



The Boğaziçi Law Review

ISSN: 3023-4611

Journal homepage: <https://dergipark.org.tr/tr/pub/blr>

Bilgisayarlara Yetkisiz veya Erişim Yetkisini Aşarak Girme Suçu Hakkında Bir Amerika Birleşik Devletleri Yüksek Mahkemesi Kararı: Van Buren/Birleşik Devletler

A Decision of Supreme Court of the United States of America on the Crime of Accessing a Computer without Authorization or Exceeding Authorized Access

Burak Taş

To cite this article: US Supreme Court, ‘Van Buren v. Birleşik Devletler (Bilgisayarlara Yetkisiz veya Erişim Yetkisini Aşarak Girme Suçu Hakkında Bir Amerika Birleşik Devletleri Yüksek Mahkemesi Kararı)’, Burak Taş (çev.), (2024) 2(1) The Boğaziçi Law Review 93.

Submission Date: 21 February 2024

Acceptance Date: 28 July 2024

Article Type: Translation



© 2024 Burak Taş. Published with license by Boğaziçi University Publishing



Published online: September 2024



Submit your article to this journal [↗](https://dergipark.org.tr/tr/pub/blr)

Full Terms & Conditions of access and use can be found at
<https://dergipark.org.tr/tr/pub/blr>

BİLGİSAYARLARA YETKİSİZ VEYA ERİŞİM YETKİSİNİ AŞARAK GİRME SUÇU HAKKINDA BİR AMERİKA BİRLEŞİK DEVLETLERİ YÜKSEK MAHKEMESİ KARARI: VAN BUREN/ BİRLEŞİK DEVLETLER

SUPREME COURT OF THE UNITED STATES, VAN BUREN v. UNITED STATES (2021) (A DECISION OF SUPREME COURT OF THE UNITED STATES OF AMERICA ON THE CRIME OF ACCESSING A COMPUTER WITHOUT AUTHORIZATION OR EXCEEDING AUTHORIZED ACCESS)

Burak Taş 

Araştırma Görevlisi Doktor, Bolu Abant İzzet Baysal Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı.

Orijinal Dil: İngilizce

Yayınlayan: US Supreme Court (Amerika Birleşik Devletleri Yüksek Mahkemesi)

AMERİKA BİRLEŞİK DEVLETLERİ YÜKSEK MAHKEMESİ

VAN BUREN V. BİRLEŞİK DEVLETLER¹

AMERİKA BİRLEŞİK DEVLETLERİ İSTİNAF MAHKEMESİ 11. DAİRESİNE YAPILAN TEMYİZ BAŞVURU YAZISI ÜZERİNE

Kısa Karar

Sayı. 19-783. Tartışıldı. 30.11.2020 Karar Verildi. 3 Haziran 2021

Eski Georgia polis çavuşu Nathan Van Buren, devriye arabasındaki bilgisayarını kullanarak, para karşılığında belirli bir plaka numarası hakkında bilgi almak üzere bir kolluk kuvveti veri tabanına erişmiştir. Her ne kadar Van Buren arama yapmak için kendi geçerli kimlik bilgilerini kullanmış olsa da bu davranışı, görevin ifası dışı amaçlarla veri tabanı bilgilerinin elde edilmesine karşı departman politikasını ihlal etmiştir. Van Buren'in haberi olmadan, yaptığı eylemler Federal Soruşturma Bürosu'nun bir operasyonunun parçasıydı. Van Buren, 1986 tarihli Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Yasası'nı (CFAA) ihlal etmekle suçlandı; bu yasa, "bir bilgisayara yetkisi olmadan kasıtlı olarak erişen veya yetkisini aşan" kişileri cezai sorumluluğa tabi tutmaktadır. 18 U. S. C. §1030(a)(2). "Erişim yetkisinin aşılması" terimi "bir bilgisayara yetki dahilinde erişmek ve bu erişimi bilgisayarda erişimcinin elde etmeye veya değiştirmeye yetkili olmadığı bilgileri elde etmek veya değiştirmek için kullanmak" anlamına gelecek şekilde tanımlanmıştır. §1030(e)(6). Jüri Van Buren'i suçlu bulmuş ve Bölge Mahkemesi onu 18 ay hapis cezasına çarptırmıştır.

¹ <https://supreme.justia.com/cases/federal/us/593/19-783/case.pdf>

Van Buren, 11. Daire'ye istinaf başvurusunda bulunarak, "erişim yetkisini aşma" klozunun, sahip oldukları erişimi kötüye kullananlar için değil, yalnızca bilgisayar erişim yetkilerinin kapsamadığı bilgileri elde edenler için geçerli olduğunu savunmuştur. 11. Daire içtihadına uygun olarak, Kurul, Van Buren'in CFAA'yı ihlal ettiğine karar verdi.

Karar: Bir kişi, bilgisayara yetkisi kapsamında eriştiğinde ancak daha sonra bilgisayarın belirli alanlarında - dosyalar, klasörler veya veritabanları gibi - kendisine yasak olan bilgileri elde ettiğinde "erişim yetkisini aşar".

(1) Taraflar, Van Buren'in "yetkisi kapsamında bilgisayara eriştiği" ve "bilgisayardaki bilgileri elde ettiği" konusunda hemfikirlerdir. Taraflar, Van Buren'in bu bilgileri "elde etme hakkına sahip olup olmadığı" konusunda anlaşmazlık içinde dilerler. Van Buren, "bu şekilde"² kelimesinin bir atıf terimi mahiyetinde amaca hizmet ettiğini ve bu sebeple ihtilafı ifadenin "belirtildiği şekilde" ilgili bilgileri edinme hakkına sahip olup olmadığını sorduğunu iddia etmektedir. Başvurucu ayrıca, tanımlayıcı hükümde halihazırda belirtilen tek bilgi edinme yönteminin kişinin erişim yetkisine sahip olduğu bir bilgisayar olduğunu belirtmektedir. Dolayısıyla, "bu şekilde elde etme yetkisi yoktur" ifadesi açıkça kişinin erişim yetkisi olan bir bilgisayarı kullanarak elde etmesine izin verilmeyen bilgiye atıfta bulunmaktadır. Hükümet, "bu şekilde" ifadesinin daha geniş kapsamlı olduğunu, "elde etme hakkına sahip değildir" ifadesinin, kişinin elde ettiği belirli şekil veya koşullarda elde etmesine izin verilmeyen bilgilere atıfta bulunduğunu savunmaktadır. Hükümete göre, kişinin bilgi edinme hakkına sahip olduğu şekil veya koşullar, kişinin bilgiye erişim hakkına ilişkin "özel ve açık" olarak bildirilen sınırlamalarla tanımlanır. Van Buren'in "bu şekilde" ifadesi, "bu şekilde" ifadesini aynı şekilde kullanan diğer federal kanunların da yansıttığı gibi, terimin bir referans terimi olarak düz anlamı ile en iyi şekilde uyum sağlamaktadır.

(2) Hükümet, Van Buren'in kanaatinin "bu şekilde" ifadesini lüzumsuz hale getirdiğini iddia etmektedir. Hükümet, "bu şekilde" ifadesinin ancak bir kişinin bilgi edinme hakkını niteleyebilecek tüm koşulları içermesi halinde değerli bir katkı sağlayacağı konusunda ısrar etmektedir. Mahkeme bu görüşe katılmamaktadır çünkü "bu şekilde" ifadesi olmadan kanun, bir kişinin bilgi edinme hakkına ilişkin her türlü sınırlamayı içerecek şekilde yorumlanabilir.

(3) Karşıt görüş, Van Buren'in "bu şekilde" tanımını kabul etmekte, ancak Hükümetin vardığı sonuca "yetkili/hak sahibi olma" kelimesiyle ulaşmaktadır. Karşıt görüşe göre, "yetkili/hak sahibi olma" terimi, erişimin uygun olup olmadığının "duruma/koşullara bağlı" bir analizini gerektirmektedir. Ancak "yetkili/hak sahibi olma" terimi "elde etmek için" ifadesiyle değiştirilmiştir. Bu ifade de okuyucuyu, erişim hakkı sahibinin hakkı üzerindeki belirli bir sınırlamayı dik-

² Çevirmen notu: Kararda, ilgili kanun metninde yer alan "entitled so to obtain" ifadesindeki "so" kelimesine çok sık yer verilmektedir. Çeviri metninde "so" kelimesinin cümlenin anlamına lafzî bir katkı sağlaması beklenmektedir. Bu kapsamda "so" ifadesinin Türkçe karşılığı olarak metinde, kanun metnindeki klozlara referans verme işlevi taşıması misyonuyla "bu şekilde" ifadesinin kullanımı tercih edilmiştir.

kate almaya yönlendirmektedir: bilgiyi “daha önce belirtilen şekilde” elde etme hakkı. Daha önce de açıklandığı üzere, daha önce belirtilen şekilde erişim yetkisi olan bir bilgisayarı kullanmaktır. Karşıt görüşün yorumunu temellendirebilmesi için kanundan “bu şekilde” kelimesinin çıkarılarak değiştirilmesi gerekecektir.

(4) Hükümet; “genel ifadeyle”, “erişim yetkisini aşmak” ifadesinin, Van Buren’in kişisel amaçlar için plaka bilgilerini elde ettiğinde kolluk kuvvetleri veri tabanına “erişim yetkisini aştığı” anlamına geleceğini iddia etmektedir. Burada sorun Van Buren’in erişim yetkisini aşıp aşmadığı değil, *CFAA’nın bu ifadeyi tanımladığı şekilde* aşıp aşmadığıdır. Daha sonra gerekçelendirileceği üzere bu yetki aşılmamıştır. “Erişim yetkisinin aşılması” ile bilgisayar kullanıcısının erişim haklarının olmadığı sistemin bir bölümüne girme eylemini bir tutmak da tanımlanan terimin anlamına aykırı olmayacaktır.

(b) Kanunun yapısı da Hükümetin görüşüne karşı çıkmaktadır. Fıkra (a)(2), hukuka aykırı olarak bilgi edinmenin iki farklı yolunu belirtmektedir: Birincisi, bir kişinin “bilgisayara yetkisi olmadan erişmesi”, §1030(a)(2), ve ikincisi, bir kişinin bilgisayara “yetkili olarak” erişerek “erişim yetkisini aşması” ve ardından “elde etmeye hakkı olduğu” bilgileri elde etmesi, §§1030(a)(2), (e)(6). Van Buren, “yetkisiz” klozunun bilgisayarların kendilerini dışarıdaki bilgisayar korsanlarından koruduğunu, “erişim yetkisinin aşılması” klozunun ise sözde içerideki bilgisayar korsanlarını hedef alarak bilgisayarlardaki belirli bilgiler için tamamlayıcı koruma sağladığını iddia etmektedir. Van Buren’in yorumuna göre, her iki madde kapsamındaki sorumluluk da “bir kapının ya açık ya da kapalı olması kıstasından (*gates-up-or-down inquiry*)” kaynaklanmaktadır. Bir kişi bir bilgisayar sistemine erişebilir ya da erişemez ve sistem içindeki belirli alanlara erişebilir ya da erişemez. Bu, hükümleri tutarlı bir şekilde ele almakta ve bilgisayar bağlamında erişimin giriş olarak anlaşılmasıyla uyum sağlamaktadır. Buna karşın, Hükümet ilk “yetkisiz” ifadesini yukarıdan aşağıya bir sorgulama olarak ve ikinci “erişim yetkisini aşma” ifadesini koşullara bağlı olarak yorumlamayı önermektedir. Bu da fıkra (a)(2)’nin sistematığı ve yapısı ile tutarsız bir yorumdur. Hükümetin yorumu, kanunun neden bilgisayarın kendisine değil de bilgisayar bilgilerine uygunsuz bir saikle erişilmesini yasakladığını cevapsız bırakmaktadır.

