



PAK MINUTA DERI TEK MBROJTJA E TË DHËNAVE

Reforma e shumëpritur e ligjit evropian të mbrojtjes së të dhënave, ka marrë më së fundi formë, sikurse shpjegon **Maurizio Mensi**

Mbrojtja e të dhënave është duke pësuar një ndryshim domethënës në të gjithë Bashkimin Evropian. Një rishikim madhor i kuadrit ligjor të mbrojtjes së të dhënave nisi në vitin 2009 me qëllim harmonizimin e mëtejshëm të legjislacionit të mbrojtjes së të dhënave anembanë Evropës, duke qenë se fragmentimi i tij aktual, ngarkon së tepërmi operatorët e tregut që kryejnë aktivitete ndërkufitare. Kështu që BE-ja ka nevojë për një marrëveshje të re në lidhje me mbrojtjen e të dhënave, të aftë për të lehtësuar qarkullimin e të dhënave, si në BE ashtu edhe tek partnerët e saj tregtarë dhe për të garantuar të drejtat dhe liritë e individëve.

Për këtë qëllim, propozimi i Komisionit Evropian për një reformë tërësore të Direktivës së BE-së të 1995-ës për Mbrojtjen e të Dhënave, synon të përforcojë të drejtat për privatësi dhe të përkrahë ekonominë digjitale të Evropës, duke modernizuar parimet e sanksionuara në direktivën e 1995-s, duke i zhvendosur ato në erën digjitale. Propozimi i Komisionit i datës 25 janar 2012, përfshin një komunikim politikash, të cilat përcaktojnë objektivat e Komisionit² dhe dy masa legislative: një rregullore e cila përcakton një kuadër të përgjithshëm për mbrojtjen e të dhënave të BE-së (GDPR) dhe një direktivë për mbrojtjen e të dhënave personale të përpunuara për qëllime të parandalimit, zbulimit, hetimit apo procedimin e veprave penale dhe aktiviteteve gjyqësore të lidhje me to (Direktiva e BE-së për Mbrojtjen e të Dhënave).

Në vijim të rishqyrtimit të kryer nga komitetet e Parlamentit, më 12 mars 2014, Parlamenti Evropian aprovoi tekstet e kompromisit të GDPR-së së bashku me direktivën për mbrojtjen e të dhënave të policisë dhe drejtësisë penale. Ky miratim i përshpejtuar u ndikua në mënyrë të veçantë nga “Datagate-i”, skandali i përgjimeve masive të programit Prism, të Agjencisë së Sigurisë Kombëtare të SHBA-ve, të cilat u zbuluan prej analistit Edward Snowden, në qershor të 2013-ës, që kishin të bënin me mbledhjen e të dhënave të milionave të përdoruesve të telefonisë.

Në 15 qershor 2015, ministrat përfaqësues të vendeve anëtare të Këshillit të BE-së për Drejtësinë dhe Çështjet e Brendshme ranë dakord për një “qasje të përgjithshme” për GDPR-në e propozuar³. Miratimi i qasjes mbarte me vete autoritet për presidencën për të ndërmarrë negociata me Komisionin dhe Parlamentin, duke përcaktuar kornizën për arritjen e një teksti kompromisi, i cili do të miratohej si rregullore përfundimtare. Diskutimet trepalëshe nisën në qershor duke synuar të miratonin një tekst nga fundi i vitit. Debati mbi Direktivën e BE-së për Mbrojtjen e të Dhënave ashtu si edhe GDPR-në nga Parlamenti dhe Këshilli, janë zhvilluar paralelisht, teksa institucionet ranë dakord për një strategji fleksibël.

Së fundmi, më 15 dhjetor 2015, përfaqësuesit nga Komisioni Evropian, Parlamenti Evropian dhe shtetet anëtare, arritën një marrëveshje politike jo formale mbi paketën e mbrojtjes së të dhënave⁴.

