşçilerin ve Aile Bireylerinin Haklarının Korunmasına İlişkin Uluslararası

[1] BM, "İnsan Hakları Evrensel Bildirgesi", https://digitallibrary.un.org/record/666853?v=pdf (erişim: 03.04.2026)
[2] BM, "Çocuk Hakları Sözleşmesi", http://www.un-documents.net/a44r25.htm (erişim: 03.04.2026)

Sözleşmenin[3] 14. maddesinde ve Engelli Haklarına İlişkin Sözleşmenin[4] 22. maddesinde düzenlenmiştir. BM'nin mahremiyet hakkı alanında en kapsamlı düzenlemeyi içeren belgesi Medeni ve Siyasal Haklara İlişkin Sözleşmedir.[5] Bu konu Sözleşmenin 17. maddesinde düzenlenmiştir:

Bu belgelerde mahremiyet hakkı açısından güvence sağlayan maddelerin kişisel verileri de kapsadığı kabul edilmektedir. Çarpıcı teknolojik gelişmelerin ve dijital uygulamaların kişisel veriler açısından doğurduğu sonuçlar, bireylerin yaygın bir şekilde izlenebilmelerine ve denetlenebilmelerine olanak tanıyan yeni yöntemlerin ortaya çıkışı bu verilerin etkili bir şekilde korunmasının önemini her geçen gün artırmış ve ayrı düzenlemeler yapılmasını zorunlu kılmıştır. Ancak, bu gerçeğe karşın kişisel verilerin korunması konusu uzun yıllar BM insan hakları koruma ve izleme mekanizmaları tarafından ele alınmamıştır. Kişisel verilerin korunması alanında ilk önemli uluslararası düzenleme Avrupa Konseyi tarafından yapılmıştır. Avrupa Konseyi 1981 yılında "Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme"yi[6] kabul etmiştir. 1985 yılında yürürlüğe giren Sözleşme kişisel verilerin korunması konusunda uluslararası alanda kabul edilen ilk bağlayıcı metindir.

BM ilk olarak 1988 yılında kişisel verilerin korunması konusunu ele almıştır. BM Medeni ve Siyasal Haklara İlişkin Sözleşmesinin Sözleşmeye taraf olan devletlerde uygulanmasını izlemek amacıyla kurulmuş olan İnsan Hakları Komitesi, Sözleşmenin 17. maddesi hakkında yayınlamış olduğu 16 sayılı Genel Yorumun[7] 10. paragrafında kişisel veriler konusunu ele almıştır. Komite kişisel verilerin korunabilmesi için üye devletlere şu tavsiyelerde bulunmuştur: İster kamusal makamlar isterse özel şahıslar ya da organlar tarafından, kişisel verilerin bilgisayarlarda, veri bankalarında ve diğer araçlarda toplanması ve tutulması konusunda yasal düzenleme yapılmalıdır. Hangi kişisel verilerinin ve hangi amaçla otomatik veri dosyalarında saklandığı hakkında bireylere bilgi edinme hakkı tanınmalıdır. Şayet bu dosyalar doğru olmayan veriler içeriyorlarsa ya da yasanın hükümlerine aykırı bir şekilde işleniyorsa, ilgili bireylere bu verilerin düzeltilmesini ya da silinmesini isteme hakkı tanınmalıdır.

İnsan Hakları Komitesi tarafından yayınlamış olan 16 sayılı Genel Yorum hem kişisel verilerin korunması konusunu ilk kez ele almış olması ve hem de yalnız kamusal makamlardan gelecek müdahalelere karşı değil aynı zamanda özel şahıslar ya da organlar tarafından gerçekleştirilecek müdahalelere karşı da kişisel verilerin korunması gerektiğini belirtmesi açısından

[3] BM, "Tüm Göçmen İşçilerin ve Aile Bireylerinin Haklarının Korunmasına İlişkin Uluslararası Sözleşme", http://www.un-documents.net/a45r158.htm (erişim: 03.04.2026)

[4] BM, "Engelli Haklarına İlişkin Sözleşme", https://treaties.un.org/doc/source/docs/a_res_61_106-e.pdf (erişim: 03.04.2026)

[5] BM, "Medeni ve Siyasal Haklara İlişkin Sözleşme", http://www.un-documents.net/a21r2200.htm (erişim: 05.04.2026)

[6] Convention for the Protection of Individual with Regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, European Treaty Series-No.108, https://rm.coe.int/1680078b37 (erişim: 05.04.2026)

[7] CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988, https://www.refworld.org/legal/general/hrc/1988/27539 (erişim: 07.04.2026)

önemli bir belgedir, ancak doğrudan doğruya kişisel veriler için hazırlanmış ayrıntılı bir metin değildir. Ayrıca bağlayıcı nitelikte olan bir belge değildir.

16. Genel Yorum hazırlandığı dönem açısından önemli bir ilerlemeyi ifade etmektedir ancak mahremiyet hakkının ihlalinin dijital bağlamını ayrıntılı olarak ele almadığı için günümüzde güncelliğini yitirmiştir.[8]

BM'nin yalnızca kişisel veriler konusunu ele aldığı ilk metin 1990 yılında Genel Kurul tarafından kabul edilen "Bilgisayar Ortamında işlenen Kişisel Veri Dosyalarının Düzenlenmesine ilişkin Rehber İlkeler"dir.[9] Söz konusu belgede, üye devletlerin ulusal mevzuatlarında uymaları gereken ve bu alanda asgari güvenceleri sağlayan ilkeler ortaya konulmuştur. Bu konuda 10 temel ilke kabul edilmiştir. Ancak, bu ilkelerin uygulanmasındaki usullerin belirlenmesi konusunda inisiyatif taraf devletlere bırakılmıştır.

Birinci ilke, hukuka ve dürüstlük kuralına uygunluk ilkesidir. Bu ilkeye göre, kişisel veriler hukuka ve dürüstlük kuralına aykırı bir şekilde toplanmamalı ve işlenmemelidir.

İkinci ilke, doğruluk ilkesidir. Bu ilkeye göre, dosyaların hazırlanmasından ve saklanmasından sorumlu olan kişiler, saklanan verilerin güncelliğini ve doğruluğunu düzenli olarak kontrol etmeli ve bu veriler işlenilmeye ve kullanılmaya devam edildiği sürece, mümkün olduğunca eksiksiz korunmalarını ve güncellenmelerini sağlamalıdır.

Üçüncü ilke, amacın belirlenmesi ilkesidir. Bu ilkeye göre, kişisel verilerin hangi amaçla toplandığı ve kullanılacağı belirtilmeli ve ilgili kişilere bu konuda bilgi verilmelidir. Kişisel verilerin saklanma süresi, belirtilen amaçların gerçekleştirilmesini sağlayacak süreyi aşmamalıdır.

Dördüncü ilke, ilgili kişilerin kendi verilerine erişebilmesi ilkesidir. Bu ilkeye göre, ilgili kişiler kimliklerini kanıtlamak şartıyla, verilerinin işlenip işlenmediğini bilme, bu verilere ulaşma ve uygun düzeltmelerin yapılmasını isteme hakkına sahiptir.

Beşinci ilke, ayrımcılık yasağı ilkesidir. Bu ilkeye göre, altıncı ilkede belirtilen istisnai durumlar dışında ırksal veya etnik köken, renk, cinsel yaşam, siyasi görüşler, dini, felsefi ve diğer inançlar ile bir dernek veya sendika üyeliği gibi yasa dışı veya keyfi ayrımcılığa yol açması olası olan veriler toplanmamalıdır.

Altıncı ilke, istisnalar koyma yetkisine ilişkindir. Bu ilkeye göre, ilk dört ilkede belirlenen güvencelere ancak ulusal güvenlik, kamu düzeni, kamu sağlığı ya da kamu ahlakını korumak ve diğer kişilerin, özellikle de zulüm gören kişilerin hak ve özgürlüklerini korumak için gerekli olması şartıyla, istisnalar getirilebilir. Ancak, bu istisnalar yasal bir düzenleme ile açıkça belirtilmiş olmalıdır.

[8] Daniel Joyce, "Privacy in the Digital Era: Human Rights Online?", Melbourne Journal of International Law, Cilt: 16, Sayı:1, 2015, https://law.unimelb.edu.au/__data/assets/pdf_file/0003/1586811/16109Joyce2.pdf (erişim: 10.04.2026)s.8.

[9] A/RES/45/95 (1990), Guidelines for the Regulation of Computerized Personnel Data Files Adopted by the General Assembly Resolution 45/95 of 14 December 1990. https://digitallibrary.un.org/record/105299?v=pdf (erişim: 10.04.2026)

Yedinci ilke, güvenlik ilkesidir. Bu ilkeye göre, veri dosyalarının hem doğal tehlikelere (kazara kaybedilmesi veya tahrip olması gibi) hem de insan kaynaklı tehlikelere (yetkisiz erişim, verilerin yasa dışı kullanımı veya bilgisayar virüslerinin bulaşması gibi) karşı korunması için uygun önlemler alınmalıdır.

Sekizinci ilke, denetim ve yaptırımlar konusunu düzenlemektedir. Bu ilkeye göre, bu düzenlemede belirtilen ilkelerin uygulanmasını denetlemek üzere her ülkenin iç hukuk sistemine uygun olarak bir yetkili makam belirlenmelidir.

Dokuzuncu ilke, sınır ötesi veri transferine ilişkindir. Bu ilkeye göre, sınır ötesi veri transferinin yapılabilmesi için ilgili iki ya da daha fazla devletin yasalarının mahremiyet hakkının korunması konusunda eşdeğer güvenceler sağlıyor olması gerekir.

Onuncu ilke, bu belgede yer alan ilkelerin uygulama alanını düzenlemektedir. Buna göre, bu ilkeler öncelikle bilgisayar ortamına aktarılmış tüm kamusal ve özel dosyalara ve ayrıca gerekli düzenlemelerin sağlanması koşuluyla kapsamı genişletilerek manuel dosyalara da uygulanmalıdır.

Bu düzenleme ile BM üyesi devletlerin ulusal mevzuatlarında bu alanda kabul edilmesi gerekli olan temel ilkeler belirlenmiştir. Bunlar arasında, belirtilen ilkelerin yerine getirilip getirilmediğini denetlemek amacıyla üye devletlerce bağımsız ve tarafsız bir otoritenin kurulmasını zorunlu kılan düzenleme özellikle önemlidir. Ancak bu metin bağlayıcı bir metin değildir. Bağlayıcı olmamasından dolayı, sınırlı bir pratik öneme sahip olduğu gerekçesiyle çok fazla eleştiri almıştır.[10] Metnin tavsiye niteliğinde olması nedeniyle üye devletlerde böyle bir organın kurulması ve etkili bir şekilde çalışması üye devletlerin inisiyatifine kalmıştır.