Hükümet için bir başka yapısal sorun da şudur: §1030(a)(2) aynı zamanda hukuki sorumluluk doğurur, §1030(g), kanun “zarar” ve “kayıp” kavramlarını tanımlayarak bir hukuk davasında davacının neleri elde edebileceğini belirtir. §§1030(e)(8), (11). Her iki terim de bilgisayar verilerine veya sistemlerine yönelik teknolojik zararlara odaklanmaktadır. Bu tür hükümler bilgisayar korsanlığının olağan sonuçlarından kaçınmayı amaçlayan bir programda anlamlıdır ancak çalışanların bilgisayarlarını kullanarak izinli bir şekilde eriştikleri hassas bilgilerin “kötüye kullanımını” düzeltmek için uygun değildir.

(c) Hükümetin, emsal kararların ve yasal geçmişin kendi yorumunu desteklediği yönündeki iddiaları kolayca bertaraf edilebilir. Bu Mahkeme’nin *Musacchio v. Bir-*

leşik Devletler, 577 U. S. 237, davasındaki kararı buradaki konuyu ele almamıştır ve Mahkeme bu davadaki herhangi bir hükmü takip etmek zorunda değildir. Yasal geçmişe gelince, Hükümet 1984 tarihli Kanunun ilk halinde “erişim yetkisini aşma” ifadesinin öncülünün -“bilgisayara yetkiyle eriştikten sonra, bu erişimin sağladığı imkânı yetkinin kapsamadığı amaçlar için kullanan” herhangi bir kişiyi kapsadığını- kendi yorumunu desteklediğini iddia etmektedir. Ancak Kongre’nin CFAA’da “amaç” ile ilgili herhangi bir referansı kaldırmış olması, kanunun amaca dayalı sınırlamaları kapsayacak şekilde yorumlanmasını engellemektedir.

(d) Hükümetin “erişim yetkisini aşma” klozunu yorumlaması, sıradan bilgisayar faaliyetlerine olağanüstü düzeyde cezai yaptırım getirecektir. Örneğin, işverenler genellikle bilgisayarların ve elektronik cihazların sadece iş amaçlı kullanılabilceğini belirtmektedir. Hükümetin yorumuna göre, iş bilgisayarını kullanarak kişisel bir e-posta gönderen veya haberleri okuyan bir çalışan CFAA’yı ihlal etmiş olur. Hükümet, diğer hükümlerin soruşturulma yetkisini sınırlayabileceğini düşünmektedir, ancak suçlama uygulaması ve politikası aksini göstermektedir. Hükümetin yaklaşımı ayrıca cezai sorumluluğun değerlendirilmesine keyfilik katacaktır, çünkü Van Buren’inki gibi bir davranışın CFAA’yı ihlal edip etmediği, işverenin ihlal ettiği politikayı nasıl ifade ettiğine (“kullanım” veya “erişim” kısıtlaması olarak) bağlı olacaktır.

940 F. 3d 1192, bozuldu ve geri gönderildi.

Hâkim BARRETT; hâkim BREYER, SOTOMAYOR, KAGAN, GORSUCH ve KAVANAUGH’un katıldığı Mahkeme görüşünü sunmuştur. Hâkim THOMAS, ROBERTS, C. ve ALITO’nun katıldığı bir muhalefet şerhi sunmuştur.

AMERİKA BİRLEŞİK DEVLETLERİ YÜKSEK MAHKEMESİ

NATHAN VAN BURE V. BİRLEŞİK DEVLETLER

AMERİKA BİRLEŞİK DEVLETLERİ İSTİNAF MAHKEMESİ 11. DAİRESİNE YAPILAN TEMYİZ BAŞVURU YAZISI ÜZERİNE

Mahkeme Kararı

Sayı. 19-783.

3 Haziran 2021

Hâkim BARRETT Mahkeme’nin görüşünü sunmuştur.

Eski bir polis çavuşu olan Nathan Van Buren, para karşılığında kolluk kuvvetlerine ait bir bilgisayar veri tabanında plaka araması yapmıştır. Van Buren’in davranışı, kendisine veri tabanı bilgilerine yalnızca kolluk görevinin ifası amaçları için erişim yetkisi veren departman politikasını açıkça ihlal etmiştir. Van Buren’in aynı zamanda 1986 tarihli Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Kanununu (CFAA) da ihlal edip etmediğine karar vermeliyiz; bu kanun “bilgisayara yetkisiz olarak erişmeyi ve bu erişimi, erişenin elde etmeye veya değiştirmeye yet-

kili olmadığı bilgileri elde etmek veya değiştirmek için kullanmayı” hukuka aykırı kılmaktadır.

Ancak Van Buren bu fiili işlememiştir. Söz konusu hüküm, bilgisayar erişim yetkilerinin kapsamı dışındaki dosya, klasör veya veri tabanları gibi bilgisayarın belirli alanlarından bilgi edinenleri kapsamaktadır. Van Buren gibi, halihazırda erişebilecekleri bilgileri uygunsuz saiklerle elde edenleri kapsamaz.

I

A

1980’lerin şafağında yaşanan teknolojik gelişmeler, bilgisayarları ülke çapında okullara, ofislere ve evlere taşıdı. Ancak kamu ve özel sektörler gelişim ve yenilik için bilgisayarın gücünden yararlanırken, sözde bilgisayar korsanları bilgisayarları yasadışı amaçlar için kullanmanın yollarını aradılar. Kamuoyunun dikkatini çeken bir dizi bilgisayar korsanlığının ardından, geleneksel hırsızlık ve izinsiz giriş kanunlarının, bilgisayar sahiplerini geleneksel anlamda mülkiyetten mahrum bırakmayan siber suçları ele almak için uygun olmadığı anlaşıldı.

Kongre, birkaç Eyaletin öncülüğünü takip ederek, 1984 tarihli Kapsamlı Suç Kontrol Kanunu’nun bir parçası olarak ilk federal bilgisayar suçları kanununu yürürlüğe koyarak yanıt vermiştir. §2102(a), 98 Stat. 2190-2192. Birkaç yıl sonra Kongre, bu davanın konusu olan hükümleri içeren CFAA’yı kabul etmiştir. Kanun, “bilgisayara kasıtlı olarak yetkisiz erişim sağlayan ya da erişim yetkisini aşan” ve böylece bilgisayar verilerini elde eden herkesi cezai sorumluluğa tabi tutmaktadır. 18 U. S. C. §1030(a)(2). “Erişim yetkisini aşmak” terimini “bilgisayara yetkiyle erişmek ve bu erişimi bilgisayarda erişenin elde etmeye veya değiştirmeye yetkili olmadığı bilgileri elde etmek veya değiştirmek için kullanmak” şeklinde tanımlamaktadır. §1030(e)(6).

Başlangıçta, fıkra (a)(2)’nin öngördüğü yasak, yalnızca belirli finansal bilgilere erişimi kapsamaktaydı. O zamandan beri, “Eyaletler arası veya dış ticaret ya da iletişimde kullanılan veya bunları etkileyen” herhangi bir bilgisayardaki herhangi bir bilgiyi kapsayacak şekilde genişletilmiştir. §1030(e)(2)(B). Sonuç olarak, yasak artık - en azından - internete bağlanan tüm bilgisayarlardaki tüm veriler için geçerlidir. §§1030(a)(2)(C), (e)(2)(B).

§1030(a)(2)’yi ihlal edenler, para ve kabahat cezalarından 10 yıl kadar hapse kadar değişen cezalarla karşı karşıya kalmaktadırlar. §1030(c)(2). Ayrıca bu kişiler, CFAA ihlallerinden zarar gören veya kayba uğrayan kişilerin tazminat ve hakkaniyete uygun giderim için dava açmalarına olanak tanıyan CFAA’nın özel dava nedeni kapsamında hukuki sorumluluk riskiyle de karşı karşıyadırlar. §1030(g).

B

Bu dava Van Buren’in Georgia’da polis çavuşu olarak görev yaptığı döneme dayanmaktadır. Görevi sırasında Van Buren’in yolu Andrew Albo adında bir kişiyle kesişmiştir. Van Buren’in departmanının şef yardımcısı, Albo’nun “çok dengesiz” olduğunu düşünmüş ve departmandaki memurları onunla dikkatli bir şekilde ilgilenmeleri konusunda uyarmıştır. Bu uyarıya rağmen Van Buren, Albo ile dostane bir ilişki geliştirmişti, veyahut Van Buren

borç istemek için Albo'ya gittiğinde böyle düşünmüştü. Van Buren'in haberi olmadan Albo bu talebi gizlice kaydetmiş ve yerel şerifin ofisine götürerek Van Buren'in kendisinden nakit para için "haraç almaya" çalıştığından şikayet etmiştir.

Kayda alınan konuşma Federal Soruşturma Bürosu'na (FBI) ulaşmış ve büro Van Buren'in para için ne kadar ileri gidebileceğini görmek için bir operasyon hazırlamıştır. Adımlar basitti: Albo, Van Buren'den eyalet emniyetinin bilgisayar veri tabanında, Albo'nun yerel bir striptiz kulübünde tanıştığı bir kadına ait olduğu iddia edilen bir plakayı aramasını isteyecekti. Yasal sorunlara yabancı olmayan Albo, Van Buren'e kadının aslında gizli bir memur olmadığından emin olmak istediğini söyleyecekti. Arama karşılığında Albo, Van Buren'e yaklaşık 5.000 dolar ödeyecekti.

Her şey plana göre gitmiş, Van Buren devriye arabasındaki bilgisayarını kullanarak geçerli kimlik bilgileriyle emniyet veri tabanına erişmiştir. Veri tabanında Albo'nun verdiği plakayı aramıştır. FBI tarafından oluşturulmuş plaka girişini elde ettikten sonra Van Buren, Albo'ya paylaşacak bilgileri olduğunu söylemiştir.

Federal Hükümet daha sonra Van Buren'i, Albo için plakayı aramasının 18 U. S. C. §1030(a)(2)'nin "erişim yetkisini aşma" klozunu ihlal ettiği gerekçesiyle CFAA'yı ağır bir biçimde ihlal etmekle suçlamıştır.³ Duruşmadaki kanıtlar, Van Buren'in veritabanını "herhangi bir şahsi kullanım" olarak tanımlanan "uygunsuz bir saik" için kullanmamak üzere eğitildiğini göstermiştir. Dolayısıyla Van Buren, aramanın departman politikasını ihlal ettiğini bilmekteydi. İlâveten Hükümete göre, departman politikasının söz konusu ihlali, CFAA'yı da ihlal etmiştir. Bu görüşle tutarlı olarak Hükümet, jüriye Van Buren'in veri tabanına "görevin kapsamı dışı bir amaçla" erişmesinin, CFAA'nın "işin veya politikanın yasakladığı" bir şekilde bir bilgisayar ağını "kullanma" kavramını ihlal ettiğini söylemiştir. Jüri Van Buren'i suçlu bulmuş ve Bölge Mahkemesi Van Buren'i 18 ay hapis cezasına çarptırmıştır.