Kompromisi për zgjidhjen e konflikteve institucionale

GDPR-ja përcakton veprimtari dhe gjoba proporcionale, duke nisur nga një rekomandim ose paralajmërim deri në 20 milion € ose 4% të xhiros totale vjetore të vitit financiar paraardhës, cilido qoftë më i lartë dhe sanksionet do të jenë fleksibël. Një numër faktorësh do të merren në konsideratë në përcaktimin e nivelit të gjobave përfshirë edhe kohëzgjatjen dhe seriozitetin e shkeljes tek të dhënat, neglizhencën dhe qëllimin si edhe ndikimin tek përdoruesit. Vëmendje e veçantë i duhet kushtuar gjithsesi *“veprimeve të ndërmarra për zbutjen e dëmtimit të pësuar, shkallës së përgjegjësisë apo çdo shkeljeje të mëparshme serioze, mënyrës me të cilën u vu në dijeni autoriteti mbikëqyrës për shkeljen, përputhshmërisë me masat e urdhëruara ndaj kontrolluesit apo përpunuesit, zbatimin e një kodi sjelljeje dhe çdo rrethanë tjetër rënduese apo lehtësuese”* (pika 118b).

GDPR-ja do të përcaktojë një set homogjen rregullash mbi mbrojtjen e të dhënave në fuqi nëpër krejt BR-në në mënyrë uniforme. Pika 21 përcakton: *“Përpunimi i të dhënave personale të subjekteve të të dhënave që ndodhen në Union nga një kontrollues apo përpunues të vendosur jashtë Unionit, duhet të jetë gjithashtu subjekt i kësaj rregulloreje, kur kjo ka lidhje me monitorimin e aktivitetit të këtyre subjekteve të të dhënave, për sa kohë që aktiviteti i tyre zhvillohet brenda Bashkimit Evropian.”*

Vijon me atë se juridiksioni i GDPR-së do të shtrihet jashtë BE-së, meqenëse gjen aplikim tek oferta e mallrave dhe shërbimeve drejt ose tek monitorimi i subjekteve të të dhënave jashtë BE-së. Kontrolluesit jashtë BE-së që përmbushin këtë lidhje juridiksionale, do të duhet të përcaktojnë një përfaqësues nga BE-ja, *“përveçse në rastet kur përpunimi që ai kryen është rastësor”* dhe *“nuk ka të ngjarë të rezultojë në risk për të drejtat dhe liritë”* e individit (pika 63).

Vini re se gjatë negociatave, Këshilli i Ministrave i bëri ndryshime të rëndësishme tekstit të Komisionit dhe qasja aktuale e përgjithshme ndryshon dukshëm nga teksti i miratuar nga Komisioni në janar të 2012-s, ashtu si edhe nga amendimet e tekstit të Komisionit, të propozuara nga Parlamenti Evropian gjatë shqyrtimit të tij të parë në mars 2014. Një sërë problemesh u shfaqën nga mosmarrëveshja midis institucioneve të përfshira.

Së pari, GDPR-ja nxjerr në pah një *“one stop shop”* për operatorët e tregut dhe përdoruesit, të cilët do të kenë të bëjnë me një autoritet mbikëqyrës të vetëm, duke thjeshtuar operacionet ndër-kufitare dhe biznesin. Ky mekanizëm ka për qëllim të garantojë konsekuencë në interpretimin dhe zbatimin e rregullores në të gjithë BE-në nga autoritetet mbikëqyrëse, duke reduktuar në mënyrë

domethënëse kostot dhe duke ofruar siguri më të madhe ligjore në çështjet e zbatimit të ligjit, të cilat përfshijnë shumë autoritete të mbrojtjes së të dhënave. Gjithsesi, dispozitat e “*one stop shop-it*” u zbutën nga Këshilli, sikurse në shkeljet shumë-juridiksionesh, ku autoriteteve mbikëqyrëse përkatëse do të duhet t’u merret mendimi dhe do të kenë mundësi të hedhin poshtë vlerësimin e autoritetit drejtues të procesit.

Për më tepër, në rastet kur përfshihet vetëm një juridiksion, autoriteti mbikëqyrës në atë juridiksion do të jetë precedencë në lidhje me çështjen, përkundër autoritetit drejtues të procesit, sikurse përcaktohet nga parimi i “*one stop shop-it*”. Kjo nënkupton një qartësim të kompetencës së autoritetit mbikëqyrës dhe përzgjedhjen e autoritetit lider në çështje të përpunimit transnacional. Autoritetet e mbrojtjes së të dhënave duhet të jenë të gatshme të ushtrojnë rolet e tyre, kur rregullorja të hyjë në fuqi dhe të përcaktojnë mjetet juridike proporcionale dhe të përshtatshme dhe sanksionet administrative në bazë të të gjitha rrethanave të lidhura me to.