II. 1991-2013 YILLARI ARASINDA YAPILAN DÜZENLEMELER

Kişisel verilerin korunması konusunda BM'nin üçüncü çalışması ancak 2009 yılında gerçekleşmiştir. Terörizmle mücadele sürecinde insan hakları ve temel özgürlüklerin korunması ve geliştirilmesi konusunu ele almak üzere atanmış olan BM Özel Raportörü 2010 yılında hazırlamış olduğu raporda[11] kişisel verilerin korunması konusu da ele almıştır.

Söz konusu raporda genel olarak kişisel veriler üzerinde değil özellikle biyometrik verilerin ve DNA verilerinin korunması konusu üzerinde durulmuştur. Tüm kimlik ve erişim yönetimi işlemlerinin tek bir ortamda toplandığı merkezi kimlik sisteminde, biyometrik verilerin ve DNA verilerinin kullanımının tehlikelerine dikkat çekilmiştir.

Özel Raportör bu konudaki endişelerini raporun 24. paragrafında açıklamıştır: Yeni kimlik politikalarının temel bileşenlerinden biri, yüz tanıma, parmak izi ve iris tanıma gibi

[10] Paul De Hert ve Evangelos Papakonstantinou, "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?", I/S: A Journal of Law and Policy for Information Society, Cilt: 9, Sayı: 2, (2013) https://cris.vub.be/ws/portalfiles/portal/17831773/pdh13_vpISjournalthreescenariosUNagency.pdf (erişim:15.04.2026) s.282.

[11] A/HRC/13/37 (2009) Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, https://docs.un.org/en/A/HRC/13/37 (erişim: 15.04.2026)

biyometrik yöntemlerin kullanılmasıdır. Bu yöntemler, bazı durumlarda şüpheli teröristlerin kimlik tespiti için meşru bir araç olabilse de özellikle biyometrik verilerin kimlik belgesinde değil, merkezi bir veri tabanında saklandığı, böylece verilerin güvenliği açısından risklerin arttığı ve bireylerin savunmasız kaldığı durumlar endişeye neden olmaktadır. Biyometrik verilerin toplanması arttıkça, hata oranları önemli ölçüde artabilir. Bu durum, bireylerin haksız yere suçlu ilan edilmesine veya toplumsal dışlanmaya yol açabilir. Diğer bir sorun da DNA verilerinin tahrif edilebilmesidir.

Özel Raportörün konuya ilişkin ortaya koyduğu endişeler haklı bir temele dayanmaktadır. Örneğin, e-pasaport uygulamasında, e-pasaport sisteminde yer alan verilerin ulusal kimlik kartlarına aktarılması, kimlik hırsızlığına karşı son derece savunmasız bir kimlik doğrulama altyapısı oluşturabilmektedir.[12] DNA verilerinin tahrif edilebileceğine ilişkin kaygılar da son derece önemlidir. Yapılan bilimsel araştırmalar, özellikle ceza davalarında kullanılabilecek adli delillerin altın standardı olarak kabul edilen DNA verilerinin tahrif edilebileceğini ortaya koymuştur.[13] Bilim insanları, kan ve tükürük örneklerini, kan ve tükürük bağışçısından farklı bir kişiye ait DNA içerecek şekilde üretmişlerdir. Ayrıca, bir veri tabanındaki DNA profiline erişimleri varsa, o kişiden herhangi bir doku almadan o profille eşleşen bir DNA örneği oluşturabileceklerini de kanıtlamışlardır.[14]

Özel Raportör bu risklerin önüne geçilebilmesi için devletlere verilerin işlenmesine, saklanmasına ve paylaşılmasına sınırlar getiren; bireylere net yasal korumalar sağlayan; bireylerin verilerinin nasıl kullanıldığı konusunda bilgilendirilmelerini sağlayan, erişim ve tazminat hakkına sahip olmalarını zorunlu kılan kapsamlı bir veri koruma yasası kabul etmeleri tavsiyesinde bulunmuştur.[15]

2009 yılında gerçekleşen bu çalışmanın dışında, 1990 ile 2013 yılları arasında BM Genel Kurulu ya da BM insan hakları organları tarafından kişisel verilerin korunması konusunda herhangi bir karar ya da rapor kabul edilmemiştir.

III. 2013 YILINDAN İTİBAREN YAPILAN DÜZENLEMELER

BM'nin kişisel veriler konusunu ayrıntılı bir şekilde ele alması ancak 2013 yılından sonra olmuştur. 2013 yılında Edward Snowden tarafından yapılan açıklamaların[16] dünya

[12] Eleni Kosta vd.,"An Analysis of Security and Privacy Issues Relating to RFID Enabled ePassports", New Approaches for Security, Privacy and Trust in Complex Environments. (haz. Hein Venter, Mariki Eloff, Les Labuschagne, Jan Eloff, Rossouw Solms,) International Federation for Information Processing, Cilt 232. (2007) Springer, Boston, MA. https://link.springer.com/chapter/10.1007/978-0-387-72367-9_42#preview (erişim: 15.04.2026) s.469.

[13] Joseph L. Peterson ve Anna S. Leggett, "The Evolution of Forensic Science: Progress Amid the Pitfalls", Stetson Law Review, Cilt:36, (2007), https://stetsonlawreview.org/wp-content/uploads/2022/02/36.3.02.Peterson.pdf (erişim: 17.04.2026) s.654.

[14] Dan Frumkin vd., "Authentication of forensic DNA samples", Forensic Science International: Genetics, Cilt: 4, Sayı: 2 (2010) http://www.sakkyndig.com/psykologi/artvit/frumkin2010.pdf (erişim: 20.04.2026)s.98 (ss.95–103) ; Andrew Pollack, "DNA Evidence Can Be Fabricated, Scientists Show", the New York Times, 17.08.2009 https://www.nytimes.com/2009/08/18/science/18dna.html (erişim:20.04.2026)

[15] A/HRC/13/37, para. 61.

[16] Edward Snowden tarafından yapılan açıklamaların ayrıntısı için bkz. Ewen Macaskill ve Gabriel Dance, 'NSA Files: Decoded', The Guardian, 01.11.2023 https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (erişim: 25.04.2026)

genelinde yaratmış olduğu etki BM'nin yaklaşımını değiştirmesine ve kişisel verilerin korunması konusuna daha fazla önem vermesine neden olmuştur.

ABD Ulusal Güvenlik Ajansında (NSA) ve Merkezi İstihbarat Teşkilatında (CIA) teknik istihbarat analisti ve bilgisayar sistem yöneticisi olarak çalışan Edward Snowden ABD Ulusal Güvenlik Ajansının binlerce gizli belgesini 2013 yılında basına açıklamıştır. Bu belgeler gizli izleme programlarına ilişkin belgelerdir.

Açıklanan belgeler, ABD Ulusal güvenlik Ajansı ve İngiltere Hükümet İletişim Merkezi (GCHQ) gibi istihbarat teşkilatlarının, ABD'nin küresel telekomünikasyon şirketlerinin sunucularından büyük miktarda veri topladığını ortaya koymaktaydı. Ele geçirilen ve saklanan bu veriler arasında iletişim içeriği (e-postalar, anlık mesajlar ve tam web tarama geçmişleri gibi) ve iletişimle ilgili meta veri bilgileri (örneğin, iletişimin kimden kime gönderildiği; nereden nereye gönderildiği; ziyaret edilen web alan adlarının kaydı; ve cep telefonu konum verileri) yer almaktaydı.[17]

Edward Snowden'ın ABD ve müttefiklerinin kitlesel izleme uygulamalarını ortaya koyan açıklamalarının sonuçları çok önemli olmuştur. Söz konusu açıklamalar büyük miktardaki verinin nasıl yasadışı bir şekilde ele geçirildiğini ortaya koymuştur.

Son yıllarda, hızlı ve sürekli devam eden teknolojik gelişmeler neredeyse sınırsız miktarda veri üretilmesine neden olmuştur. Büyük veri olarak adlandırılan bu veri birikimi her geçen gün gelişmeye ve genişlemeye devam etmektedir.[18] Büyük veri, geleneksel veri tabanı ve yazılım teknikleriyle işlenmesi zor olacak kadar büyük miktarda yapılandırılmış ve yapılandırılmamış veriyi ifade etmektedir. Bu veriler çok farklı kanallardan elde edilmektedir; sosyal medya sitelerine yapılan gönderiler, çevrimiçi olarak yayınlanan dijital resimler ve videolar, çevrimiçi satın alımların işlem kayıtları ve cep telefonu GPS sinyalleri bunlardan sadece birkaçıdır.[19]

Büyük veri analitik teknikleri veya araçları kullanılarak, bireyin kimliğini ortaya çıkarabilecek ve her türlü amaç için kullanılabilecek veriler elde edilir.[20] Büyük veri sistemleri aracılığıyla toplanan muazzam miktardaki kişisel veri, mahremiyet hakkı açısından önemli sorunlara yol açmaktadır. Çoğunlukla veriler farklı yasal düzenlemelere sahip ülkeler arasında aktarılmaktadır. Bu durumda bireyler verilerinin nasıl kullanıldığı veya yeterli korumanın

[17] Vian Bakir, Martina Feilzer ve Andrew McStay, "Introduction to Special Theme Veillance and Transparency: A Critical Examination of Mutual Watching in the Post-Snowden, Big Data Era", Big Data & Society Cilt:4, Sayı:1 (2017) https://journals.sagepub.com/doi/10.1177/2053951717698996 (erişim:26.04.2026) s.2.

[18] Hossein Hassani vd., "Big Data and the United Nations Sustainable Development Goals (UN SDGs) at a Glance", Big Data and Cognitive Computing. Cilt: 5, Sayı: 3 (2021) https://www.mdpi.com/2504-2289/5/3/28 (erişim: 16 Mayıs 2026)s.2.

[19] United Nations Global Pulse "Big Data for Develeopment: Challenges and Opportunities", (2012) New York, https://unstats.un.org/unsd/trade/events/2014/beijing/documents/globalpulse/Big%20Data%20for%20Development%20-%20UN%20Global%20Pulse%20-%20June2012.pdf (erişim: 20.05.2026) s.13.

[20] Qing Tan ve Frederique Pivot, "Big Data Privacy: Changing Perception of Privacy", 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (Smart City) 2015, https://ieeexplore.ieee.org/document/7463831 (erişim: 20.05.2026) s.861.

mevcut olup olmadığı konusunda genellikle çok az bilgiye sahip olmaktadır. Bu durum kişisel verilerin korunmasını çok zorlaştırmaktadır.[21]

Edward Snowden'ın açıklamaları kişisel veriler açısından mevcut olan bu risklerin daha görünür hale gelmesini sağlamış ve BM'de dijital çağda mahremiyet hakkı üzerine bir tartışmanın başlamasına neden olmuştur. Bu tartışma, esas olarak BM Genel Kurulu ve İnsan Hakları Konseyi tarafından bir dizi kararın kabul edilmesine ve İnsan Hakları Yüksek Komiserliği ve BM Özel Raportörleri tarafından bir dizi tematik rapor hazırlanmasına neden olmuştur.[22]

A. BM Genel Kurulunun 68/167 Sayılı Kararı

Edward Snowden'ın açıklamalarının yarattığı tartışmaların da etkisiyle Birleşmiş Milletler Genel Kurulu BM tarafından kişisel verilerin korunması konusunda kabul edilen ilk önemli kararı 2013 yılında kabul etmiştir. Bu karar "Dijital Çağda Mahremiyet Hakkı" başlığını taşıyan 68/167 sayılı karardır.[23]

Karar, çevrimdışı alanda korunan mahremiyet hakkının çevrimiçi ortamda da korunması gerektiğini teyit eden dönüm noktası niteliğinde bir karardır. Bireylerin gerçek (fiziksel hayatta) hayatta sahip oldukları, başta mahremiyet hakkı olmak üzere tüm temel hak ve özgürlüklerinin, dijital dünyada ve internet ortamında da aynı şekilde korunması gerektiği üzerinde önemle durmuştur.