Van Buren, 11. Daire'ye istinaf başvurusunda bulunarak, "erişim yetkisini aşma" klozunun yalnızca bilgisayar erişimlerinin kapsamadığı bilgileri elde edenler için geçerli olduğunu, halihazırda sahip olduğu erişimi kötüye kullananlar için geçerli olmadığını savundu. Bazı Daireler bu maddeyi Van Buren'in yorumladığı şekilde görürken, 11. Daire daha geniş bir görüş benimseyenler arasında yer almaktadır.⁴ Kurul, kendi Daire içtihadıyla tutarlı şekilde Van Buren'in veritabanına "geçersiz bir nedenle" erişerek CFAA'yı ihlal ettiğine karar vermiştir. 940 F. 3d 1192, 1208 (2019). CFAA'nın "erişim yetkisini aşan" koluz özelindeki sorumluluğun kapsamına ilişkin yetki ayrılığını çözmek için temyiz başvurusunu kabul ettik. 590 U. S. ____ (2020).

³ Van Buren ayrıca dürüst hizmet dolandırıcılığı ile suçlanmış ve mahkûm edilmiştir. Buradaki meseleyle doğrudan ilgili olmayan ayrı bir kararda, Amerika Birleşik Devletleri İstinaf Mahkemesi On Birinci Daire, Van Buren'in dürüst hizmet dolandırıcılığı mahkûmiyetini, *McDonnell v. Birleşik Devletler*, 579 U. S. 550 (2016) kararına aykırı olduğu gerekçesiyle bozmuştur.

⁴ Krş. *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F. 3d 756 (CA6 2020); *United States v. Valle*, 807 F. 3d 508 (CA2 2015); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F. 3d 199 (CA4 2012); *United States v. Nosal*, 676 F. 3d 854 (CA9 2012) (en banc), with *United States v. Rodriguez*, 628 F. 3d 1258 (CA11 2010); *United States v. John*, 597 F. 3d 263 (CA5 2010); *International Airport Centers, L.L.C. v. Citrin*, 440 F. 3d 418 (CA7 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F. 3d 577 (CA1 2001).

II

A

1

Hem Van Buren hem de Hükümet, kendi yorumlarını desteklemek için bir dizi politika argümanı öne sürmektedir. Ancak biz her zaman olduğu gibi kanun metninden başlıyoruz. Burada, en ilgili metin “erişim yetkisini aşmak” ifadesidir; bu ifade “bilgisayara yetkiyle erişmek ve bu erişimi, bilgisayarda bulunan ve erişenin elde etmeye yetkili olmadığı bilgileri elde etmek için kullanmak” anlamına gelmektedir. §1030(e)(6).

Taraflar, Van Buren’in devriye arabasındaki bilgisayarını ve geçerli kimlik bilgilerini kullanarak veritabanına giriş yaptığında “yetkisi olan bir bilgisayara eriştiği” konusunda hemfikirler. Taraflar ayrıca Van Buren’in Albo’nun plaka kaydını ele geçirdiğinde “bilgisayardaki bilgileri elde ettiği” konusunda da hemfikirdirler. Anlaşmazlık Van Buren’in bu kaydı “elde etmeye yetkili” olup olmadığı hususuna dayanmaktadır.

“Yetki verme (*entitle*)”, “bir şeye unvan, hak vermek veya bir şey üzerinde hak iddia etmek” anlamına gelir. Taraflar Van Buren’e emniyetin bilgisayar veri tabanından plaka bilgilerini edinme hakkı verildiği, yani “edinme hakkına sahip olduğu” konusunda hemfikirdir. Ancak Van Buren, kanunun gerektirdiği gibi plaka bilgilerini “elde etme hakkını” haiz miydi?

Van Buren bu soruya olumlu cevap vermektedir. Kanunda yer verilen “bu şekilde” ifadesinin, “belirtildiği gibi” veya “açıklanan şekilde veya tarzda” anlamına gelen bir atıf (referans) terimi olarak kullanıldığını belirtmektedir. Dolayısıyla, ihtilafı olan “elde etme hakkına sahip” ifadesi, kişinin ilgili bilgiyi “belirtildiği şekilde” elde etme hakkına sahip olup olmadığını sormaktadır. Tanımlayıcı hükümde halihazırda belirtilen tek bilgi edinme şeklinin ise “[kişinin] başka bir şekilde erişim yetkisine sahip olduğu bir bilgisayar aracılığıyla” olduğu düzenlenmektedir. Bunları bir araya getiren Van Buren, “elde etme yetkisi yoktur” şeklindeki ihtilafı ifadenin açıkça kişinin erişim yetkisi olan bir bilgisayarı kullanarak elde etmesine izin verilmeyen bilgilere atıfta bulunduğunu iddia etmektedir. Bu yoruma göre, bir kişinin bir bilgisayarda depolanan bilgilere erişimi varsa - örneğin, kişinin izin verilebilir bir şekilde bilgi alabileceği Y klasöründe - o zaman bu bilgileri yasaklanmış bir amaç için alıp almadığına bakılmaksızın, bu bilgileri elde ederek CFAA’yı ihlal etmez. Ancak bilgi bunun yerine kişinin erişiminin olmadığı yasaklı X klasöründe bulunuyorsa, kişi bu bilgiyi elde ederek CFAA’yı ihlal etmiş olacaktır.

Hükümet, kanunun “bu şekilde” kelimesini referans anlamında kullandığını kabul etmekte, ancak bu ifadenin daha geniş kapsamlı olduğunu savunmaktadır. “Bu şekilde elde etme hakkına sahip değildir” ifadesini, kişinin elde ettiği belirli şekil veya koşullarda elde etmesine izin verilmeyen bilgilere atıfta bulunduğu şeklinde yorumlamaktadır. Hükümete göre, bir kişinin bilgi edinme hakkına sahip olduğu şekil veya koşullar, kişinin bilgiye erişim hakkına ilişkin “özel ve açık” olarak bildirilen sınırlamalarla tanımlanır. Hükümetin görüşüne göre, bir çalışan yasal bir amaçla, örneğin bir iş toplantısına hazırlanmak gibi, sabahları Y Klasöründen yasal olarak bilgi çekebilir. Ancak aynı bilgiyi öğleden sonra yasak-

lanmış bir amaçla, örneğin rakip bir işverene sunmak üzere bir özgeçmiş hazırlamaya yardımcı olmak gibi, Y Klasöründen bilgi çektiğinde yasal olmayan bir davranışta bulunmuş olur.

Hükümetin yorumu ilk bakışta cazip görünse de kurnazlıktan ibarettir. Hükümet, “bu şekilde” ifadesinin bir “tarz veya duruma” atıfta bulunduğunu vurgularken, aynı zamanda tanımın söz konusu tarz veya durumun halihazırda “belirtilmiş”, “ileri sürülmüş” veya “tarif edilmiş/tanımlanmış” olması gerektiği yönündeki talimatını da görmezden gelmektedir. Hükümetin yaklaşımına göre, bir kişinin davranışını yasadışı kılan durum kanunun başlarında tanımlanmamıştır. Bunun yerine, “bu şekilde” Birleşik Devletler Kanunu’nun herhangi bir yerinde, bir eyalet kanununda, özel bir anlaşmada veya başka herhangi bir yerde ortaya çıkan duruma dayalı herhangi bir sınırı kapsamaktadır. Hükümet, bu tür bir sınırın “özellikle ve açıkça” belirtilmiş, “açık” ve “yetkinin kendisinde içkin” olması gerektiğini öne sürerek yorumunu sınırlamaya çalışsa da, Hükümet bu koruyucu sınırlamalar için herhangi bir metinsel temel tanımlamamaktadır.

Van Buren’in “bu şekilde” ifadesine verdiği anlam ile ilgili açıklaması -“bu şekilde” ifadesinin §1030(e)(6) metninde daha önce belirtilen “şekil veya duruma” atıfta bulunduğu Hükümetin açıklamasından daha makul görünmektedir. “Bu şekilde” ifadesi, herhangi bir yerde belirtilen herhangi bir sınırlama ile sabit bir anlam taşıyacak ve birden çok anlamı ifade edecek nitelikte bir terim (*free-floating term that provides a hook*) değildir. “Önceki” metinde belirtilen, tanımlanabilir bir önermeye atıfta bulunur; aslında, “bu şekilde” tipik olarak “halihazırda kullanılan bir kelime veya ifadeyi” “temsil” eder, böylece tekrarlama ihtiyacını ortadan kaldırır. Sayısız federal yasa bu olağan kullanımı örneklemektedir. Van Buren ile aynı fikirdeyiz: “Elde etme hakkına sahip değildir” ifadesi, bir kişinin erişim yetkisine sahip olduğu bir bilgisayarı kullanarak elde etme hakkına sahip olmadığı bilgilere atıfta bulunacak şekilde okunmalıdır.⁵

2

Hükümetin temel karşı argümanı, Van Buren’in yorumunun “bu şekilde” kelimesini gereksiz kıldığıdır. Tanımı hatırlamak gerekirse: “bilgisayara yetkisiz olarak erişmek ve bu erişimi, bilgisayarda bulunan ve erişenin elde etmeye yetkili olmadığı bilgileri elde etmek için kullanmak.” §1030(e)(6) Hükümete göre, “bu şekilde” ifadesi, yalnızca daha önce belirtilen, kişinin yetkiyle eriştiği bir bilgisayarı kullanarak bilgi edinme yöntemine atıfta bulunuyorsa, cümleye hiçbir şey katmamaktadır. Hükümete göre Van Buren’in yorumunda önemli olan, kişinin elde etmeye hakkı olmadığı bilgileri elde etmesidir ve bu nokta “bu şekilde” ifadesi silinse dahi ortaya konabilir. Buna karşın Hükümet, “bu şekilde” ifadesinin,

⁵ Karşı görüş, bu yorumu “mülkiyet hukukunun temel ilkeleri” ve özellikle de “başka bir kişinin mülkünü kullanma hakkının duruma özgü olduğuna dair bilinen kural” ile tutarsız olduğu gerekçesiyle eleştirmektedir. (Hâkim THOMAS’ın görüşü). Ancak ortak hukuk ilkeleri, Kongre “ortak hukuk terimlerini kullanmadan ortak hukuk suçuna benzer bir suç” belirlediğinde değil, “yalnızca Kongre bir ortak hukuk terimi kullandığında” kanun metnine ithal edilmelidir. *Carter v. Birleşik Devletler*, 530 U. S. 255, 265 (2000). Genel hukuka güvenmek burada özellikle tavsiye edilmez çünkü Kongre’yi CFAA’yı yürürlüğe koymaya teşvik eden, önceden var olan hukukun bilgisayar suçlarını yakalamadaki başarısızlığıydı.

bir kişinin bilgi edinme hakkını niteleyebilecek tüm koşulları içermesi halinde değerli bir katkı sağlayacağı konusunda ısrar etmektedir. Hükümet, kendi yorumunda “bu şekilde” ifadesinin bir fonksiyon icra ettiği için, bu ifadenin gereksiz olduğuna yönelik karşı kuralın kendi yorumunun kazanacağı anlamına geldiğini iddia etmektedir. Bkz. Sudan Cumhuriyeti / Harrison, 587 U. S. ___, ___ (2019)

Ancak bu madde Hükümete yardımcı olmamaktadır çünkü Van Buren’in yorumu “bu şekilde” ifadesini gereksiz kılmamaktadır. Van Buren’in işaret ettiği gibi, “bu şekilde” ifadesi olmadan, kanun bireylerin dijital olmayan formda bilgi edinme haklarını CFAA sorumluluğuna karşı bir savunma olarak kullanmalarına izin verecektir. Bilgisayarını kullanarak öğrenme hakkına sahip olmadığı kısıtlı personel dosyalarını indiren bir kişi örneğinde böyle bir kişi, personel dosyalarına başka bir yöntemle (örneğin, insan kaynaklarından dosyaların basılı kopyalarını talep ederek) erişme hakkına sahip olsaydı, bu bilgileri “edinme hakkına” sahip olduğunu iddia edebilirdi. “Bu şekilde” ifadesi ile CFAA bu savunma teorisini geçersiz kılmaktadır. Kanun, bir kişinin bilgisayarda ne yaptığıyla ilgilidir; bilgisayar korsanının koridorda yürüyüp fiziksel bir kopyasını alabilecek olması, elektronik bir personel dosyasına izinsiz girmesini (hacklenmesini) mazur göstermez.