Së dyti, GDPR-ja detyron marrjen e pëlqimit paraprak përpara mbledhjes dhe përpunimit të të dhënave të subjekteve. Subjektet e të dhënave duhet të jenë gjithnjë të informuar mbi të drejtën e tyre për refuzim të pëlqimit për përpunimin e të dhënave të tyre personale. Gjithashtu, “subjektet e të dhënave duhet të informohen mbi ekzistencën e profilizimit dhe pasojat e një profilizimi të tillë” (pika 48). “Profilizimi” përkufizohet si çdo formë përpunimi automatik të dhënash personale, e cila vlerëson aspektet personale, për sa kohë që prodhon efekte ligjore, në lidhje me subjektin e të dhënave. Teksti i miratuar më 15 dhjetor 2015, ka përcaktuar më ngushtësisht natyrën e pëlqimit të informuar, duke përkufizuar kufijtë e cilësisë së pëlqimit, që kontrolluesit e të dhënave duhet të marrin, për të zotëruar bazë ligjore për përpunimin e të dhënave, meqenëse është përdorur mbiemri “eksplicit”.

Përkundrazi, drafti i mëparshëm i Këshillit kërkonte që pëlqimi “të jepet në mënyrë të qartë”, çka do t’u jepte kontrolluesve të të dhënave më shumë liri veprimi në përdorimin e mëtejshëm të të dhënave, e cila nuk ishte parashikuar gjatë mbledhjes së të dhënave. Gjithsesi, profilizimi në vetvete nuk është burim shqetësimi. Përkundër tij, mungesa e informacionit adekuat mbi mekanizmat algoritmike e cila nxit profilizimin dhe synon praktikën reklamuese, duhet të trajtohet nëpërmjet rritjes së transparencës së kontrolluesve të të dhënave, në përputhje me qasjen e përgjithshme.

Profilizimi i përdoruesve nëpërmjet posedimit të të dhënave masive, është epiqendra e disa tregjeve, sikurse reklamimi në internet, ku është mundësia të

krijohen, nëpërmjet teknologjisë së internetit, profile përdoruesish më të sakta, të cilat krijojnë mundësinë të afrohen tipa specifike konsumatorësh (duke u dërguar atyre mesazhe të shënjestruara, me nivele të shtuara përshtatshmërie) dhe të matet më saktësisht efektshmëria e fushata reklamuese. Në këtë perspektivë, rëndësi strategjike i jepet mbledhjes së të dhënave të përdoruesve, të cilat përbëjnë asete me vlerë ekonomike të padiskutueshme, meqenëse ato kanë të ngjarë të përfshihen si pjesë e industrisë së publicitetit. Nga këtu del nevoja për më shumë neutralitet dhe transparencë në platformat kërkimore-reklamuese.

Në këtë kuadër, Google-i është akuzuar se manipulon rezultatet e kërkimeve të veta organike, për të favorizuar shërbimet e veta. Këto akuza janë shoqëruar shpeshherë nga thirrje për ndërhyrje rregulatore apo *antitrust*. Ato duhet gjithsesi të marrin në konsideratë të plotë natyrën e dyanshme të platformës kërkimore-publicitare dhe efektet reaguese të cilat lidhin masat e rezultateve të kërkimeve organike me konsumatorët dhe shitjen tek bizneset e reklamimit. Komisioni Evropian, në kuadër të strategjisë së tregut unik digjital për Evropën, ndërmori në maj 2015, planet për nisjen e një vlerësimi tërësor të rolit të platformave dhe ndërmjetësve në internet, i cili do të mbulojë problematika sikurse transparenca (p.sh. në rezultatet e kërkimeve), duke përfshirë lidhjet në internet me pagesë (*paid-for links*) dhe/ose reklamat.