Genel Kurul, hızla gelişen teknolojilerin mahremiyet hakkı üzerinde yarattığı olumsuz sonuçlara çözüm bulmak için bu kararı daha sonraki yıllarda belirli aralıklarla güncelleyerek ve teknolojik gelişmelere bağlı olarak zaman içinde bu alanda öne çıkan yeni sorunları ve çözüm yollarını ekleyerek genişletmiştir. Genel Kurul dijital çağda mahremiyet hakkı başlıklı bu kararlarıyla, dijitalleşme sürecinde bireylerin mahremiyet hakkının korunmasını hedeflenmektedir. Bu kararlarda kişisel verilerin korunması konusu da oldukça önemli bir yer tutmaktadır.

Bu kararlar mahremiyet hakkının ve kişisel verilerin korunması konusunda uluslararası alanda ortak düzenlemelerin yapılmasını hedefleyen kararlardır. Söz konusu kararlarda devletler ve özel sektör tarafından bireylerin izlenmesi ve kişisel verilerinin yasa dışı bir şekilde toplanması ve yapay zekâ ile biyometrik teknolojilerin kullanımının yarattığı olumsuz sonuçlar ayrıntılı ele alınmıştır. Bu kararlar, teknoloji hızla gelişmeye devam ederken devletlerin ve özel sektörün mahremiyet hakkı ve kişisel verilerin korunması konusuna gerekli özeni göstermelerini sağlamak için rehber görevi gören kararlardır.

68/167 sayılı karar, uluslararası düzeyde mahremiyet hakkının korunması alanında önemli bir gelişmeyi temsil etmektedir. Kararın odak noktası dijital çağda mahremiyet hakkının güvence altına alınmasıdır, ancak karar aynı zamanda Edward Snowden tarafından yapılan

[21] Lanxin Li vd., "Big Data and Data Science in Global Governance: Anticipating Future Needs and Applications in the UN and Beyond", Frontiers in Political Science, 18 Ağustos 2025, https://researchonline.lse.ac.uk/id/eprint/129350/1/fpos-07-1583772.pdf (erişim: 26.05.2026) s.14.

[22] Kinfe Micheal Yilma, "The United Nations' Evolving Privacy Discourse and Corporate Human Rights Obligations", American Society of International Law, Cilt: 23, Sayı:: 4, (2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4215111 (erişim:27.05.2026) s.1.

[23] A/RES/68/167, (2013) The right to privacy in the digital age Resolution adopted by the General Assembly on 18 December 2013, https://docs.un.org/en/a/res/68/167 (erişim:30.05.2026)

ifşaatların ardından uluslararası toplumdan gelen ağır ve doğrudan bir kınama olarak da görülebilir.[24]

Söz konusu kararda kişisel verilerin korunması konusunda şu hususlara vurgu yapılmıştır; teknolojilerin hızlı gelişimi, tüm dünyada devletlerin, şirketlerin ve bireylerin izleme, dinleme ve veri toplama kapasitesini artırmaktadır. Bu durum, mahremiyet hakkı başta olmak üzere insan haklarını ihlal edebileceği için ciddi bir endişeye neden olmaktadır. Yasadışı veya keyfi şekilde kişisel verilerin toplanması demokratik toplum ilkelerine aykırılık oluşturmaktadır.

Kararda kişisel verilerin korunması konusunda devletlere şu çağrıda bulunulmuştur: Dijital iletişim alanındaki ihlalleri önlemek için gerekli tüm önlemler alınmalıdır. Devletler iletişimin izlenmesi, dinlenilmesi ve kişisel verilerin toplanmasıyla ilgili uygulamalarını ve mevzuatlarını gözden geçirmeli, ulusal mevzuatın uluslararası insan hakları hukuku alanındaki yükümlülüklere uygun olmasını sağlamalıdır. Bu konuda şeffaflığı ve denetimi sağlayabilecek bağımsız ve etkili ulusal denetim mekanizmaları kurmalı veya bu özelliğe uygun olan mevcut mekanizmaları korumalıdır.[25]

Kararda, BM İnsan Hakları Yüksek Komiserliğinden ülke içi ve sınır ötesi izleme ve/veya dijital iletişimlerin ele geçirilmesi ve kişisel verilerin, kitlesel ölçek de dahil olmak üzere, toplanması konusunda mahremiyet hakkının korunması ve geliştirilmesine ilişkin hazırlayacağı bir raporu, görüş ve tavsiyeleri ile birlikte, İnsan Hakları Konseyine ve Genel Kurula sunması istenmiştir.[26]

Genel Kurulun talebi doğrultusunda BM İnsan Hakları Yüksek Komiserliği bir rapor hazırlamıştır[27]. Raporda en çok dikkat çeken hususlardan biri, dijital izleme alanında özel sektörün gittikçe artan ve tehlikeli boyutlara varan rolüne özellikle vurgu yapılmış olmasıdır. Rapora göre, devletler dijital izlemeyi yürütmek ve kolaylaştırmak için özel sektöre giderek daha fazla yetki vermektedirler. Her kıtada, devletler kişisel verilere erişim sağlamak için hem resmi yasal mekanizmaları hem de gizli yöntemleri kullanmaktadırlar.[28]

Gerçekten de özellikle ABD ve İngiltere tarafından 'küresel internet trafiğinin' izlendiğine ilişkin Edward Snowden tarafından yapılan açıklamalar, devletler arasında stratejik istihbarat ilişkilerini, özel şirketlerin düzenleyici kontrolünü ve ticari sözleşmeleri içeren ulusötesi bir ağı ortaya koymaktadır. Raporda ortaya konulan saptamalar, hem kamu hem de özel sektörün mahremiyet hakkına yönelik ihlallerini ve karşılıklı suç ortaklıklarını net bir şekilde gözler önüne sermektedir.[29]

Rapor, mahremiyet hakkı ve kişisel verilerin korunması konusunda güçlü bir yaklaşım ortaya koymuştur. Birçok devlette mevcut kurumsal ve yasal düzenlemelerin yetersiz olduğunu

[24] Joyce, "Privacy in the Digital Era: Human Rights Online?", s.2.
[25] A/RES/68/167, para.4.
[26] A/RES/68/167, para.5.
[27] A/HRC/27/37, The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014, https://docs.un.org/en/a/HRC/27/37 (erişim: 30.05.2026)
[28] A/HRC/27/37, para.42.
[29] Joyce, "Privacy in the Digital Era: Human Rights Online?", s.6.

saptamış ve daha fazla çalışmanın ve yeni düzenlemelerin yapılmasının zorunlu olduğunu belirtmiştir[30].

BM İnsan Hakları Yüksek Komiserliği tarafından hazırlanan rapor sonrasında çok sayıda sivil toplum örgütü BM Genel Kuruluna ortak bir çağrı yapmıştır[31]. Çağrı şöyledir; "BM Genel Kurulu, İnsan Hakları Yüksek Komiserliği tarafından hazırlanan rapordaki saptamaları dikkate alarak yeni bir karar almalıdır. Yeni alınacak kararda, özellikle şu ilkeler güçlü bir şekilde tekrarlanmalıdır: İzleme, yalnızca kamuya açık, net, kapsamlı ve ayrımcı olmayan bir yasal çerçeve temelinde yapılmalıdır; izleme sonucunda mahremiyet hakkı ihlal edilen bireyler, ayrımcılığa uğramadan etkili bir çözüm yoluna erişebilmelidir. Birleşmiş Milletlerin bu alanda atabileceği en önemli adım da bu konuyu ele alacak bir özel raportörün atanmasıdır."

B. BM Genel Kurulunun 69/166 Sayılı Kararı

İnsan Hakları Yüksek Komiserliği tarafından hazırlanan 27/37 sayılı rapor ve sivil toplum örgütlerinden yapılan çağrı doğrultusunda BM Genel Kurulu 2014 yılında "Dijital Çağda Mahremiyet Hakkı" başlıklı yeni bir karar kabul etmiştir[32]. 69/166 sayılı karar olarak bilinen bu karar esas itibariyle daha önceki 68/167 sayılı kararı temel almakta ve büyük ölçüde önceki kararı tekrarlamaktadır.

Yeni alınan kararın en önemli özelliliği BM'nin dijital verilerin korunması konusuna artan bir şekilde önem verdiğini ve gündeminde tutmaya devam edeceğini göstermesidir. Bu kararda kitlesel izleme uygulamaları ve yabancı ülkelerdeki iletişimin izlenmesinin insan hakları üzerindeki olumsuz etkilerine özellikle dikkat çekilmiştir. Söz konusu kararın diğer bir önemi de hakları ihlal edilen bireylere hukuki çözüm yollarının sağlanmasını üye devletlerden istemesidir. Ayrıca, Yüksek Komiserliğinin raporunda dijital izleme alanında özel sektörün gittikçe artan ve tehlikeli boyutlara varan rolüne özellikle dikkat çekilmiş olması nedeniyle, 69/166 sayılı kararda da özel sektörün rolü ve sorumlulukları üzerinde durulmuştur.

Karara göre devletler, bireylerin kişisel verilerini topladıklarında ve özel sektör de dahil olmak üzere, üçüncü taraflardan kişisel verilerin açıklanmasını talep ettiklerinde mahremiyet hakkına ilişkin uluslararası insan hakları yükümlülüklerine saygı göstermelidirler. Aynı şekilde, özel sektörün de insan haklarına saygı gösterme yükümlülüğü vardır.

Kişisel verilerin ve mahremiyet hakkının korunması konusunda özel sektörün yükümlülükleri üzerinde durulması önemli bir yeniliktir. Mevcut uluslararası insan hakları hukukunda özel sektörün doğrudan bir yükümlülüğü bulunmamaktadır. BM'nin kararında

[30] Marko Milanovic, "OHCHR Publishes Report on Surveillance and Privacy in the Digital Age,", Blog of the European Journal of International Law, https://www.ejiltalk.org/ohchr-publishes-report-on-surveillance-and-privacy-in-the-digital-age/ (erişim: 02.06.2026)

[31] Call to support a strong UNGA resolution on the right to privacy in the digital age, Press Statement, 04.11.2014, https://www.apc.org/sites/default/files/UNGA_PrivacyResolution_0.pdf (erişim: 30.05.2026)

[32] A/RES/69/166 (2014) The right to privacy in the digital age, Resolution adopted by the General Assembly on 18 December 2014, [on the report of the Third Committee A/69/488/Add.2 and Corr.1)] https://docs.un.org/en/A/RES/69/166 (erişim: 01.06.2026)

mahremiyet hakkı kapsamında özel sektörün rolü ele alınarak, özel işletmeler de bu alanda yükümlülük altına konulmuş olmaktadır[33].