Bu açıklama önemlidir çünkü bu tür bir bilgilendirme hakkının geçerli olduğunun altını çizmektedir: bilgisayar kullanarak bilgiye erişme hakkı. Yukarıdaki örnekte de görüldüğü gibi bu durum sorumluluğu genişletebilir. Ancak sorumluluğu da daraltmaktadır. “Bu şekilde” ifadesi olmadan kanun, kişinin bilgi edinme hakkına ilişkin her türlü sınırlamayı içerecek şekilde okunabilir. Karşı görüşün kanunu ele alışı bunun nedenini göstermektedir.

3

Karşı görüş, Van Buren’in “bu şekilde” tanımını kabul etmekle birlikte, Hükümetin vardığı sonuca “yetkili/hak sahibi/hakkı olmak” kelimesiyle ulaşmaktadır. Muhalefet, bir kişinin bir şeyi yapmaya “hakkı” olduğunu, ancak “uygun temeller/gerekçeler” mevcut olduğunda iddia etmektedir. (Hâkim THOMAS’ın görüşü) Karşı görüş, bir kişinin bilgi edinmeye “hakkı” olup olmadığına karar vermenin, bu nedenle erişimin uygun olup olmadığına dair “duruma bağlı” bir analiz gerektirdiğini belirtmektedir. Bu değerlendirme, Hükümetinki gibi, kanunun kapsamını herhangi bir yerde ortaya çıkabilecek durum temelli herhangi bir sınırlamaya genişletecektir.

Karşı görüşün “yetkili/hak sahibi/hakkı olmak” ifadesine yaklaşımı soyut olarak iyi görünmekle birlikte bağlam içinde zayıf niteliktedir. Kanun, “erişim sahibinin elde etme hakkına sahip olmadığı bilgilerden” bahsetmemektedir. Yasa “erişenin elde etme hakkına sahip olmadığı bilgiler”den bahsetmektedir. 18 U. S. C. §1030(e)(6) O halde “yetkili/hak sahibi/hakkı olmak” ifadesi tek başına okuyucuyu erişim sahibinin bilgi edinme hakkının tüm kapsamını değerlendirmeye davet etmez. “Elde etmek için” ifadesi, okuyucuyu erişim hakkı üzerindeki belirli bir sınırlamayı dikkate almaya yönlendirmektedir: “Daha önce belirtilen şekilde” bilgi edinme hakkı. İlaveten, daha önce de açıklandığı üzere, daha önce belirtilen şekilde erişim yetkisi olan bir bilgisayarı kullanmaktır. Bu nedenle, Van Buren’in “bu şekilde” ifadesini yorumlama biçimini beğenmemekteyken karşı görüş, Hükümet gibi,

“bu şekilde” ifadesine herhangi bir sınırlayıcı işlev vermeyi reddetmektedir.⁶

Karşı görüş her iki yorumu aynı anda kabul edemez. Van Buren’in “bu şekilde” ifadesini yorumlamasını kabul etmenin sonucu “yetkili/hak sahibi olma” ifadesinin kapsamının daraltılmasıdır. Esasında, karşı görüşün verdiği örnekler de bunu zımnen kabul etmektedir: Hepsi de “bu şekilde” ifadesini atlayarak “yetkili/hak sahibi olma” ifadesine tam kapsamını vermektedir. Bunun işe yaraması için kanunu yeniden yazmak zorunda olan bir yaklaşım, Hükümetin yaklaşımından daha az ikna edicidir.

4

Hükümet, “erişim yetkisini aşmak” ifadesinin “yaygın kullanım” olarak tanımladığı anlamına dayanmaktadır. Hükümete göre, İngilizce dilini sıradan bir şekilde konuşan herhangi biri, Van Buren’in kişisel amaçları için plaka bilgilerini elde ettiğinde veri tabanına “erişim yetkisini aştığını” düşünecektir.

Eğer elimizdeki tek şey “erişim yetkisini aşmak” ifadesi olsaydı, Hükümet ve karşı görüş haklı olabilirdi. Ancak her ikisi de CFAA’nın “erişim yetkisini aşmak” ifadesinin açık tanımından yola çıkmaktadır. “Bir kanun bir terimin açık bir tanımını içerdiğinde”, “bir terimin olağan anlamından farklı olsa bile bu tanıma takip etmeliyiz.” *Tanzin v. Tanvir*, 592 U. S. ___, ___ (2020) Dolayısıyla, ilgili soru Van Buren’in erişim yetkisini aşıp aşmadığı değil, CFAA’nın bu ifadeyi tanımladığı şekilde erişim yetkisini aşıp aşmadığıdır. Ve daha önce de açıkladığımız gibi, kanuni tanım Van Buren’in yorumunu desteklemektedir.

Dahası, bu yorum, “uygun şekilde bilgilendirilmiş” bir dil kullanıcısının “erişim yetkisini aşmak” ifadesinin anlamını nasıl anlayacağını gayet iyi biçimde yansıtır. Kanunları yorumlarken, mahkemeler “teknik anlamlar” taşıyan terimlere dikkat ederler. “Erişim” bu terimlerden biridir ve bilgisayarlarla ilgili bir kanunu yorumlarken önemli olan “bilgisayım-sal anlamda” uzun süredir “yerleşik” bir anlam taşımaktadır. Bilgisayar bağlamında “erişim” terimi, bir bilgisayar “sisteminin kendisine” veya dosyalar, klasörler veya veri tabanları gibi belirli bir “bilgisayar sisteminin bir bölümüne” girme eylemini ifade eder. Dolayısıyla, “erişim yetkisinin aşılması” ile, bilgisayar kullanıcısının erişim ayrıcalıkları olmayan bir sistem bölümüne girme anlamını eşleştirmek bu anlamla tutarlıdır.⁷ Hükümet ve karşı görüşün daha geniş yorumu ne mümkün olan tek ne de en doğal yorumdur.

B

Kanunun dili Hükümetin pozisyonu için “sorun yaratırken”, “kanunun yapısına daha

⁶ Aynı sebepten ötürü, muhalefet şerhi, bizim yorumumuzun kanuna “olası her koşulda” ifadesini eklediğini iddia ederken yanılmaktadır. Bizim yorumumuz bunun yerine “bu şekilde elde etmek için” ifadesini, kanun tarafından tanımlanan izin verilen bilgi erişiminin tek “durumunu” içerecek şekilde yorumlamaktadır: Kişinin bilgisayarını kullanarak bilgiyi elde etmek.

⁷ Karşı görüş, yorumumuzun “tanımladığı terimin olağan anlamına aykırı” bir hükmü değerlendirerek “karşı kari-neyi” ihlal ettiği yönünde garip bir suçlamada bulunmaktadır. Ancak bunun gibi bir kanun “teknik bir konuyu ele aldığı anda, özel bir anlam çıkarması beklenir.” Bu ilkeyle tutarlı olarak, yorumumuz bilgisayar bağlamında “erişimin” özel anlamını takip etmektedir. Bu yorum, örneğin “köpek kelimesinin tüm atları kapsadığı kabul edilir” diyen bir tanım hükmünün aksine “erişim yetkisinin aşılması” ifadesinin anlamına “aykırı” olmaktan uzaktır.

geniş bir bakış, bize duraksamamız için daha fazla neden veriyor.” *Romag Fasteners, Inc. v. Fossil Group, Inc.*, 590 U. S. ___, ___-___ (2020)

Fıkra (a)(2)’nin “yetkisiz” ve “erişim yetkisini aşan” klozları arasındaki etkileşim bilhassa dikkat çekicidir. Bu maddeler yasadışı bilgi edinmenin iki farklı yolunu belirtmektedir. İlk olarak, bir kişi “bir bilgisayara yetkisi olmadan eriştiğinde” hükmü ihlal etmiş olur. §1030(a)(2). İkinci olarak, bir kişi bir bilgisayara “yetkiyle” erişerek ve daha sonra “elde etme hakkına sahip olmadığı” bilgileri elde ederek “erişim yetkisini aştığında” hükmü ihlal eder. §§1030(a)(2), (e)(6). Van Buren’in yorumu, hükmün parçalarını “uyumlu bir bütün haline” getirmektedir. *Roberts v. SeaLand Services, Inc.*, 566 U. S. 93, 100 (2012) Ancak Hükümetin yorumu ise böyle değildir.

Van Buren’in görüşü ile başlamak gerekirse; Van Buren’in iddiasına göre “izinsiz” ibaresi, “herhangi bir izin olmaksızın bir bilgisayara erişen” sözde dış bilgisayar korsanlarını hedef alarak bilgisayarların kendilerini korumaktadır. *LVRC Holdings LLC v. Brekka*, 581 F. 3d 1127, 1133 (CA9 2009); ayrıca bakınız *Pulte Homes, Inc. v. Laborers’ Int’l Union of North Am.*, 648 F. 3d 295, 304 (CA6 2011). Van Buren, “erişim yetkisini aşan” klozunu bilgisayarlardaki belirli bilgiler için tamamlayıcı koruma sağlamak üzere değerlendirmektedir. Van Buren’e göre bu madde, içeriden bilgisayar korsanları olarak adlandırılan, bir bilgisayara izinle erişen ancak daha sonra “bilgisayarın yetkinin kapsamadığı bir alanına girerek yetkili erişim parametrelerini aşan kişileri” hedef almaktadır. *United States v. Valle*, 807 F. 3d 508, 524 (CA2 2015).