Sa i takon njoftimeve për shkelje, GDPR-ja dikton se autoritetet mbikëqyrëse dhe individët e prekur, duhet të njoftohen për shkelje të cilat kanë gjasa të vënë në rrezik të drejtat dhe liritë e individëve, me njoftim të autoriteteve mbikëqyrëse “pa vonesa të paligjshme dhe kur kjo është e mundur, jo më vonë sesa 72 orë”. Kjo qasje ndryshon nga ajo e Komisionit, e cila përcakton detyrimet për përputhshmëri të cilat duhet të përmbushen nga të gjithë kontrolluesit e të dhënave, e cila është më pak e përshtatur me riskun. Komisioni fillimisht sugjeroi që njoftimi për shkelje të sigurisë së të dhënave duhet të bëhet brenda një periudhe jo më pak se 24 orë, që nga momenti kur kontrolluesi i të dhënave vihej në dijeni për shkeljen.

Një aspekt tjetër i rëndësishëm i rregullores së propozuar është parashikimi i hollësishëm i së drejtës për t’u harruar, e cila tashmë pranohet si një parim i përgjithshëm evropian, në vijim të çështjes së marrë si pikë referimi të gjykatës Evropiane të Drejtësisë (ECJ). Më 13 maj 2014, ECJ-ja vendosi se, duke kërkuar automatikisht për informacion të publikuar në internet, duke indeksuar faqe të internetit, duke regjistruar dhe vënë ato në dispozicion, operatori i motorit të kërkimit është duke “përpunuar” të dhëna personale, në kuptimin e Nenit 2(b) të Direktivës 95/46/EC (shih çështjen Google Spanjë).⁵ Në vijim të

vendimit të saj të mëparshëm, ⁶ Gjykata konfirmoi se, edhe kur informacioni i mbledhur nga operatori i një motori kërkimi, ka qenë publikuar gjetkë nga të tjerë, aktiviteti i motorit të kërkimit në fjalë, duhet sërish të klasifikohet si përpunim sipas direktivës.

Vendimi detyronte Google-in të shqyrtonte kërkesat e individëve për të fshirë lidhje interneti të cilat ata pretendojnë se shkelin privatësinë e tyre. Kjo dispozitë do t'i jepte kujtdo të drejtën “për të përfituar prej kontrolluesit fshirjen e të dhënave të tyre personale (...) pa vonesa të paarsyeshme”. (“kontrolluesi i të dhënave” është në thelb njësi vendimmarrëse mbi ato sesi e për çfarë qëllimi përpunohen të dhënat). GDPR-ja njeh në mënyrë të hollësishme të drejtën e subjektit të të dhënave për të përfituar prej kontrolluesit fshirjen e të dhënave personale pa vonesë të paarsyeshme (shih nenin 17).

REFORMA E DIREKTIVËS SË E-PRIVATËSISË

Viti 2015 ishte padyshim viti i ndryshimit të madh. Komisioni i ri, i drejtuar nga Jean-Claude Juncker, në mënyrë ambicioze përcaktoi objektivin “për të ndërmarrë, brenda gjashtë muajve të parë të mandatit [të tij], hapa ambiciozë legjislativë drejt një tregu unik digjital të ndërlidhur”. Edhe pse paketa e Kontinentit të Ndërlidhur ishte pjesërisht e pasuksesshme për shkak të konflikteve ndërmjet Këshillit dhe Parlamentit (pasi qëllimi i tij kufizohej tek roaming-u dhe neutraliteti i internetit), strategjia e Komisionit për tregun unik digjital (DSM) është gjithsesi një program që mirëpret iniciativën, me synime, qëllim dhe afat zbatimi ambicioz.

Përsiatja e GDPR-së është mbështetur dhe përforcuar nga strategjia e DSM-së, e cila sheshon 16 aktivitete me objektiva, për t'u vënë në jetë nga fundi i 2016-s. Njëra nga aktivitetet nxit një reformë të Direktivës 2002/58/EC (direktivës së e-privatësisë).⁷ Privatësia është një çështje me rëndësi të madhe për qytetarët e BE-së, duke qenë se dy të tretat janë të shqetësuar për faktin se nuk kanë kontroll të plotë mbi informacionin që ata japin në internet.⁸ Në të vërtetë, miratimi i GDPR-së, e cila do të zëvendësojë Direktivën 95/46/EC, do të ketë pasoja gjithashtu edhe për direktivën e e-privatësisë, e cila është *lex specialist* (ligji rregullator) për sektorin e komunikimeve elektronike.