69/166 sayılı karar Yüksek Komiserlik tarafından hazırlanan raporda yer alan tespitleri dikkate alarak çözüm yollarına odaklanmaktadır. Ancak bu karar dijital izlemeye karşı alınacak önlemler konusunda yeterli bulunmayarak eleştirilmiştir. Genel Kurulun kararında önerdiği şey, önceden var olan bir çerçevenin güncellenmesi ve yeniden konumlandırılması çağrısına benzetilmiştir.[34] Dijital alanda insan haklarının korunabilmesi için BM tarafından atılması gereken önemli adımlar olduğu üzerinde durulmuş ve bu alanda atılacak ilk pratik adımın, bu sorunu ele alacak bir özel raportörün atanması olduğu belirtilmiştir.[35] Özellikle Privacy International isimli sivil toplum örgütü, BM tarafından bu alanda çalışacak bir özel raportörün atanması konusunda bir kampanya başlatmış ve bu kampanya çok sayıda sivil toplum örgütü tarafından desteklenmiştir.[36]

C. Özel Raportör Atanmasına İlişkin 28/16 Sayılı Karar

Sivil toplum örgütlerinin yürüttüğü kampanyanın etkisiyle 2015 yılında BM İnsan Hakları Konseyi 28/16 sayılı kararıyla "Dijital Çağda Mahremiyet Hakkı" konusunu ele almak üzere üç yıl süreyle görev yapacak bir özel raportör atanmasına karar vermiştir.[37]

Özel Raportörün görev süresi 28/16 sayılı kararda belirtilen şartlarla aynı olmak üzere 2018[38], 2021[39] ve 2024[40] yıllarında alınan kararlarla her defasında üçer yıl süreyle uzatılmıştır. Bu kararlarda Özel Raportörden; ulusal ve uluslararası alanda mahremiyet hakkı ve kişisel verilerin korunması alanındaki gelişmeleri ve sorunları incelemesi ve mahremiyet hakkının ve kişisel verilerin korunmasını sağlamak için İnsan Hakları Konseyine öneri ve tavsiyelerde bulunması istenmiş ve ayrıca İnsan Hakları Konseyine ve Genel Kurula yıllık rapor sunma görevi verilmiştir.

Özel Raportör ilk raporunu 2016 yılında hazırlamıştır.[41] Bu raporda, dijital çağda mahremiyet hakkının korunması için kritik öneme sahip çalışma alanları tespit edilmiştir. Bu alanlar şunlardır: Kurumsal çevrimiçi iş modelleri ve kişisel verilerin kullanımı. Güvenlik, izleme,

[33] Yilma "The United Nations' Evolving Privacy Discourse and Corporate Human Rights Obligations", s.1.
[34] Joyce, "Privacy in the Digital Era: Human Rights Online?", s.12-13.
[35] Eileen Donahoe, "Human Rights in the Digital Age", Just Securiy, 23.12.2014, https://www.justsecurity.org/18651/human-rights-digital-age/ (erişim: 04.05.2026)
[36] Recognition of Privacy in UN Human Rights Mechanisms, Privacy International, 02-05.2018, https://privacyinternational.org/privacy-un-human-rights-mechanisms (erişim: 04.05.2026)
[37] A/HRC/RES/28/16 (2015) The right to privacy in the digital age, Resolution adopted by the Human Rights Council, https://docs.un.org/en/a/hrc/res/28/16 (erişim: 05.06.206)
[38] A/HRC/RES/37/2 (2018) The right to privacy in the digital age, Resolution adopted by the Human Rights Council on 22 March 2018, https://digitallibrary.un.org/record/1484920?v=pdf (erişim: 06.06.2026)
[39] A/HRC/RES/46/16 (2021) The right to privacy in the digital age, Resolution adopted by the Human Rights Council on 23 March 2021, https://docs.un.org/A/HRC/RES/46/16 (erişim: 06.06.2026)
[40] A/HRC/RES/55/3 (2024) The right to privacy in the digital age, Resolution adopted by the Human Rights Council on 3 April 2024, https://docs.un.org/en/A/HRC/RES/55/3 (erişim: 06.06.2026)
[41] A/HRC/31/64, Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/31/64 (erişim: 08.06.2026)

orantılılık ve siber barış. Açık veri ve büyük veri analitiğinin mahremiyet hakkı üzerindeki etkisi. Genetik veriler ve mahremiyet hakkı. Biyometrik veriler ve mahremiyet hakkı.

Özel Raportörün ilk raporunda belirlemiş olduğu çalışma alanlarının sayısı ve kapsamı oldukça geniştir. Özel Raportör bu seçimi ile aslında güvenlik ve izlemenin mahremiyet hakkı için doğuracağı risklere öncelik vermeye devam etmek ile büyük veri ve yeni teknolojilerin güvenlik bağlamı dışında insan hakları üzerindeki etkisine dair daha geniş bir bakış açısı benimsemek arasında iyi bir denge kurmuştur. Bu konu bugüne kadar yeterince ele alınmamış bir konudur.[42]

Özel Raportör tarafından daha sonraki yıllarda hazırlanan raporlarda da şu konular üzerinde durulmuştur: Ulusal ve uluslararası perspektiften hükümetlerin izleme faaliyetleri (2017 raporu).[43] Güvenlik ve İzleme (2018 raporu).[44] Toplumsal cinsiyet perspektifinden mahremiyet hakkı, teknoloji ve diğer insan hakları (2019 raporu).[45] Güvenlik ve izleme, sağlık verileri ve işletmelerin kişisel verileri kullanımı (2020 raporu).[46] Yapay zekâ ve mahremiyet hakkı ve çocukların mahremiyet hakkı (2021 raporu).[47] İbero-Amerika'da mahremiyet hakkı ve kişisel verilerin koruması: Küreselleşmeye doğru bir adım? (2022 raporu).[48] COVID-19 pandemisi bağlamında kamu kurumları tarafından toplanan kişisel verilerin işlenmesinde amaçların sınırlandırılması, verilerin silinmesi ve kanıtlanmış veya proaktif hesap verebilirlik ilkelerinin uygulanması (2023 raporu).[49] Dijital çağda kişisel verilerin koruması ve gizliliğinin sağlanmasına yönelik yasal güvenceler (2024 raporu).[50] Mahremiyet hakkı perspektifinden nöroteknolojiler ve nöroverilerin işlenmesine ilişkin örnek bir yasanın geliştirilmesine yönelik temel esaslar (2025 raporu).[51] Kişisel verilerin uluslararası alanda toplanması (2026 raporu).[52]

[42] Lorna McGregor, "First Report of the UN Special Rapporteur on the Right to Privacy to the Human Rights Council", 18.03.2016, Blog of the European Journal of International Law, https://www.ejiltalk.org/first-report-of-the-un-special-rapporteur-on-the-right-to-privacy-to-the-human-rights-council/ (erişim: 06.06.2026)

[43] A/HRC/34/60, (2017) Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/34/60 (erişim: 07.06.2026)

[44] A/HRC/37/62, (2018) Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/37/62 (erişim: 06.06.2026)

[45] A/HRC/40/63, (2019) Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/40/63. (erişim: 07.06.2026)

[46] A/HRC/43/52, (2020) Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/43/52 (erişim: 07.06.2026)

[47] A/HRC/46/37, (2021) Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/46/37 (erişim: 08.06.2026)

[48] A/HRC/49/55, (2022) Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/49/55 (erişim: 08.06.2026)

[49] A/HRC/52/37, (2023) Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/52/37 (erişim: 08.06.2026)

[50] A/HRC/55/46, (2024) Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/55/46 (erişim: 08.06.2026)

[51] A/HRC/58/58, (2025) Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/58/58 (erişim: 08.06.2026)

[52] A/HRC/61/48, (2026) Report of the Special Rapporteur on the right to privacy, https://docs.un.org/en/A/HRC/61/48 (erişim: 08.06.2026)

D. BM Genel Kurulunun 71/199 Sayılı Kararı

BM Genel Kurulu "Dijital Çağda Mahremiyet Hakkı" kararını 2016 yılında 71/199 sayılı karar[53] ile üçüncü kez güncellemiştir. Bu kararın kişisel veriler açısından en önemli özelliği, kişisel verilerin korunması alanında özel sektöre düşen yükümlülüklerin yerine getirilmesi konusunda özel sektöre doğrudan çağrı yapılmasıdır. Kararda özel sektörden, kullanıcıların mahremiyet haklarını etkileyebilecek verilerinin toplanması, kullanımı, paylaşımı ve saklanması hakkında kullanıcıları bilgilendirmeleri ve uygun şeffaflık politikaları oluşturmaları istenmiştir.[54] Ayrıca, özel sektörden güvenli iletişimi sağlama ve teknik çözümler geliştirme de dahil, bireysel kullanıcıları mahremiyet haklarına yönelik yasa dışı müdahalelere karşı korumak amacıyla çalışmalar yapmaları istenmiştir.[55]

Önceki kararlardan farklı olarak, 71/199 sayılı kararda dijital çağda mahremiyet hakkına yönelik ihlallerin kadınlar, çocuklar ve kırılgan veya ötekileştirilmiş kişiler üzerinde etkisi de ele alınmış ve bu kesimlere yönelik ihlallere karşı önleyici tedbirlerin ve çözüm yollarının geliştirilmesi gerektiği belirtilmiştir.[56]

İnsan Hakları Yüksek Komiserliği Genel Kurulun 71/199 sayılı kararı doğrultusunda hazırladığı 39/29 sayılı raporda[57] devletlerden, hem kamu hem de özel sektörün kişisel verilerin gizliliğini ihlal eden uygulamalarını araştırma, bu konuda bireylerden ve kuruluşlardan gelen şikayetleri inceleme ve kişisel verilerin hem kamu hem de özel sektör tarafından yasa dışı bir şekilde işlenmesi durumunda para cezaları ve diğer etkili yaptırımlar uygulama yetkisine sahip bağımsız otoriteler kurmaları istenmiştir. [58]

E. BM Genel Kurulunun 73/179 Sayılı Kararı

BM Genel Kurulu "Dijital Çağda Mahremiyet Hakkı" başlıklı kararını 2018 yılında kabul ettiği 73/179 sayılı karar[59] ile dördüncü kez güncellemiştir. 73/179 kararın en önemli özelliği, yapay zekâ teknolojilerinin kişisel veriler açısından yaratacağı tehlikelere dikkat çekmesidir. Uygun güvenceler sağlanmadan yapay zekâ teknolojilerinin kullanımının insan haklarını olumsuz etkileyebilecek kararlara yol açabileceği; bu nedenle, söz konusu teknolojilerin tasarımında, değerlendirilmesinde ve düzenlenmesinde uluslararası insan hakları hukukunun uygulanmasının son derece önemli olduğu belirtilmiştir.