Van Buren’in fıkra (a)(2) açıklaması, “yetkisiz” ve “erişim yetkisini aşan” hükümlerini tutarlı bir şekilde ele aldığı için yasal yapıyı anlamlandırmaktadır. Van Buren’in yorumuna göre, her iki fıkra kapsamındaki sorumluluk, bir bilgisayar sistemine ya erişilebileceği ya da erişilemeyeceği ve sistem içindeki belirli alanlara ya erişilebileceği ya da erişilemeyeceği şeklindeki kapının açık ya da kapalı olması yaklaşımından kaynaklanmaktadır.⁸ Ve her iki maddeyi de “kapının açık ya da kapalı olması” yaklaşımını benimseyecek şekilde okumak, bilgisayar bağlamında erişimin giriş olarak anlaşılmasıyla uyumludur.⁹

Hükümetin pozisyonunun başka bir yapısal sorunu daha vardır. Van Buren’in suçlandığı hüküm olan §1030(a)(2)’yi ihlal etmenin hukuki sorumluluk da doğurduğunu hatırlamak gerekir. Bkz. §1030(g). “Zarar” ve “kayıbı” tanımlayan hükümler, bir hukuk davasında davacının neleri geri alabileceğini belirtir. Kanuna göre “zarar”, “verilerin, bir programın, bir sistemin ya da bilginin bütünlüğünün ya da kullanılabilirliğinin bozulması” anlamına

⁸ Mevcut amaçlar doğrultusunda, bu sorgulamanın yalnızca erişim üzerindeki teknolojik (veya “kod tabanlı”) sınırlamalara mı yoksa bunun yerine sözleşmelerde veya ilkelere yer alan sınırlamalara da bakıp bakmadığına değinmemize gerek yoktur.

⁹ Van Buren’in açık-kapalı kapı yorumu CFAA’nın şifre ticareti yasağıyla da uyumludur. “Erişim yetkisini aşan” tanımıyla birlikte 1986 yılında yürürlüğe giren şifre kaçakçılığı hükmü, “bilgisayara yetkisiz olarak erişilebilecek herhangi bir şifre veya benzer bilginin” satışını yasaklamaktadır. §1030(a)(6). Dolayısıyla hüküm, diğer kapsam temelli kısıtlamalardan ziyade kullanıcının kimlik bilgilerinin bir bilgisayarın erişim kapısından geçmesine izin verip vermediğine bağlı olan “belirli bir yetkilendirme türünü, yani kimlik doğrulamayı” öngörmektedir. (“yetkilendirmeyi” “kimlik doğrulama aşamasını tamamlayan kullanıcıların, yetkilerine dayanarak belirli kaynaklara erişim kazandıkları veya erişimlerinin reddedildiği bir süreç” olarak tanımlamaktadır).

gelmektedir. §1030(e)(8). “Kayıp” terimi de aynı şekilde bilgisayar verilerine, programlarına, sistemlerine veya bilgi hizmetlerine verilen zararın sebep olduğu maliyetlerle ilgilidir. §1030(e)(11). Dolayısıyla, “zarar” ve “kayıp” terimlerinin tanımları, yetkisiz kullanıcıların bilgisayar sistemleri ve veriler üzerinde neden olduğu teknolojik zararlara –örneğin dosyaların bozulması- odaklanmaktadır. “Zarar” ve “kayıp” bu şekilde sınırlandırılması, “bilgisayar korsanlığının tipik sonuçlarını önlemeyi amaçlayan” bir programda anlamlıdır. Bununla birlikte, terimin tanımları, çalışanların bilgisayarlarını kullanarak izin verilebilir bir şekilde erişebilecekleri hassas bilgilerin “kötüye kullanımını” gidermek için uygun değildir. Bu ayrıma Van Buren’in durumu örnek teşkil eder: Plakayı sorgulama, verilerin “bütünlüğünü veya kullanılabilirliğini” bozmamış veya veritabanı sisteminin kendisine başka bir şekilde zarar vermemiştir.

C

Metinden ve yapısından hareket eden Hükümet, içtihatların ve yasal geçmişin kendi yorumunu desteklediğini iddia etmektedir. Bu argümanlar kolayca bertaraf edilebilir.

Emsal kararlara gelince, Hükümet bu Mahkemenin *Musacchio v. Birleşik Devletler*, 577 U. S. 237 (2016) kararının kendi yorumunu desteklediğini ileri sürmektedir. Söz konusu kararda Mahkeme, bilgilendirme hatası (*instructional error*) için inceleme standardını ele alırken, §1030(a)(2)’yi “(1) yetkisiz erişim elde etmeyi; ve (2) yetkiyle erişim elde etmeyi ancak daha sonra bu erişimi uygunsuz şekilde kullanmayı” yasaklamak olarak tanımlamıştır. Kanunun bu şekilde özetlenmesi Hükümet için pek bir şey ifade etmemektedir. İlk olarak, Musacchio “şu anda söz konusu olan noktayı” ele almamıştır ve Hükümetin lehine çözmemiştir, bu nedenle davadaki herhangi bir görüşü “takip etmek zorunda değiliz”. *Central Va. Community College v. Katz*, 546 U. S. 356, 363 (2006). Ancak her halükarda, Van Buren’in yorumu, Hükümetin yorumu kadar, “kişinin erişimini uygunsuz bir şekilde kullanmayı” içermektedir. Bir kişinin bilgisayar erişiminin sağladığı fırsatı bilgisayar içinden yasaklanmış bilgileri elde etmek için kullanması açıkça “uygunsuzdur”.

Kanuni geçmişe gelince, Hükümet orijinal 1984 Kanununun mevcut versiyona ilişkin yorumunu desteklediğini iddia etmektedir. “Erişim yetkisini aşma” maddesinin bir öncülü olarak, 1984 Kanunu, “bilgisayara yetkili olarak eriştikten sonra, bu erişimin sağladığı imkânı bu yetkinin kapsamadığı amaçlar için kullanan” herhangi bir kişiyi kapsamış ve böylece içeriden birinin bilgisayar erişiminin amacına açıkça atıfta bulunmuştur. 18 U.S.C. §1030(a)(2)

Hükümete göre bu durum, “erişim yetkisini aşma” tanımını yaparken amaçtan bahsetmeyen değiştirilmiş CFAA’nın, Van Buren gibi bilgisayar erişimini yetkisiz bir amaç için kullanan içeriden kişileri de kapsadığını doğrulamaktadır.¹⁰ Hükümetin argümanı işleri tam

¹⁰ Hükümet Kongre’nin bu değişikliği §1030(a)(2)’nin “sadece dilini netleştirmek için” yaptığında ısrar ederken, karşı görüş farklı bir düşünceye sahiptir. Muhalefet şerhine göre, 1986 değişikliği aslında hükmü “genişleterek” sadece amaca dayalı olanları değil bilgisayar erişimine getirilen “zaman ve şekil” kısıtlamalarını da kapsar hale getirmiştir. Karşı görüşün Kongre’nin §1030(a)(2)’nin “amaç” referansını neden kaldırdığına dair farklı açıklamaları, “erişim yetkisini aşma” tanımının duruma özgü bir yaklaşımı desteklediğini kabul etmeyi gerektirmektedir. Karşı görüşün önermesini daha önce tartışılan metinsel ve yapısal nedenlerle reddediyoruz.

olarak tersine çevirmektedir. “Kongre mevzuatı değiştirdiğinde, mahkemeler değişikliğin gerçek ve önemli bir etkiye sahip olmasını amaçladığını varsaymalıdır.” *Ross v. Blake*, 578 U. S. 632, 641-642 (2016). Kongre’nin kanunda amaca yapılan atfı kaldırmayı tercih etmesi, kanunun “tam da bu kavramı kapsayacak şekilde” okunmasını engellemektedir. Dolayısıyla, yasal geçmiş Hükümetin pozisyonuna yardımcı olmaktan ziyade zarar vermektedir.

III

Üstüne üstlük, Hükümetin kanun yorumu, sıradan bilgisayar faaliyetine olağanüstü ölçüde cezai yaptırımlar getirecektir. Van Buren, Hükümetin yorumunun geniş kapsamlı sonuçlarını sanık lehine yorum (lenity) kuralını veya anayasal kaçınmayı tetikleyen bir durum olarak çerçevelemektedir. Biz böyle görmüyoruz: Metin, bağlam ve yapı, Van Buren’in yorumunu desteklediğinden, bu kanunların hiçbiri devrede değildir. Yine de ortaya çıkan sonuç, Hükümetin yorumunun mantıksızlığının altını çizmektedir. Bu, “zaten kremayla kaplanmış olan bir pastanın üzerindeki ekstra krema”dır. *Yates v. United States*, 574 U. S. 528, 557 (2015) (Hâkim KAGAN, karşı görüş).

Eğer “erişim yetkisini aşma” klozu bilgisayar kullanım politikasının her ihlalini suç sayıyorsa, o zaman kanunlara uyan milyonlarca vatandaş suçlu olacaktır. İşyerini ele alacak olursak, işverenler genellikle bilgisayarların ve elektronik cihazların sadece iş amaçlı kullanılabileceğini belirtirler. Dolayısıyla, Hükümetin kanunu yorumlamasına göre, iş bilgisayarını kullanarak kişisel bir e-posta gönderen veya haberleri okuyan bir çalışan, CFAA’yı ihlal etmiş olur. Ya da interneti düşünmek gerekirse “korunan bilgisayarlardan” “bilgi” sağlayan birçok web sitesi, hizmet ve veri tabanı, §1030(a)(2)(C), bir kullanıcının erişimine yalnızca belirli hizmet koşullarına uymayı kabul etmesi halinde izin vermektedir. “Erişim yetkisini aşma” klozu işverenlerin bilgisayarlarındaki duruma dayalı erişim kısıtlamalarının ihlallerini kapsıyorsa, web sitesi sağlayıcılarının bilgisayarlarındaki bu tür kısıtlamaların ihlallerini de neden kapsamadığını anlamak zor olacaktır. Gerçekten de çok sayıda tarafsız müdahil (*amici*), Hükümetin fıkra (a) (2)’ye dair yorumunun bir çevrimiçi randevu profilini süslemekten Facebook’ta takma ad kullanmaya kadar her şeyi suç haline getireceğini açıklamaktadır.¹¹

Bu noktalara cevaben Hükümet, kanundaki diğer terimlerin, özellikle de “yetkilendirme” ve “kullanma” terimlerinin, kovuşturma yetkisini “pekala” kamufle etmeye hizmet edebileceğini ileri sürmektedir. (“araçsal” kullanım; “bireyselleştirilmiş” ve “oldukça spesifik” yetkilendirme). Yine de Hükümet bu tür sınırlamaları onaylamaktan uzak durmaktadır. (“yetkilendirme” kavramı “mantıksal olarak geçerli olmayabilir”); (“kullanım”, “genellikle daha geniş bir tanıma sahip olsa da” daha “sınırlı” bir şekilde okunabilir); (mens rea gerekliliği bazı durumlarda sorumluluğu “engellenebilir”). Van Buren, kanunu bu tür sınırlamalar içerecek şekilde okuduğu herhangi bir önceki örneğe de atıfta bulunmuyor, aksine, okumadığı örneklere atıfta bulunuyor. (Hükümetin “oldukça önemsiz zarara” neden olan hizmet

¹¹ Bakınız tarafsız müdahil sıfatıyla Orin Kerr ‘in raporu 10-11; Tarafsız müdahil sıfatıyla Technology Companies’in raporu 6, n. 3, 11; ayrıca bakınız tarafsız müdahil sıfatıyla Reporters Committee for the Freedom of the Press ve diğerleri’nin raporu 10-13 (gazetecilik faaliyetleri); Tarafsız müdahil sıfatıyla Kyratso Karahalios ve diğerleri’nin raporu 11-17 (çevrimiçi sivil haklar test ve araştırmaları).