Kararda ayrıca hassas biyometrik verilerin artan bir şekilde toplanması konusu da ele alınmış ve özel sektör tarafından bu verilerin toplanması, işlenmesi ve paylaşımı konusu

[53] A/RES/71/199, (2016) The right to privacy in the digital age. Resolution adopted by the General Assembly on 19 December 2016, https://docs.un.org/en/A/RES/71/199 (erişim: 10.06.2026)
[54] A/RES/71/199, para.6/b.
[55] A/RES/71/199, para.7.
[56] A/RES/71/199, para.5/g.
[57] A/HRC/39/29, (2018), The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights on 3 August 2018, https://docs.un.org/en/a/hrc/39/29 (erişim: 11.06.2026)
[58] A/HRC/39/29, para.61.
[59] A/RES/73/179 (2018), The right to privacy in the digital age, Resolution adopted by the General Assembly on 17 December 2018. https://digitallibrary.un.org/record/1661346?v=pdf (erişim: 10.06.2026)

üzerinde durulmuştur. Ancak, biyometrik verilerin neleri içerdiği ve biyometrik yöntemlerin neler olduğu konusunda bir açıklama kararda yer almamıştır.

Yapay zekâ ve biyometrik teknolojilerinin yeterli güvenceler sağlanmadan son yıllarda çok geniş bir alanda kullanılması ve bu yaygın kullanımın insan haklarını ihlal etme riski taşıması bu konunun BM Genel Kurulu tarafından ele alınmasına neden olmuştur. Bugün yapay zekâ sistemleri; imalat ve üretim sanayi, havacılık ve uzay, eğitim, finans, savuma, güvenlik, adalet, sağlık ve insan kaynakları alanlarında yaygın şekilde kullanılmaktadır.[60] Yapay zekâ teknolojilerinin yaygın kullanımı özellikle kişisel veriler açısından önemli risklerin doğmasına neden olmaktadır.[61] Teknolojik gelişmeler özellikle yapay zekâ destekli elektronik gözetim sistemleri, özel hayatın gizliliği hakkını hem yeni hem de karmaşık tehditlerle karşı karşıya bırakmaktadır. Dijitalleşen dünyada mahremiyet, salt fiziksel alanlarda değil; veri tabanlarında ve algoritmik süreçlerde de korunması gereken temel bir hak haline gelmiştir. Bu nedenle, bireylerin özgürlük ve güvenlik dengesi gözetilerek, hukuki düzenlemelerin çağın gerekliliklerine uygun şekilde güncellenmesi büyük önem taşımaktadır.[62]

BM Genel Kurulu 73/179 sayılı kararında yapay zekâ teknolojilerinin yaratacağı bu riskleri dikkate alarak, insan haklarının korunabilmesi için özellikle dijital iletişimin gizliliğini korumaya yönelik teknik çözümlerin; şifreleme ve takma adlandırma (isim, kimlik numarası vb. gibi kişisel verilerin takma adlar veya kodlarla değiştirilmesi) ve anonimlik önlemleri dahil, çok önemli olduğunu ortaya koymuştur.[63]

Genel Kurul bu kararında İnsan Hakları Konseyini, İnsan Hakları Yüksek Komiserliğini ve ilgili tüm paydaşları yapay zekâ ve biyometrik teknolojilerin mahremiyet hakkını nasıl etkilediğini ayrıntılı olarak ele almaya çağırmıştır.[64]

Genel Kurulun yapmış olduğu çağrı doğrultusunda İnsan Hakları Konseyi tarafından 2019 yılında kabul edilen 42/15 sayılı kararda[65] yapay zekâ ve biyometrik teknolojilerinin kullanımının yaratacağı tehlikeler üzerinde ayrıntılı durulmuştur. Devletlerden, kişisel verilerin elde edilmesi ve toplanması, profil oluşturulması, yapay zekâ sistemlerinin ve biyometrik teknolojilerin kullanımıyla ilgili uygulamalarını ve mevzuatlarını gözden geçirmeleri ve gerekli değişiklikleri yapmaları istenmiştir.[66]

---

[60] Dilara Yüzer Eltimur, "İnsan Haklarının Korunması Bağlamında Yapay Zeka Uygulamaları", Akdeniz Üniversitesi Hukuk Fakültesi Dergisi, Cilt 12, Sayı: 2, Aralık 2022, https://doi.org/10.54704/akdhfd.1155778, (erişim:17.10.2026), s.563

[61] Nesrin Singil, "Yapay Zeka ve İnsan Hakları", Public and Private International Law Bulletin, Cilt:42, Sayı:1, (2022), http://ppil.istanbul.edu.tr/tr/_ (erişim:15.10.2026), s.22

[62] Betül Çatal**, "**Dijital Çağda Mahremiyetin Sınırları: Özel Hayatın Gizliliği Hakkı ve Elektronik Gözetim", Sakarya Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 13, Sayı: 2, (2025), https://doi.org/10.56701/shd.1719579 (erişim:16.10.2026), s.794

[63] Valentina Luna Colella, "Biometric Surveillance During Protests: A Security Matter or a Violation of Human Rights?", ITSS Verona Magazine, Cilt:2, Sayı:2 Fall/Winter (2023) https://www.itssverona.it/wp-content/uploads/2024/01/Valentina-Luna-Colella.pdf (erişim: 12.06.2026) s.16.

[64] A/RES/73/179, para.10.

[65] A/HRC/RES/42/15, Resolution adopted by the Human Rights Council on 26 September 2019 42/15. The right to privacy in the digital age, https://docs.un.org/en/A/HRC/RES/42/15 (erişim: 10.06.2026)

[66] A/HRC/RES/42/15, para.6/c.

F. BM GENEL KURULUNUN 75/176 SAYILI KARARI

Genel Kurul "Dijital Çağda Mahremiyet Hakkı"na ilişkin 2020 yılında kabul ettiği 75/176 sayılı kararda[67] da, yapay zekâ teknolojilerinin kullanımının neden olduğu sorunlar üzerinde ayrıntılı durmuştur. Ayrıca, biyometrik teknolojilerinin kullanımının yaratacağı sorunlar 73/179 sayılı karara göre daha ayrıntılı ele alınmıştır.

Karara göre, yapay zekâ teknolojilerinin kullanımı çoğu zaman çok büyük miktarda kişisel verinin işlenmesini gerektirmekte ve buna olanak sağlamaktadır. Bu veriler biyometrik verileri de içermektedir. Bu işlemler uygun güvenlik önlemleri alınmadan yapıldığında, özellikle de bireylerin kimlik tespiti, izlenmesi, profil oluşturma, yüz tanıma, sınıflandırma, davranış tahmini veya puanlanması için kullanıldığında, mahremiyet hakkı açısından ciddi riskler oluşturabilmektedir. Bu risklerin ortaya çıkmaması için yapay zekâ da dahil olmak üzere yeni ve gelişmekte olan dijital teknolojilerin tasarımında, geliştirilmesinde ve kullanımında gerekli önlemler alınmalıdır.[68]

Kararda özellikle biyometrik teknolojilerin yasa dışı kullanımının mahremiyet hakkını ihlal eden çok ağır bir müdahale olduğu ve bu tür müdahalelerin ifade özgürlüğü, barışçıl toplanma ve dernek kurma özgürlüğü ile din ve inanç özgürlüğünü ihlal ettiği belirtilmiştir. Kararda, mahremiyet hakkının düşünce ve ifade özgürlüğü, barışçıl toplanma ve dernek kurma özgürlüğü gibi diğer temel insan haklarıyla olan karşılıklı bağımlılığının ve bölünmezliğinin vurgulanması çok önemlidir. Ancak, devletleri özellikle uzaktan yüz tanıma teknolojisini kitlesel izleme için veya bir toplantıya katılanların kimliğini belirlemek için kullanmaktan kaçınmaya çağırmadığı ve bunun yasaklanmasını talep etmediği için eleştirilmiştir.[69]

Uzaktan yüz tanıma teknolojisinin kullanımın yasaklanması konusu BM tarafından ilk kez, BM İnsan Hakları Yüksek Komiserliğin BM İnsan Hakları Konseyine sunmuş olduğu 48/31 sayılı raporda[70] ele alınmıştır. Raporda, devletlerden gizlilik ve veri koruma standartlarına uygun gerekli yasal düzenlemeler yapılıncaya kadar, kamusal alanlarda uzaktan yüz tanıma yöntemi gibi biyometrik teknolojilerinin kullanımını durdurmaları istenmiştir. [71]

Yüz tanıma, dijital görüntüler üzerinde yer alan nesnelerin arasından insan yüzünün konumunu ve boyutunu belirleyen bir bilgisayar teknolojisidir.[72] Özellikle uzaktan yüz tanıma yöntemi son yıllarda çok yoğun kullanılan bir yöntemdir. Bu yöntem ile çok sayıda insanın görüntüsü onlar bu işlemin yapıldığını fark etmeden, uzak bir mesafeden hızlı bir şekilde taranabilmektedir. Diğer birçok biyometrik yöntem ise ancak kişilerin tarama cihazına çok yakın

[67] A/RES/75/176 (2020) The right to privacy in the digital age, Resolution adopted by the General Assembly on 16 December 2020, https://docs.un.org/en/A/RES/75/176 (erişim:11.06.2026)
[68] A/RES/75/176, para.6.
[69] Dünya genelinde ifade özgürlüğünü ve bilgi edinme hakkını savunan Article19 isimli uluslararası örgüt tarafından yapılan eleştiri için bkz. "UN: To protect privacy in the digital age, world governments can and must do more", 25.01.2021, https://www.article19.org/resources/un-to-protect-privacy-in-the-digital-age-world-goverments-can-and-must -do-more (erişim:11.06.2026)
[70] A/HRC/48/31 (2021), The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, https://docs.un.org/en/a/hrc/48/31 (erişim: 12.06.2026)
[71] A/HRC/48/31, para.59/d.
[72] Yaşar Safalı, Erdinç Avaroğlu, "Derin Öğrenme ile Yüz Tanıma ve Duygu Analizi" Avrupa Bilim ve Teknoloji Dergisi Sayı 31 (Ek Sayı 1), Aralık 2021, https://doi.org/10.31590/ejosat.1010450, (erişim:16.10.2026) s.765.

bir mesafede olması halinde kullanılabilmektedir.[73] Genellikle meşru amaçlara yönelik olarak kullanıldığı belirtilen bu yöntem (örneğin suçun önlenmesi veya kamu düzeninin korunması gibi) dernek çalışmalarını veya barışçıl toplantıları izlemek gibi amaçlarla da kullanılabilmektedir.[74]

Bu yöntem özellikle gösterilere katılan kişilerin kimliğini tespit etmek için son yıllarda çok kullanılan bir yöntemdir. BM İnsan Hakları Yüksek Komiserliğinin ilk kez 48/31 sayılı rapor ile uzaktan yüz tanıma yönteminin kullanılmasının durdurulmasını istemesi bu açıdan çok önemlidir.

BM Genel Kurulunun 75/176 sayılı kararından kısa bir süre sonra BM'nin uzman kuruluşu olan UNESCO da yapay zekâ teknolojilerinin kullanımının yaratabileceği tehlikeleri ele almış ve 2021 yılında "Yapay Zekâ Etiği Üzerine Tavsiye Kararı"nı[75] kabul etmiştir. Bu kararda kişisel verilerin korunması konusuna da yer verilmiştir. Üye devletlerden özellikle uluslararası hukuka uygun belirli istisnalar haricinde, bireylere yapay zekâ sistemlerinde yer alan kendi kişisel verilerine erişebilme ve bu verileri sildirebilme olanağı tanımaları; verilerin mikro hedefli reklamcılık gibi ticari amaçlarla kullanıldığı veya sınır ötesine aktarıldığı durumlarda, veri koruma mevzuatına tam uyumlu, yeterli düzeyde bir koruma sağlamaları ve bu amaçla etkili ve bağımsız çalışacak bir denetim mekanizması kurmaları istenmiştir.[76]

G. BM Genel Kurulunun 77/211 Sayılı Kararı

BM Genel Kurulu "Dijital Çağda Mahremiyet Hakkı"na ilişkin 2022 yılında kabul ettiği 77/211 sayılı kararda[77] da yine yapay zekâ ve biyometrik teknolojilerin kullanılmasının mahremiyet hakkı ve kişisel veriler üzerindeki etkisini ayrıntılı ele almıştır.

Karar, Covid-19 pandemisinin yaşandığı bir süreçte alındığı için, bu sürecin kişisel veriler üzerindeki etkisi de ele alınmıştır. Karara göre, yeni ve gelişmekte olan dijital teknolojiler, Covid-19 pandemisi de dahil olmak üzere sağlık alanındaki acil sorunların çözümüne katkıda bulunmaktadır Bu süreçte sağlıkla ilgili olanlar dahil, kişisel verilerin korunması son derece önemlidir. Ancak, örneğin temas takibi gibi, Covid-19 pandemisiyle mücadele çabalarının bazıları mahremiyet hakkını olumsuz etkilemiştir.

Covid-19 pandemisi sırasında çeşitli izleme yöntemleri kullanılmıştır. İzleme yöntemleri arasında mobil uygulamalar yoluyla izleme önemli bir yer tutmuştur. Pandemi

[73] Christopher S. Milligan, "Facial Recognition Technology, Video Surveillance, and Privacy", Southern California Interdisciplinary Law Journal , Cilt:9, Sayı:1, (1999), s.311.

[74] Gina Romero, Pete Fussey ve Daragh Murray, "Pushed into Shadow: Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association", 13.06.2026,https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf (erişim:10.05.2026)s.11.

[75] UNESCO, Recommendation on the Ethics of Artificial Intelligence, UNESCO Doc. SHS/BIO/REC-AI/2021/1 (Nov. 23, 2021) https://unesdoc.unesco.org/ark:/48223/pf0000381137 (erişim:16.10.2026)

[76] UNESCO Doc. SHS/BIO/REC-AI/2021/1, para.73

[77] A/RES/77/211 (2022) The right to privacy in the digital age, Resolution adopted by the General Assembly on 15 December 2022, https://docs.un.org/en/A/RES/77/211 (erişim: 13.06.2026)

süresince özellikle temas takibi yapan mobil uygulamalar yaygın olarak kullanılmıştır.[78] Bazı uygulamalar enfekte olmuş kişilerin temasta bulunduğu kişileri takip etmeyi amaçlarken, diğerleri ise evde kalma emirlerinin uygulanmasını kontrol etmeyi amaçlamıştır.[79] Bu tür uygulamaların yaygın olarak kullanımın kişisel veriler açısından oluşturduğu risk dikkate alındığında, BM'nin konuyu ele alması ve devletleri bu alandaki riskler konusunda uyarması önemlidir.

Bu karardaki en önemli yenilik, yapay zeka teknolojisinin uygulama alanlarından biri olan algoritmik karar verme sistemlerinin uygulanmasının ve belirli tahmin algoritmaların kullanımının kişisel veriler açısından yaratacağı olumsuz sonuçların ele alınmasıdır. Karara göre, çevrimiçi ortamda algoritmik veya otomatik karar verme süreçlerinin kullanımı, kullanıcıların çevrimiçi bilgiye erişimini ve düşünce ve ifade özgürlüğünü zayıflatacaktır.

Algoritmalar kullanıcıların geçmiş davranışlarından yola çıkarak, örneğin, sosyal medya platformlarında hangi kullanıcıya hangi reklamın gösterileceği veya kullanıcının hangi (film, müzik, kitap vb. içerikleri beğenebileceği hakkında karar vermek ve önerilerde bulunmak amacıyla sık sık kullanılmaktadır.[80]

Algoritmik karar verme sistemi, makinelerin görevleri otomatik olarak tamamlamasını ve/veya kararlar almasını sağlayan hesaplama yöntemlerinin kullanımını ifade eder. Algoritmalar, mevcut olan çok büyük miktardaki elektronik veriler sayesinde karar verebilir. Genellikle büyük veri olarak tanımlanan bu verilerle, kuruluşlar giderek daha büyük ve karmaşık operasyonlar yürütebilir, müşteri ve diğer iş verilerini toplayabilir, depolayabilir ve işleyebilirler.[81]

Tahmin algoritmaları ise, gelecekteki sonuçları tahmin etmek için geçmiş verilerden yararlanan gelişmiş matematiksel modellerdir. Verilerdeki kalıpları, korelasyonları ve eğilimleri analiz ederek doğru tahminler elde edilmesini sağlar. Tahmin algoritmaları anlamlı sonuçlar elde etmek, eğilimleri tahmin etmek ve veriye dayalı kararlar almak için yaygın olarak kullanılır.[82] Belirli tahmin algoritmaları şirketlerin stratejik kararlar almasını sağlayan ve şirketler açısından riskleri en aza indirmesini sağlayan modern veri analitiği araçlarıdır.[83]

[78] Paul Schwartz, "Protecting Privacy on COVID-19 Surveillance apps", IAPP, 08.05.2020, https://iapp.org/news/a/protecting-privacy-on-covid-surveillance-apps (erişim: 13.06.2026)

[79] Tatsiana Ziniakova, "Privacy, Mass Electronic Surveillance, and the Rule of Law in Times of COVID-19", World Justice Project, 2020,https://worldjusticeproject.org/sites/default/files/documents/Surveillance%20COVID_v4.pdf (erişim: 14.06.2026) s.6.

[80] Hüseyin Can Aksoy, "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", Kişisel Verileri Koruma Dergisi, Cilt: 4 Sayı:2, (2022), https://izlik.org/JA38BX44TH (erişim:16.10.2026) s.73

[81] Christoph F. Breidbach, "Responsible Algorithmic Decision-making", Organizational Dynamics, Cilt: 53 Sayı:2, (2024) 101031, https://www.sciencedirect.com/science/article/pii/S0090261624000044 (erişim: 10.05.2026) s.2.

[82] Swati Gupta-Balkishan, ve Preeti Gulia, "Comparative Analysis of Predictive Algorithms for Performance Measurement", IEEE Access, Cilt: XX, (2017) https://www.researchgate.net/publication/378669257_Comparative_Analysis_of_Predictive_Algorithms_for_Performance_Measurement (erişim: 10.05.2026) s.1.

[83] Teaganne Finn ve Ian Smalley, "Predictive Analytics, Defined" 10.06.2026, https://www.ibm.com/think/topics/predictive-analytics (erişim: 16.05.2026)

BM Genel Kurulunun 77/211 sayılı kararı doğrultusunda BM İnsan Hakları Konseyinin kabul ettiği 54/21 sayılı kararda[84] da algoritmaların kullanılmasının, kullanıcıların kişisel verileri açısından tehlike oluşturabileceği ve özellikle sosyal medya platformlarında yanlış bilgilendirme, dezenformasyon ve nefret söyleminden kaynaklanan tehditleri yoğunlaştırabileceği belirtmiştir.

H. BM Genel Kurulunun 79/175 Sayılı Kararı

BM Genel Kurulunun "Dijital Çağda Mahremiyet Hakkı" konusunu ele aldığı son kararı 2024 yılında kabul ettiği 79/175 sayılı karardır[85]. Bu kararda hem devletlerden hem de özel sektörden verilerin toplanması, işlenmesi ve saklanması sürecine ilişkin güvenlik standartlarını güçlendirmeleri istenmiş ve dijital izleme uygulamalarını yasallık, gereklilik ve orantılılık ilkelerine dayandırmalarını talep etmiştir.

Özel sektörden iş operasyonlarını veri toplama ve veri işleme uygulamalarını gözden geçirerek BM standartlarına uygun hale getirmeleri ve sundukları ürünlerin ve faaliyetlerinin özellikle de algoritmaların rolünün, insan hakları üzerindeki etkilerini incelemeleri ve gerekli düzeltmeleri yapmaları istenmiştir.

BM Genel Kurulu yapay zekâ ve biyometrik teknolojilerinin kullanımının kişisel veriler açısından doğurduğu olumsuz sonuçlar hakkında önceki kararlarındaki açıklamaları bu kararında da tekrarlamıştır. Ancak, Genel Kurul önceki kararlarında yer almayan önemli bir hususa bu kararda yer vermiştir. Karara göre, yüz tanıma da dahil olmak üzere uzaktan biyometrik izleme sistemleri, uygun ve özel güvenlik önlemleri olmadan kullanıldığında, son derece müdahaleci nitelikte oldukları için ve çok sayıda insanı geniş çapta etkilemeleri söz konusu olduğu için bu yöntemlerin kullanılması orantılılık ilkesini ihlal edebilecektir.[86]

79/175 sayılı kararın dijital çağda mahremiyet hakkına ilişkin önceki kararlardan diğer bir farkı da bu kararda yeni ve gelişmekte olan dijital teknolojilerin, özellikle yardımcı dijital teknolojilerin, engelli bireyler üzerindeki etkisine değinilmesidir. Tüm işletmelere, özellikle de veri toplayan, saklayan, kullanan, paylaşan ve işleyen işletmelere engelliler de dahil olmak üzere, tüm kullanıcıları mahremiyet haklarını etkileyebilecek verilerinin toplanması, işlenmesi, paylaşımı ve saklanması konusunda bilgilendirmeleri çağrısını yapmıştır[87]

İ. BM Genel Kurulunun 78/265 Sayılı Kararı

Yapay zekâ teknolojilerinin son yıllarda yaygın bir şekilde kullanılması ve bu teknolojilerin kullanımının mahremiyet hakkına ve kişisel verilere yönelik önemli tehditler içermesinden dolayı BM Genel Kurulu bu konuyu "Dijital Çağda Mahremiyet Hakkı" kararlarından ayrı bir kararda daha ayrıntılı olarak ele almıştır.