şartları ihlallerine dayalı bir CFAA kovuşturması başlatabileceğini belirten Adalet Bakanlığı ifadesini tartışırken). Hükümetin mevcut CFAA suçlama politikası, Van Buren'in endişelerinin neden "varsayımsal" olmaktan uzak olduğunu göstermektedir: Politika, "sanığın yalnızca bir internet hizmet sağlayıcısı veya web sitesi ile yapılan bir sözleşmede veya hizmet şartında yer alan bir erişim kısıtlamasını ihlal ederek erişim yetkisini aşması halinde" federal kovuşturmanın "garanti edilmeyebileceğini" - yasaklanmayacağını değil - talimat vermektedir.¹² Hükümet, kasıt şartının bir başka emniyet supabı işlevi gördüğünde ısrar etse de bu şart, bilgisayarlarını kasıtlı olarak "işlerinin veya politikalarının yasakladığı" bir şekilde, örneğin spor skorlarını kontrol ederek veya işyerinde fatura ödeyerek kullananlar için hiçbir şey yapmayacaktır.

Son bir gözlem: Hükümetin yaklaşımı cezai sorumluluğun değerlendirilmesine keyfilik katacaktır. Hükümet, olması gerektiği gibi, "izin verilen erişimi aşan" hükmün yalnızca yasa dışı bilgi "erişimini" yasakladığını, sonraki bilgi "kötüye kullanımını" yasaklamadığını kabul etmektedir (kanun "sonraki bilgi kötüye kullanımını" kapsamamaktadır). Ancak Hükümetin okumasına göre bu ikisi arasındaki çizgi ince olabilir. Erişim üzerindeki amaca dayalı sınırlamalar genellikle bilginin kötüye kullanımına yönelik olarak tasarlandığından, erişim ya da kullanım kısıtlamaları olarak ifade edilebilirler. Örneğin, bir polis departmanı gizli bir veritabanının görevin ifası dışı bir amaçla kullanılmasını yasaklayabilirken (erişim kısıtlaması), bir diğeri veritabanındaki bilgilerin görevin ifası dışı bir amaçla kullanılmasını yasaklayabilir (kullanım kısıtlaması). Van Buren'inki gibi davranışlar her iki şekilde de nitelendirilebilir ve bir işveren ikisi arasında pek bir fark görmeyebilir. Ancak Hükümetin yorumuna göre, bu davranış ancak işverenin politikayı bir erişim kısıtlaması olarak ifade etmesi halinde CFAA'yı ihlal edecektir. Özel tarafların taslak hazırlama uygulamaları tarafından kontrol edilen ince bir ayrıma bu kadar çok dayanan bir yorumun en makul olan olduğunu ileri sürmek zordur.

IV

Özetle, bir kişi bilgisayara yetkiyle eriştiğinde ancak daha sonra bilgisayarın belirli alanlarında - dosyalar, klasörler veya veritabanları gibi - kendisine yasak olan bilgileri elde ettiğinde "erişim yetkisini aşmış" olur. Taraflar Van Buren'in kolluk kuvvetleri veri tabanı sistemine yetkiyle eriştiği konusunda hemfikirdir. Tek sorun Van Buren'in plaka bilgilerini almak için sistemi kullanıp kullanamayacağıdır. Her iki taraf da bunu yapabileceği konusunda hemfikirdir. Buna göre Van Buren, veri tabanından uygunsuz bir amaçla bilgi elde etmiş olsa bile, CFAA'nın bu ifadeyi tanımladığı gibi veri tabanına "erişimde yetkiyi aşmamıştır". Bu nedenle, On Birinci Daire'nin aksi yöndeki kararını bozuyor ve davayı bu görüşle tutarlı yeni işlemler için geri gönderiyoruz.

Bu şekilde hükmedilmiştir.

¹² Hükümet, "tarihsel olarak" Van Buren'in korktuğu sıradan ihlalleri değil, sadece Van Buren'inki gibi "temel davranışları" kovuşturduğunu iddia etse de Van Buren ve avukatlarının aktardığı aksi örnekler bu güvenceden şüphe duymak için bir neden vermektedir.

Hâkim THOMAS'ın Muhalefet Şerhi

AMERİKA BİRLEŞİK DEVLETLERİ YÜKSEK MAHKEMESİ
BAŞVURUCU NATHAN VAN BUREN V. BİRLEŞİK DEVLETLER
AMERİKA BİRLEŞİK DEVLETLERİ İSTİNAF MAHKEMESİ 11.
DAİRESİNE YAPILAN TEMYİZ BAŞVURU YAZISI ÜZERİNE

Sayı. 19-783.

3 Haziran 2021

Baş hâkimin ve hâkim ALITO'nun da katıldığı Hâkim THOMAS'ın muhalefet şerhi.

Hem müşterek hukuk hem de yazılı hukuk, başkalarına ait bir mülkü kullanırken rıza kapsamını aşanları uzun süredir cezalandırmaktadır. Örneğin bir vale, park etmek için bir kişinin arabasını alabilir, ancak onu gezintiye çıkaramaz. Bilgisayar Dolandırıcılığı ve Suistimali Kanunu bu ilkeyi bilgisayar ve bilgileri de kapsayacak şekilde genişletmektedir. Kanun, başka bir kişiye ait bir bilgisayarı kullanırken rıza kapsamının aşılmasını yasaklamaktadır. Özellikle, bir bilgisayara “kasıtlı olarak yetkisi olmadan erişen veya yetkisini aşan ve böylece o bilgisayardan bilgi elde eden” herkesi cezalandırır. 18 U. S. C. §1030(a)(2).

Bir polis memuru olarak Nathan Van Buren'in bir devlet veri tabanından plaka bilgilerini alma izni sadece görevinin ifası amaçları için bulunmaktaydı. Van Buren, birkaç bin dolar karşılığında veri tabanını potansiyel bir gizli soruşturmacının maskesini düşürmek için kullandığında bu sınırlamayı göz ardı etmiştir.

Buradaki soru açıktır: İngilizce dilinin sıradan bir okuyucusu, Van Buren'in veri tabanını açıkça yasaklanmış koşullarda kullanırken veri tabanına “izin verilen erişimi aştığını” anlar mıydı? Benim görüşüme göre cevap evettir. Bu verileri elde etmesine izin veren gerekli ön koşul mevcut değildi.

Mahkeme, “erişim yetkisini aşan” ifadesinin Van Buren'in davranışını kolayca kapsadığına itiraz etmemektedir. Bunun yerine, kanunun bu ifade için bir tanım içerdiğini ve “bir terimin olağan anlamından farklı olsa bile bu tanıma uymamız gerektiğini” belirtmektedir. *Tanzin v. Tanvir*, 592 U. S. ___, ___ (2020) Bununla birlikte, çoğunluk görüşü için sorun, metnin, mülkiyet hukukunun olağan ilkelerinin ve kanuni tarihin, tanımlayıcı hükmün tanımladığı terimle oldukça tutarlı olduğunu ortaya koymasıdır.

I

A

Kanun, “yetkiyi aşan erişimi” “bilgisayara yetkiyle erişmek ve bu erişimi bilgisayarda erişiminin elde etmeye veya değiştirmeye yetkili olmadığı bilgileri elde etmek veya değiştirmek için kullanmak” olarak tanımlamaktadır. §1030(e)(6). Bu istinaf başvurusunun amaçları doğrultusunda, Van Buren'in bir devlet veri tabanına giriş yapma yetkisine sahip olduğu ve girişini bu veri tabanından sahte plaka bilgileri elde etmek için kullandığı kabul edilmek-

tedir. Dolayısıyla, bu davanın Van Buren'in sahte plaka bilgilerini "elde etmeye yetkili" olup olmadığına bağlı olduğu konusunda çoğunluğa katılıyorum. Ayrıca "bu şekilde" ifadesinin Van Buren'in bu bilgileri tanımda daha önce belirtilen yollarla elde etme hakkına sahip olup olmadığını sorduğuna da katılıyorum: (1) bir bilgisayara yetkiyle erişmek ve (2) bu erişimi bilgisayardaki bilgileri elde etmek için kullanmak. Başka bir deyişle, Van Buren'in davranışı ancak veri tabanına erişim yetkisini kullanarak söz konusu plaka bilgisini elde etme hakkına sahip olması halinde yasaldır.

Ancak Van Buren'in davranışı yasal değildi. Bir kişinin bir şeyi yapma yetkisi yalnızca bu şeyi yapma "hakkına" sahip olduğunda geçerlidir. Van Buren'in belirli plaka bilgilerini elde etmek için bilgisayarı kullanmaya hiçbir zaman "hakkı" olmamıştır. Herkes onun bu bilgileri geçerli bir görevin ifası amacı için değil, kişisel kazanç için elde ettiğini kabul etmektedir. Ve kanunu uygulamaya yönelik geçerli bir amacı olmaksızın, bu bilgileri elde etmek için bilgisayarı kullanması yasaktı.

B

Çoğunluk, bu tanımlayıcı hükmün alternatif bir okumasını önermektedir: Bir kişi en az bir durumda bilgi edinmek için bilgisayar kullanma hakkına sahip olduğu sürece, kişi verileri bu durum dışında elde etse bile bu kanun uygulanmaz. Aslında çoğunluk, kanunu yalnızca bir kişinin "herhangi bir olası koşul altında" bilgi edinme hakkına sahip olmadığı durumlarda geçerli olacak şekilde okumaktadır. Bu yorum bir dizi nedenden dolayı hatalıdır.

I

Her şeyden önce bu yorum, metnin düz anlamına aykırıdır. Yetkiler zorunlu olarak koşullara bağlıdır; bir kişi ancak "uygun gerekçeler" veya olaylar mevcut olduğunda bir şey yapma hakkına sahiptir. "Bu şekilde" ifadesine odaklanan çoğunluk, "yetkili/hak sahibi olma" terimini analiz etmekten büyük ölçüde kaçınarak, başlangıçta tek bir cümleyle Van Buren'in bu plaka bilgilerini alma hakkına sahip olduğu sonucuna varmıştır. Ancak "yetkili/hak sahibi olma" ifadesinin düz anlamı, tam tersi bir sonuca zorlamaktadır. Van Buren'in görevin ifası amacı olmadığı için, "uygun gerekçeler" mevcut değildi. Bunu yaptığında verileri elde etme hakkına da sahip değildi.

Birkaç gerçek hayat senaryosu bu noktayı açıklamaktadır. Bir yangın durumunda alarmı çalıştırma hakkına sahip olan bir çalışan, hazırlıksız olduğu bir toplantıyı ertelemek gibi başka bir amaçla alarmı çalıştırma hakkına sahip değildir. Bir restoran müşterisinden araba alan bir vale - §1030(e)(6)'daki ifadenin lafzına başvurursak – "arabaya erişme" ve arabayı park etmek ve geri almak için "bu erişimi kullanma" "yetkisine/hakkına" sahiptir. Ancak araçla gezmek için "bu erişimi kullanma" "hakkına" sahip değildir. Bkz. örneğin, Ind. Code §35-43-4-3 (2020) ("mülk bir motorlu araçsa" "başkasının mülkü üzerinde bilerek veya kasıtlı olarak yetkisiz kontrol uygulamak" için suç teşkil eden cezai hal); *In re Clayton*, 778 N. E. 2d 404, 405 (Ind. 2002) (bu kanunu, aksi takdirde erişim hakkı olan bir kişinin mülkünün kötüye kullanılmasını kapsayacak şekilde yorumlayarak). Bu kanuna daha yakın bir örnek vermek gerekirse, bir araba kiralama şirketi çalışanı, kiralık bir arabanın GPS konum geçmişini gösteren "bir bilgisayara erişme" ve çalıntı ihbarı yapılması halinde arabanın yerini

tespit etmek için “bu erişimi kullanma” “hakkına” sahip olabilir. Ancak eski kız arkadaşını takip etmek için “bu erişimi kullanmaya” “hakkı olduğunu” söylemek doğal olmayacaktır.