[84] A/HRC/RES/54/21 (2023) Right to privacy in the digital age, Resolution adopted by the Human Rights Council on 12 October 2023, https://docs.un.org/en/a/hrc/res/54/21 (erişim: 16.06.2026)
[85] A/RES/79/175 (2024) The right to privacy in the digital age, Resolution adopted by the General Assembly on 17 December 2024, https://docs.un.org/en/A/RES/79/175 (erişim: 10.06.2026)
[86] A/RES/79/175, para.7.
[87] A/RES/79/175, para.9/b.

Bu karar 2024 yılında kabul edilen "Sürdürülebilir Kalkınma İçin Güvenli, Emniyetli ve Güvenilir Yapay Zekâ Sistemlerinin Sunduğu Olanaklardan Yararlanılması" başlıklı 78/265 sayılı karardır.[88] Karar, yapay zekâ düzenlemeleri ve uygulamaları konusunda devletlere ve ilgili tüm paydaşlara rehberlik için bir temel oluşturmayı amaçlamaktadır. Kararda öncelikle tüm üye devletlerden ve diğer paydaşlardan, insan haklarını ihlal eden, özellikle de kırılgan durumda olanlar açısından aşırı risk oluşturan, yapay zekâ sistemlerinin kullanımını durdurmaları istenmiştir.[89]

Kararda kişisel verilerin korunması konusuna da ayrıntılı yer verilmiştir. Bu konuda devletlerden ve ilgili tüm ilgili paydaşlardan şu hususları dikkate almaları istenmiştir: Yapay zekâ sistemlerinin yaşam döngüsü boyunca kişisel verilerin koruması ve mahremiyet politikaları da dahil olmak üzere, veri güvenliği mekanizmalarının geliştirilmesi ve uygulanması[90]; yapay zekâ sistemlerin test edilmesi ve değerlendirilmesi sırasında mahremiyet hakkının ve kişisel verilerin korunması ve kişisel verilerin kullanımına ilişkin olanlar da dahil, geçerli uluslararası, ulusal ve ulus-altı yasal çerçevelere uygun olarak şeffaflığın sağlanması ve raporlama yükümlülüğünün yerine getirilmesi[91]; kullanıcıları etkileyen kararlar alan veya destekleyen yapay zekâ sistemlerinin yaşam döngüsü boyunca aktif insan gözetiminin sağlanması.[92]

Yapay zekâ sistemlerinin aktif insan gözetimi altında yürütülmesi oldukça önem taşımaktadır. Aktif insan gözetimi, yapay zekâ kullanımının insan hakları açısından doğuracağı riskleri önlemek veya azaltmak ve güvenli, etik ve hesap verebilir kalmasını sağlamak için şarttır.[93]

Yapay zekâ sistemlerin tüm dünyada insanlığın yararına sunulmasını amaçlayan 78/265 sayılı karar güvenli, emniyetli ve güvenilir yapay zekâ sistemlerinin geliştirilmesini ve insan haklarına uygunluğunu sağlamayı hedefleyen önemli bir belgedir. Ancak, bu karar da üye devletler açısından bağlayıcı olmayan tavsiye niteliğinde bir karardır. Oysa aynı yıl Avrupa Birliği bu alanda üye devletleri bağlayıcı nitelikte olan "Yapay Zekâ Hakkında Uyumlaştırılmış Kurallar Getiren ve Bazı Birlik Yasama Tasarruflarını Değiştiren 2024/1689 Sayılı Tüzüğü"[94] kabul etmiştir. BM'nin de bu alanda bağlayıcı nitelikte bir belge kabul etmesi yapay zekâ sistemlerinin doğurduğu risklere karşı etkili bir koruma mekanizmasının oluşturulmasını sağlayabilir.

[88] A/RES/78/265 (2024) Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development, Resolution adopted by the General Assembly on 21 March 2024, https://docs.un.org/en/A/RES/78/265 (erişim: 18.06.2026)
[89] A/RES/78/265, para.5.
[90] A/RES/78/265, para.6/e.
[91] A/RES/78/265, para.6/j.
[92] A/RES/78/265, para.6/k.
[93] Romero, Fussey ve Murray, "Pushed into Shadows: Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association", s.14.
[94] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L2024/1689, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689 (erişim: 10.06.2026)

DEĞERLENDİRME VE SONUÇ

BM kişisel verilerin korunması konusunu ele alan ilk kararı 1990 yılında kabul etmiştir. Bu karar Genel Kurul tarafından kabul edilen "Bilgisayar Ortamında işlenen Kişisel Veri Dosyalarının Düzenlenmesine ilişkin Rehber İlkeler"dir. Bu karar ile kişisel verilerin korunması için BM üyesi devletlerin ulusal mevzuatlarında kabul edilmesi gerekli olan asgari güvenceler belirlenmiştir. Kararda yalnızca bilgisayar ortamında işlenen kişisel veri dosyaları açısından güvencelere yer verilmiştir. Kararın uygulama alanı oldukça dardır. Diğer önemli bir sorun da, Kararda kişisel verilerin korunması sorununun temel bir insan hakkı sorunu olarak ele alınmamasıdır. Kişisel verilerin korunması sorunu, bilgisayar ortamında işlenen dosyaların güvenliğini ve doğruluğunu sağlamayı amaçlayan teknik bir veri yönetimi sorunu olarak ele alınmıştır.

2013 yılında Edward Snowden'ın devletlerin kitlesel izleme faaliyetlerini ortaya koyan açıklamalarının dünya genelinde yarattığı büyük tepki ve BM'nin kişisel verilerin korunması konusunda oldukça yetersiz kaldığı yönünde yapılan eleştiriler BM'nin bu alanda yaklaşımını değiştirmesine neden olmuştur. BM bu tarihten itibaren kişisel verilerin korunması konusunda insan hakları merkezli bir yaklaşım ortaya koymaya başlamıştır. 2013 yılında Genel Kurul tarafından "Dijital Çağda Mahremiyet Hakkı" başlıklı kararın kabulü bu alanda bir dönüm noktası olarak değerlendirilebilir. Bu kararda kişisel verilerin toplanması, işlenmesi ve saklanması alanındaki ihlaller doğrudan insan hakları ihlalleri olarak tanımlanmıştır.

BM genel kurulunun her iki yılda bir güncellenen "Dijital Çağda Mahremiyet Hakkı" başlıklı kararlarında 2018 yılından itibaren önemli bir değişim gerçekleşmiştir. Bu yıl güncellenen "Dijital Çağda Mahremiyet Hakkı" başlıklı kararda yapay zekâ teknolojilerinin kişisel veriler açısından yaratacağı tehlikeler de ele alınmıştır. BM 2020 yılından sonra aldığı kararlarda da yapay zekâ teknolojilerinin yaratacağı tehlikeleri ve bu alanda yapılması gerekenleri daha ayrıntılı düzenlemiştir. Uygun güvenceler sağlanmadan yapay zekâ teknolojilerinin yaygın kullanımının çok ciddi insan hakları ihlallerine yol açabileceği gerçeği BM'nin bu konuda adım atmasını zorunlu kılmıştır.

Gerek BM Genel Kurulu gerekse BM İnsan Hakları Konseyi tarafından bugüne kadar kabul edilen ve kişisel verilerin korunması konusunda düzenlemeler içeren kararlar bağlayıcı kararlar değildir. Bu alanı düzenleyen ve bağlayıcı nitelikte olan bir uluslararası sözleşmenin BM tarafından şimdiye kadar kabul edilmemiş olması önemli bir eksikliktir.

Avrupa Konseyi ve Avrupa Birliği gibi bölgesel örgütler bu alanda bağlayıcı belgeler kabul etmişken, BM gibi uluslararası bir örgütün bu konuda evrensel nitelikte bağlayıcı olan bir düzenleme yapmamış olması önemli bir yasal boşluğun oluşmasına neden olmakta ve bu alanda güçlü bir koruma sisteminin oluşturulmasını engellemektedir.

Yeni teknolojiler eşi benzeri görülmemiş bir hızla ilerlemeye ve kişisel veriler açısından önemli bir tehdit oluşturmaya devam etmektedir. Bu nedenle, BM kişisel verilerin korunması sorununu temel odak noktalarından biri haline getirmelidir.

Günümüzde kişisel veriler açısından en önemli tehdit yapay zekâ ve biyometrik teknolojilerinin kullanımından kaynaklanmaktadır. Özellikle bu alanda gerekli güvencelerin sağlanması son derece önem taşımaktadır. Hem devletler hem de özel sektörün bu alandaki yükümlülüklerini yerine getirmeleri için BM tarafından daha güçlü bir baskı oluşturulması gerekmektedir. Tüm üye devletler açısından bağlayıcı olacak bir sözleşme kabul etmesi BM'nin bu alanda atacağı en önemli adım olacaktır.

BM kararlarında ortaya konulan ilkelerin, bu ilkeler bağlayıcı bir sözleşme metninde düzenlenmemiş olsa dahi, BM üyesi ülkeler tarafından ulusal mevzuatlarına dahil edilmeleri gerekir. Hem devletlerin hem de özel şirketlerin bu ilkelere uyması bireylerin mahremiyet hakkının ve kişisel verilerinin korunması açısından temel önemdedir.

KAYNAKÇA

Aksoy, Hüseyin Can, "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme", Kişisel Verileri Koruma Dergisi, Cilt: 4 Sayı:2, (2022), https://izlik.org/JA38BX44TH (erişim:16.10.2026) (ss.69-87)

Bakir, Vian, Martina Feilzer ve Andrew McStay. "Introduction to Special Theme Veillance and Transparency: A Critical Examination of Mutual Watching in the Post-Snowden, Big Data Era", Big Data & Society Cilt:4, Sayı:1 (2017) https://journals.sagepub.com/doi/10.1177/2053951717698996 (erişim:26.04.2026) (ss.1-5)

Breidbach, Christoph F. "Responsible Algorithmic Decision-making", Organizational Dynamics, Cilt: 53 Sayı: 2, (2024) 101031, https://www.sciencedirect.com/science/article/pii/S0090261624000044 (erişim: 10.05.2026) (ss.1-7)

Colella, Valentina Luna. "Biometric Surveillance During Protests: A Security Matter or a Violation of Human Rights?", ITSS Verona Magazine, Cilt:2, Sayı:2 Fall/Winter (2023) https://www.itssverona.it/wp-content/uploads/2024/01/Valentina-Luna-Colella.pdf (erişim: 12.06.2026)

Çatal, Betül, "Dijital Çağda Mahremiyetin Sınırları: Özel Hayatın Gizliliği Hakkı ve Elektronik Gözetim", Sakarya Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 13, Sayı: 2, (2025), https://doi.org/10.56701/shd.1719579 (erişim: 16.10.2026) (ss.776-800)

Donahoe, Eileen. "Human Rights in the Digital Age", Just Securiy, 23.12.2014, https://www.justsecurity.org/18651/human-rights-digital-age/ (erişim: 04.05.2026)

De Hert, Paul ve Evangelos Papakonstantinou. "Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?", I/S: A Journal of Law and Policy for Information Society, Cilt:9, Sayı: 2, (2013) https://cris.vub.be/ws/portalfiles/portal/17831773/pdh13_vpISjournalthreescenariosUNagency.pdfs (erişim:15.04.2026) (ss.271-324)

Eltimur, Dilara Yüzer, "İnsan Haklarının Korunması Bağlamında Yapay Zeka Uygulamaları", Akdeniz Üniversitesi Hukuk Fakültesi Dergisi, Cilt 12, Sayı:2, Aralık 2022, https://doi.org/10.54704/akdhfd.1155778, (erişim:17.10.2026) (ss.559-594)

Frumkin, Dan, Adam Wasserstrom, Ariane Davidson ve Arnon Grafit. "Authentication of forensic DNA samples", Forensic Science International: Genetics, Cilt: 4, Sayı: 2 (2010) http://www.sakkyndig.com/psykologi/artvit/frumkin2010.pdf (erişim: 20.04.2026), (ss.95–103); Andrew Pollack, "DNA Evidence Can Be Fabricated, Scientists Show", the New York Times, 17.08.2009 https://www.nytimes.com/2009/08/18/science/18dna.html. (erişim:20.04.2026)

Finn, Teaganne ve Ian Smalley. "Predictive Analytics, Defined" 10.06.2026, https://www.ibm.com/think/topics/predictive-analytics (erişim: 16.05.2026)

Gupta, Swati, Balkishan, ve Preeti Gulia. "Comparative Analysis of Predictive Algorithms for Performance Measurement", IEEE Access, Cilt: XX, (2017) https://www.researchgate.net/publication/378669257_Comparative_Analysis_of_Predictive_Algorithms_for_Performance_Measurement (erişim: 10.05.2026) (ss.1-17)

Hassani, Hossein, Xu Huang, Steve MacFeely ve Mohammad Reza Entezarian. "Big Data and the United Nations Sustainable Development Goals (UN SDGs) at a Glance", Big Data and Cognitive Computing. Cilt:5, Sayı:3 (2021) https://www.mdpi.com/2504-2289/5/3/28 (erişim: 16 Mayıs 2026) (ss.1-29)

Joyce, Daniel. "Privacy in the Digital Era: Human Rights Online?", Melbourne Journal of International Law, Cilt: 16, Sayı:1, 2015, https://law.unimelb.edu.au/__data/assets/pdf_file/0003/1586811/16109Joyce2.pdf (erişim: 10.04.2026)

Kosta, Eleni, Martin Meints, Marit Hansen ve Mark Gasson. "An Analysis of Security and Privacy Issues Relating to RFID Enabled ePassports", New Approaches for Security, Privacy and Trust in Complex Environments. (haz. Hein Venter, Mariki Eloff, Les Labuschagne, Jan Eloff, Rossouw Solms,) International Federation for Information Processing, Cilt 232. (2007) Springer, Boston, MA. https://link.springer.com/chapter/10.1007/978-0-387-72367-9_42#preview (erişim: 15.04.2026) (ss. 467-472)

Li, Lanxin, Jiarou Wang, Xi Wang, Peng Peng, Jiaying Shen, Haining Zhu ve Ziyang Zhang. "Big Data and Data Science in Global Governance: Anticipating Future Needs and Applications in the UN and Beyond", Frontiers in Political Science, 18 Ağustos 2025, https://researchonline.lse.ac.uk/id/eprint/129350/1/fpos-07-1583772.pdf (erişim: 26.05.2026) (ss.1-26)

Macaskill, Ewen ve Gabriel Dance. 'NSA Files: Decoded', The Guardian, 01.11.2023 https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (erişim: 25.04.2026)

McGregor, Lorna. "First Report of the UN Special Rapporteur on the Right to Privacy to the Human Rights Council", 18.03.2016, Blog of the European Journal of International Law, https://www.ejiltalk.org/first-report-of-the-un-special-rapporteur-on-the-right-to-privacy-to-the-human-rights-council/ (erişim: 06.06.2026)

Milanovic, Marko. "OHCHR Publishes Report on Surveillance and Privacy in the Digital Age,", Blog of the European Journal of International Law, https://www.ejiltalk.org/ohchr-publishes-report-on-surveillance-and-privacy-in-the-digital-age/ (erişim: 02.06.2026)

Milligan, Christopher S. "Facial Recognition Technology, Video Surveillance, and Privacy", Southern California Interdisciplinary Law Journal, Cilt:9, Sayı:1, (1999) (ss.295-333)

Peterson, Joseph L., Anna S. Leggett. "The Evolution of Forensic Science: Progress Amid the Pitfalls", Stetson Law Review, Cilt:36, (2007), https://stetsonlawreview.org/wp-content/uploads/2022/02/36.3.02.Peterson.pdf (erişim: 17.04.2026) (ss.621-660)

Privacy International, "Recognition of Privacy in UN Human Rights Mechanisms", 02-05.2018, https://privacyinternational.org/privacy-un-human-rights-mechanisms (erişim: 04.05.2026)

Privacy International, "UN: To protect privacy in the digital age, world governments can and must do more", 25.01.2021, https://www.article19.org/resources/un-to-protect-privacy-in-the-digital-age-world-goverments-can-and-must -do-more (erişim:11.06.2026)

Romero, Gina, Pete Fussey ve Daragh Murray. "Pushed into Shadow: Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association", 13.06.2026,https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf (erişim:10.05.2026)

Safalı Yaşar, Erdinç Avaroğlu, "Derin Öğrenme ile Yüz Tanıma ve Duygu Analizi" Avrupa Bilim ve Teknoloji Dergisi Sayı 31 (Ek Sayı 1), Aralık 2021, https://doi.org/10.31590/ejosat.1010450, (erişim:16.10.2026) (ss. 764-770)

Schwartz, Paul. "Protecting Privacy on COVID-19 Surveillance apps", IAPP, 08.05.2020, https://iapp.org/news/a/protecting-privacy-on-covid-surveillance-apps. (erişim: 13.06.2026)

Singil, Nesrin, "Yapay Zeka ve İnsan Hakları", Public and Private International Law Bulletin, Cilt:42, Sayı:1, (2022), http://ppil.istanbul.edu.tr/tr/_ (erişim:15.10.2026) (ss.121-158)

Tan, Qing ve Frederique Pivot. "Big Data Privacy: Changing Perception of Privacy", 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (Smart City) 2015, https://ieeexplore.ieee.org/document/7463831 (erişim: 20.05.2026) (ss. 860-865)

United Nations Global Pulse "Big Data for Develeopment: Challenges and Opportunities", (2012) New York, https://unstats.un.org/unsd/trade/events/2014/beijing/documents/globalpulse/Big%20Data%20for%20Development%20-%20UN%20Global%20Pulse%20-%20June2012.pdf (erişim: 20.05.2026)

Yilma, Kinfe Micheal. "The United Nations' Evolving Privacy Discourse and Corporate Human Rights Obligations", American Society of International Law, Cilt: 23, Sayı:: 4, (2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4215111 (erişim:27.05.2026) (ss.1-5)

Ziniakova, Tatsiana ."Privacy, Mass Electronic Surveillance, and the Rule of Law in Times of COVID-19", World Justice Project, 2020,https://worldjusticeproject.org/sites/default/files/documents/Surveillance%20COVID_v4.pdf (erişim: 14.06.2026)

Extended Summary

The United Nations' Work on the Protection of Personel Data

Songül Atak, Assist. Prof..
Dicle University, songulatak@hotmail.com
https://orcid.org/0000-0002-2573-7602

In recent years, rapidly increasing technological advancements have posed a significant threat to the right to privacy and the protection of personal data. In particular, the use of artificial intelligence and biometric technologies has increased considerably worldwide in the last decade. The use of artificial intelligence and biometric technologies often requires and enables the processing of very large amounts of personal data, including biometric data.

These rapid technological advancements provide states and the private sector with much broader capabilities in obtaining, processing, and storing personal data. The most important justification for the widespread collection, processing, and storage of personal data by states is ensuring national security. However, this often leads to violations of individuals' fundamental rights and freedoms. The key here is to strike a balance between ensuring national security and protecting fundamental rights and freedoms.

International regulations are essential for the effective protection of personal data. The inadequacy of existing international regulations in protecting of personal data has been strongly voiced, particularly by international organizations. The high number of violations in this area, and especially the reactions from international organizations, have made it imperative for the United Nations to create regulations in this field.

This article examines the steps taken by the United Nations General Assembly in the field of personal data protection and analyzes its decisions in depth. Furthermore, this article also examines the work of the UN Human Rights Council, the UN Commissioner for Human Rights, and UN Special Rapporteurs in this area.

The focus of this study is on the resolutions adopted by the United Nations in the field of personal data protection. The factors that played a role in the preparation of these resolutions are examined, and it is assessed that the resolutions do not meet the needs in this area. In particular, the resolutions entitled "The Right to Privacy in the Digital Age," first adopted by the UN General Assembly in 2013 and subsequently updated at certain intervals, are examined in detail. The issue of personal data protection occupies an important place in these resolutions. The adequacy of these resolutions in terms of protecting personal data has been evaluated.

The study explains what artificial intelligence and biometric technologies, big data, algorithmic decision-making systems, and certain predictive algorithms, which

are prominent concepts in this field, are discussed, and clarifies the types of violations of privacy rights and personal data caused by the use of these technologies. Furthermore, the evaluations made regarding these decisions are included, and suggestions are put forward regarding the steps the UN should take to ensure stronger international protection of personal data in the future.

The study proposes that the UN adopt a convention binding on all member states in the field of personal data; that the UN put stronger pressure on both states and the private sector to fulfill their obligations in this area; and that, in general, the UN should make the issue of personal data protection one of its main focuses.

The primary research sources used in this study are the resolutions of the UN General Assembly, the UN Human Rights Council, the UN Human Rights Commissioner, and the reports prepared by UN Special Rapporteurs regarding the protection of personal data and the right to privacy. This study utilizes secondary sources such as international law textbooks, international journals, and other relevant scientific publications that address the issue of personal data protection.

The study is based on a doctrinal legal research approach. The study includes the resolutions adopted by the UN and doctrinal assessments related to the research topic. First, an analysis of the UN resolutions on the protection of personal data has been conducted; focusing on the nature of these resolutions, the problems addressed in them, and the solutions proposed. The study also includes doctrinal assessments of the issues posing risks in terms of personal data protection and how these issues are addressed in UN resolutions.

The analysis conducted in this study reveals that UN resolutions are not binding and therefore their impact is weak. It also shows that the UN generally acts late in addressing problems in this area.

The study argues that the most important problem in this area lies in the fact that a binding international convention has not been adopted, and that the United Nations lacks effective enforcement power in implementing its resolutions.