Çoğunluk gerçek bir yanıt vermemektedir. “Yetkili/Hak sahibi” ifadesinin “bu şekilde” ile değiştirildiğini ve bu nedenle mahkemelerin bir kişinin bilgi edinmek için bilgisayar kullanma hakkına sahip olup olmadığını değerlendirmesi gerektiğini belirtmektedir. Ancak bir kişi bilgi edinme hakkına sahip değilse, bu zorunlu olarak “bilgisayar kullanarak bilgiye erişme hakkı” olmadığı sonucunu doğurur. Van Buren’in bu bilgiyi elde etmeye tamamen yetkili olduğu çünkü bir yetkiyi sağlamak için gerekli olan ön koşul –bir kolluk kuvveti amacı- mevcut değildi.

2

İlaveten, çoğunluğun yorumu mülkiyet hukukunun temel ilkeleriyle çelişmektedir. Şimdiye kadar, bir bilgisayarda bulunan bilgilerin “mülk” olduğu iyice yerleşmiştir. Örneğin, bilgisayarda depolanan bir filmin fikri mülkiyet olduğundan kimsenin şüphesi yoktur. Federal ve eyalet kanunları genel olarak “mülkiyeti” bilgisayar verilerini içerecek şekilde tanımlamaktadır. Örneğin, 12 U. S. C. §5433; N. Y. Penal Law Ann. §155.00 (Batı 2010). Ve çoğunluk dahi bu kanunun mülkiyeti korumak için tasarlandığını kabul etmektedir. Yine de yorumunu, başka bir kişinin mülkünü kullanma hakkının duruma özgü olduğuna dair bilinen kuralla bağdaştıramamaktadır.

İzinsiz giriş örneğinde, bir kişi araziye girme yetkisine sahipse ve bu girişi bir amaç için kullanma hakkına sahipse ancak bunu başka bir amaç için yaparsa, izinsiz girmiş olur. İkinci Haksız Fiil Düzenlemesinin açıkladığı üzere, “araziye girmek için şartlı veya kısıtlı bir rıza, yalnızca şarta veya kısıtlamaya uyulduğu sürece bunu yapmak için bir hak yaratır.” §168, p. 311 (1964). Söz konusu düzenleme yararlı bir örnek içermektedir:

“3. A, komşusu B’ye A’nın arazisine girmesi ve B’nin kendi kullanımı için A’nın kaynağından su çekmesi için izin verir. A, C’nin A’nın arazisine girmesine ve kaynaktan su çekmesine özellikle izin vermemiştir. C’nin kışkırtmasıyla B, A’nın arazisine girer ve C için kaynaktan su çeker. B’nin girişi haneye tecavüzdür.”

Arazi için doğru olan bilgisayar bağlamında da doğrudur; bir şirket bir çalışanına bilgisayarı belirli bir amaç için kullanma izni verirse, çalışanın bilgisayarı başka amaçlar için kullanma yetkisi yoktur.

Hırsızlık suçundaki yaygın anlayışı da göz önünde bulunduralım. Bir mülkü sınırlı bir amaç için elinde bulundurma yetkisine sahip olan bir kişi, bu mülk üzerinde “yasadışı kontrol uyguladığı” anda hırsızlık suçunu işlemiş olur; bu da “rıza veya yetki aşıldığında” gerçekleşir. ALI, Model Ceza Kanunu §223.2(1), s. 162, 168 (1980). Yine §1030(e)(6)’daki lafza göre, bir polis memuru departmanın banka hesabına “erişim” yetkisine sahip olabilir ve bu erişimi kolluk harcamalarını karşılamak için “kullanabilir”, ancak yine de bu erişimi kendi cebini doldurmak için “kullanırsa” zimmete para geçirmekten suçludur. Başka koşullar altında hesaptan para “alma hakkına” sahip olduğu için aklanmayacaktır.

Ya da kefaleti ele aldığımızda bir kefil, “kefil olunan şeyi kullanma yetkisi olmamasına rağmen onu kullandığında veya belirli bir şekilde kullanma yetkisi olmasına rağmen onu

farklı bir şekilde kullandığında” -birçok yargı alanında suç olarak kabul edilen- hakkı olmadığı mülkiyete tecavüz suçu (*conversion*) işlemiş olur. 8 C. J. S., Bailments §43, s. 480-481 (2017) Bir bilgisayar teknisyeni, çöken bir sabit diskteki verileri kurtarmak için bir ünlünün bilgisayarına erişme yetkisine sahip olabilir, ancak erişimini bu bilgisayarda depolanan fotoğrafları kopyalamak ve basına sızdırmak için kullanamaz.

Çoğunluk, yorumunu bu bilinen ilkeyle bağdaştırmak için hiçbir girişimde bulunmamaktadır. Bunun yerine, Kongre’nin bu kanuna herhangi bir müşterek hukuk terimi dahil etmediğini belirterek bu bağlamı ortadan kaldırmaktadır. Ancak kanunda diğer mülkiyet bağlamında yaygın olarak kullanılan “aşma” ve “yetki” gibi kelimeler kullanılmaktadır. Ve çoğunluk, Kongre’nin etmesi gerektiğini düşündüğü herhangi belirli mülkiyet hukuku terimlerini asla tanımlamamaktadır.

Çoğunluk daha sonra, mülkiyet hukukunun önceden var olan kavramlarına güvenmenin “tavsiye edilmez” olduğunu, çünkü Kongre’nin bu kanunu “önceden var olan yasanın bilgisayar suçlarını yakalamadaki başarısızlığı” ışığında çıkardığını söylüyor. Ancak önceden var olan yasanın yetersiz görülmesinin nedenleri çoğunluğun görüşünü zayıflatmaktadır. Birincisi, eyalet kanunları Van Buren’inki gibi davranışları kapsamak için kullanılıyordu, ancak bunu yapmak “önemli ölçüde yaratıcılık gerektiriyordu”, çünkü bu yasalar tipik olarak ya “fiziksel” girişi (bilgisayarlara pek uymuyordu) ya da mağduru “mülkünden mahrum bırakmayı” (bir kişinin verileri “yalnızca kopyaladığı” veya yasak “kişisel kullanımlar” yaptığı durumlarda pek uymuyordu) gerektiriyordu. İkinci olarak, “kapsamı daha sınırlı” olan federal kanunlar için uyum daha da garipti. Kongre bu kanunu, mülkiyeti kullanma hakkının duruma özgü olduğuna dair yerleşik ilkeyi ortadan kaldırmak için değil, bunun yerine mahrumiyet ve fiziksel giriş gerekliliklerini ortadan kaldırmak için çıkarmıştır.

Yorumunu mülkiyet hukukunun yerleşik ilkeleriyle bağdaştıramayan çoğunluk, yorumunun kanundaki “bir bilgisayara yetkisiz erişimi” yasaklayan ayrı bir maddeyle daha uyumlu olduğunu iddia etmektedir. §1030(a)(2). Çoğunluğun anlatımına göre, bu madde “bilgisayar sistemine ya erişilebilir ya da erişilemez” şeklinde kapının ya açık ya da kapalı olduğu yönünde bir sorgulama gerektirmektedir, dolayısıyla aynı cümledeki “erişim yetkisini aşan” klozunu da aynı yaklaşımı içerecek şekilde okumak mantıklıdır.

İki maddenin uyumlu bir şekilde okunması gerektiğine katılıyorum, ancak kapıların tek bir durumda açık olduğuna inanmak için hiçbir neden yoktur; bu kapıların süresiz olarak açık kalması gerektiği anlamını taşımaz. Hassas savunma bilgileriyle çalışan birisi, ofisten uzaktayken işvereni tarafından kendisine verilen dizüstü bilgisayarda oturum açma yetkisine sahip olabilir. Ancak işvereni ağ bağlantılarına güvenilemeyecek bir ülkeye seyahat ederken oturum açmaması talimatını verirse, yine de oturum açarsa bilgisayara yetkisi olmadan erişmiş olur. Her iki madde için de kapıların açık mı yoksa kapalı mı olduğunu anlamak için kapıların hareket etmesine neden olan koşulların göz önünde bulundurulması gerekir.

Aslında, benim okumam her iki maddeyi de mülkiyet hukukunun yerleşik kavramlarıyla uyumlu hale getirmektedir. Mülkiyet hukuku genellikle hem hukuka aykırı girişe hem de girişten sonra hukuka aykırı kullanıma karşı koruma sağlar. Örneğin, İkinci Haksız Fiil Düzenlemesi §214, Comment e, at 408-409; 8 C. J. S., Bailments §43, at 480-481. Aynı

durum burada da geçerlidir. Polis departmanı, memurların uygunsuz bir amaçla giriş yapmasını yasaklayarak bilgileri koruyabilir, ancak bir memurun vardiyasının başında uygun bir niyetle giriş yapması ve saatler sonra hala sistemdeyken, ödeme karşılığında plaka araması yapması durumunda bu pek işe yaramayacaktır. Kongre, hem “yetkisiz” hem de “erişim yetkisini aşan” klozlarını dâhil ederek, uygunsuz girişin yanı sıra uygun girişten sonra kötüye kullanıma karşı da koruma sağlamıştır.

3

Çoğunluğun yorumu -suçluluğun bir yasağın tek bir istisnası olup olmadığına bağlı olduğu- aynı zamanda garip sonuçlara yol açmaktadır. Bu yoruma göre, müşterilerin satın alma geçmişini elde etmesi yasak olan bir kredi kartı şirketi çalışanı, işvereni kendisine bir hesap, olası dolandırıcılık faaliyeti için işaretlendiğinde satın alma geçmişi verilerini elde edebileceğini ve aktarabileceğini söylemediği sürece, eski karısı hakkında bu verileri elde ettiğinde Kanunu ihlal etmiş olur. Aynı durum, yeniden çalışmaya başlamadan dakikalar önce bilgisayarındaki tüm dosyaları silen kişi için de geçerlidir. *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F. 3d 756, 758 (CA6 2020). Bir çalışan, varsayımsal bir durumda her bir dosyayı elde edebildiği veya değiştirebildiği sürece, dokunulmazdır. Ancak, bir tur solitaire oynayan kişi, dikkatinin dağılmasından endişe eden işvereni Windows’taki “oyunlar” klasörüne erişimi kategorik olarak yasakladığında, çoğunluğun yorumuna göre suçludur. Tek bir istisnanın varlığı ya da yokluğu üzerine “bu kadar çok bel bağlamak” garip bir yorumdur.

Çoğunluğun yorumu, kanundaki diğer maddelere uygulandığında özellikle gariptir. Bölüm 1030(a)(1), “elde edilen bilgilerin Birleşik Devletler’in zararına veya herhangi bir yabancı ülkenin yararına kullanılabileceğine inanmak için bir nedene sahip olarak kısıtlı verileri” elde etmek için “erişim yetkisini aşmayı” ve bu verileri saklamayı veya dağıtmayı yasaklamaktadır. “Kısıtlı veriler” terimi, “(1) atom silahlarının tasarımı, üretimi veya kullanımına ilişkin tüm verileri” içerecek şekilde tanımlanmıştır. 42 U. S. C. §2014(y). Çoğunluğun yorumuna göre, bir bilim adamı, en azından bir durumda atom silahlarının planlarını elde edebildiği sürece, bu verileri düşman bir ulusun nükleer cephanelik kurmasına yardımcı olmak gibi uygunsuz bir amaçla elde etmesi halinde dokunulmaz olacaktır. 1984’ten beri büyük ölçüde benzer biçimde yürürlükte olan bu hükmün, çoğunluğun yorumuna göre ne gibi bir gücü olduğunu anlamak zordur.

4

Hangi yorumun kanuna daha iyi uyduğu konusunda herhangi bir şüphe kalırsa, tanımlanan terim bunu çözecektir. Bir tanımın birden fazla yoruma açık olduğu durumlarda, tanımlanan terimin açık anlamına en iyi uyan yorum normal olarak kontrol edilir. Bkz. örneğin, *Bond v. Birleşik Devletler*, 572 U. S. 844, 861 (2014) (“tanımlanmış bir terimin olağan anlamı” dikkate alınır); (Hâkim Scalia, karara katılmaktadır) (mahkemeler “tanımladığı bir belirsizliği çözmek amacıyla tanımlanan terimin olağan anlamını kullanabilir”). Çünkü bir hükmün, tanımladığı terimin olağan anlamına aykırı olarak okunmasına karşı “bir karine vardır”. (“Tanımın anlamı neredeyse her zaman tanımlanan kelimenin olağan anlamıyla yakından ilişkilidir”).

Çoğunluk bunun yerine, tanımda varsayılan belirsizliği tanımlanan teriminin anlamına aykırı bir şekilde çözmektedir. Tanımın “tercih edilen” bir yorumunu benimsemekte ve ardından tanımlanan terimin bu “tercih edilen” görüşle “tutarlı” bir şekilde yorumlanıp yorumlanamayacağını sormaktadır. Ancak “Kongre’nin bir terimi olağan ve geleneksel anlamına aykırı bir şekilde tanımladığına inanmamızı sağlamak için en güçlü kanıtlar gerekir.” *Babbitt v. Sweet Home Chapter, Communities for Great Ore.*, 515 U. S. 687, 719 (1995) (Hâkim Scalia, karşı görüşte). Çoğunluk böyle bir kanıt tanımlamamaktadır. Çoğunluğun söylediği en fazla şey, benim “erişim yetkisini aşan” ifadesini yorumlamamın “zorunlu olarak” en iyisi olmadığıdır çünkü “erişim” teknik bir anlama sahip olabilir: Bilgisayar sisteme veya bilgisayar sisteminin bir bölümüne girmek. Ancak “erişim” ne anlama gelirse gelsin, “yetki” – “hak” gibi- duruma bağlıdır. Çoğunluğun “erişim” yorumu bu noktayı doğrulamaktadır. Çoğunluğun atıfta bulunduğu tanımlar sadece girişe değil, belirli verileri elde etmek için girişi kullanmaya atıfta bulunmaktadır. Bu, bir kişinin bilgisayara girdikten sonra bilgisayarı “kullanmasını” düzenleyen buradaki tanımla uyumludur. §1030(e)(6). Burada, mülkiyet hukukunun diğer bağlamlarında olduğu gibi, bir kişinin mülke erişimini kullanma yetkisi duruma bağlıdır. Çoğunluğun “erişim” terimine odaklanması -“yetki” ve “hak” terimlerinin pahasına- argümanına yardımcı olmak yerine zarar vermektedir.

II

Metnin ve mülkiyet hukukunun yerleşik kavramlarının açıkça ortaya koyduğu şeyi, yasal tarih de pekiştirmektedir. Bu Kanunun orijinal metni, bilgisayara yetkilendirme ile erişmeyi ve daha sonra “bu erişimin sağladığı imkânı, bu yetkilendirmenin kapsamadığı amaçlar için kullanmayı” açıkça yasaklamıştır. Dolayısıyla Kanun, tıpkı Van Buren’in burada tartışmasız bir şekilde yaptığı gibi, kişiler bilgisayarları uygunsuz nedenlerle kullandığında uygulanmaktaydı.

Çoğunluk bunu inkâr etmemektedir. Bunun yerine, Kongre’nin 1986 yılında metni değiştirerek bugünkü tanımına getirdiğini belirtmekte ve Mahkeme’nin Kongre’nin “amaç” terimini çıkarma kararının uygunsuz bir amaç için bilgi edinmeye karşı herhangi bir yasağı zorunlu olarak ortadan kaldırdığını varsayabileceğini söylemektedir.

Ancak çoğunluk bu geçmişten bu kadar kolay kaçamaz. Doğru, kanun daha önce “amaç” terimini içeriyordu ve şimdi içermiyor, ancak çoğunluk bu değişikliğin kanunu nasıl etkilediğini dikkate almıyor. Genellikle, bir kelimenin silinmesi bir hükmün kapsamını daraltmak yerine genişletir. Eğer bir şehir bir parktaki tabelayı “tasmasız köpek giremez” yerine “köpek giremez” olarak değiştirirse, kimse artık tasmasız köpeklere izin verildiğini düşünmez. Aynı durum özel olanın genel olanla değiştirilmesi halinde de geçerlidir (“köpekler giremez” ibaresinin “evcil hayvanlar giremez” olarak değiştirilmesi gibi).

Kongre’nin bu kanunda yaptığı değişiklik de benzer şekilde kanunu genişletmiştir. Orijinal metin, bir bilgisayara yetkilendirme ile erişilmesini ve ardından “bu erişimin sağladığı imkânın söz konusu yetkilendirmenin kapsamadığı amaçlar için kullanılmasını” yasaklamaktaydı. “Amaç” terimi bu maddeyi amaca dayalı kısıtlamalarla sınırlandırmaktaydı. Doğal olarak zaman ve şekil kısıtlamaları gibi diğer kısıtlamaları içermemekteydi. Kongre, spesifik, sınırlı “amaçlar” terimini daha geniş, daha genel bir ifade olan “yetkisi olmayan”

ile değiştirerek, bu diğer kısıtlama türlerine de güç kazandırmıştır. Güvenli olmayan ağlara sahip düşmanca bir yabancı ülkedeyken oturum açmama talimatını ihlal eden çalışanla ilgili önceki örneği düşünün. İş e-postalarını kontrol etmek gibi uygun bir amaçla giriş yaptığı sürece orijinal metin onu kapsamayacaktır. Yeni metin onu kapsayacaktır çünkü veri elde etme ya da değiştirme yetkisi bağlama bağlıdır. Amacı masumdur ancak kullanım zamanı ya da şekli masum değildir.

III

Çoğunluk, son olarak politika argümanlarıyla bitirmiştir. Bu argümanların gerek olmadığını öne sürmektedir. (“halihazırda kremayla kaplanmış bir pastanın üzerine ekstra krema”). Yine de bu argümanlara uzun uzun vurgu yapmıştır. Ne olursa olsun, çoğunluğun bu politika argümanlarına dayanması hatalıdır.

“Olağanüstü sayıda sıradan bilgisayar faaliyetini” suç haline getirmekten endişe duyan çoğunluk, günümüzde insanların bilgisayarları kullanma şeklinin ‘Hükümetin yorumunun mantıksızlığının altını çizdiğini” söylüyor. Ancak kanunlar, “Kongre’nin kanunu yürürlüğe koyduğu zamanki olağan anlamlarına” göre okunur. *Wisconsin Central Ltd. v. Birleşik Devletler*, 585 U. S. ___, ___ (2018). Çoğunluğun 1980’lerde neyin makul olduğunu belirlemek için bilgisayarların günümüzdeki kullanımına güvenmesi, yanlış bir şekilde 1984 yılında Kongre’nin bilgisayarların 2021 yılında nasıl kullanılacağını farkında olduğunu varsaymaktadır.

Ayrıca, benim yorumumun otomatik olarak bu kadar çok davranışı kapsayacağını da hemen varsaymazdım. Birçok hüküm kanunun kapsamını makul bir şekilde daraltmaktadır. Örneğin, kanun, bir kişinin “kasıtlı olarak ... erişim yetkisini aşması” gerektiğine dair *mens rea* şartını içermektedir. §1030(a)(2). Dolayısıyla, bir kişi bilgisayarı belirli bir şekilde kullanmasına izin verildiğine inanıyorsa, örneğin bu tür bir davranış yaygın olduğu ve hoş görüldüğü için kanun uygulanmayabilir. Cf. Restatement (Second) of Contracts §223(2) (1979) (yerleşik bir “işlem seyrinin” belirli sözleşme bağlamlarında yazılı sınırlamaları nasıl silebileceğini tartışmaktadır). Kanun ayrıca sadece “bilgisayardaki bilgilerin elde edilmesi veya değiştirilmesi” ile ilgilidir, §1030(e)(6), uzaktaki bir sunucuda (yani farklı bir bilgisayarda) depolanan spor skorlarını kontrol etmek için interneti kullanmakla değil. Çoğunluk, birçok hükmün bu kanunun odak noktasını makul bir şekilde daralttığını inkâr etmemektedir. Sadece hükümeti bu noktayı daha güçlü bir şekilde tartışmadığı için suçlamaktadır. Hükümetin zararsız davranışları suçlamaya başlayabileceği ve mahkemelerin kanunu bu davranışları kapsayacak şekilde yorumlayabileceği yönündeki varsayımsal endişeye bu kadar ağırlık vermezdim.

Çoğunluğun argümanı da çok fazla şey kanıtlamaktadır. Federal Kanun’un büyük bir kısmı yaygın faaliyetleri suç saymaktadır. Ağırlaştırıcı faktörlerin yokluğunda, bu kanunu ihlal etmenin cezası kabahat için öngörülen yaptırımdır. §1030(c)(2)(A). Dolayısıyla bu kanun, madencilik suçu işleyenleri, federal yasaların National Mall’dan tek bir kum tanesini kaldıran bir kişiyi cezalandırdığı kadar sert bir şekilde cezalandırmaktadır, 40 U. S. C. §8103(b); bir Hükümet binasındaki lambayı kırmak veya bir atın federal arazide ot yemesine izin vermek, 18 U. S. C. §1857. Cezai yaptırımları tetikleyen federal kanun ve

düzenlemelerin sayısı birkaç yüz bine kadar çıkabilir. Bu kadar çok davranışın suç sayılmasından rahatsızlık duymak anlaşılabilir bir durumdur, ancak bu rahatsızlık bize kanunları değiştirme yetkisi vermez.

Sonuçta kanun, 1984'ten bu yana teknolojide meydana gelen değişiklikler nedeniyle geniş bir davranış yelpazesini kapsayabilir ya da kapsamayabilir. Ancak metin bir şeyi açıkça ortaya koymaktadır: Bir polis veritabanını, bu kullanımın açıkça yasaklandığı durumlarda bilgi edinmek için kullanmak suçtur. Saygılarımla karara muhalifim.