Në këtë mënyrë, strategjia e DSM-së nxit rivlerësimin e direktivës së e-privatësisë, veçanërisht duke qenë se shumica e neneve të direktivës aktuale gjejnë zbatim ekskluzivisht tek ofruesit e shërbimeve të komunikimeve elektronike (të cilat janë kompanitë tradicionale të telekomunikacioneve) dhe nuk përshijnë në qëllimin e tyre ofruesit e shërbimeve të shoqërisë së informacionit të cilët përdorin internetin për të ofruar shërbime komunikimi.

QËNDRIMI I ECJ-së NË LIDHJE ME DIREKTIVËN PËR MBAJTJEN E TË DHËNAVE

Institucionet evropiane duhet gjithashtu të respektojnë vendimin e ECJ-së e cila e nxori të pavlefshme Direktivën për Mbjajtjen e të Dhënave⁹ në 2014-n. ECJ-a përcaktoi se, edhe pse të dhënat e e mbajtura nuk përfshijnë përmbajtjen e komunikimeve, të dhënat mund *“të lejojnë nxjerrjen e konkluzioneve të sakta në lidhje me jetët private të personave, të dhënat e të cilëve janë mbajtur, sikurse edhe të zakoneve të jetës së përditshme, vendeve të përkohshme ose të përhershme të qëndrimit, lëvizjeve të përditshme ose të tjera, aktiviteteve të zhvilluara, lidhjeve shoqërore të atyre personave dhe ambienteve shoqërore të frekuentuara prej tyre”*.

Me fjalë të tjera, ECJ-ja vendosi se direktiva kufizonte privatësinë e subjekteve për shkak se *“fakti që të dhënat janë mbajtur dhe përdorur më tej pa e informuar abonentin apo përdoruesin e regjistruar, ka të ngjarë të gjenerojë në mendjet e këtyre personave ndjenjën se jetët e tyre private janë subjekt survejimi konstant”*. Direktiva nuk parashikoi një periudhë mbajtjeje *“të kufizuar tek ajo çfarë [ishte] patjetër e nevojshme”* meqenëse përbënte një minimum periudhe mbajtjeje prej gjashtë muajsh, pa bërë dallim midis llojeve të ndryshme të të dhënave apo tipave të ndryshëm të përdoruesve dhe një periudhë mbajtjeje midis gjashtë muajsh dhe dy vitesh, pa u nevojitur asnjë *“përcaktim [se] periudha duhet bazuar në kritere objektive”*.

Për këto arsye, ECJ-ja shpalli të pavlefshme direktivën për mbajtjen e të dhënave, duke arsyetuar se ajo nuk e respektonte parimin e proporcionalitetit dhe duhet të kishte parashikuar më shumë masa sigurie për të mbrojtur të drejtat themelore për privatësi dhe mbrojtje të të dhënave personale, të garantuara nga Karta e të Drejtave Themelore të BE-së.

Si President i Parlamentit Evropian, Martin Schulz-i theksoi në përgjigje të vendimit të ECJ-së se çdo propozim i ri duhet *“të respektojë në çdo detaj garancitë e parashtruara nga Karta e të Drejtave Themelore [...], [duke] parashikuar nivel të lartë të mbrojtjes së të dhënave – e cila është në tërësi më thelbësorja në erën digjitale – duke shmangur kështu ndërhyrjet e shpërpjesëtuara në jetët private të qytetarëve”*. Kështu, institucionet evropiane nuk mund të injorojnë vendimin e ECJ-së në lidhje me të dhënat personale dhe privatësinë. Në veçanti, propozimi për direktivën e BE-së për mbrojtjen e të dhënave, duhet të jetë konform vendimit të ECJ-së.¹⁰ Me të njëjtin kut, ECJ-ja

dhe gjykatat kombëtare, duhet të marrin në konsideratë Kartën e të Drejtave Themelore në raste gjykimesh të çështjeve ku ligji i BE-së është në diskutim.

Interesant ishte edhe fakti se grupi i punës këshillimor i Nenit 29¹¹ i bëri gjithashtu thirrje shteteve anëtare, që të njehësojnë pasojat e vendimit të ECJ-së në ligjet e tyre kombëtare të mbrojtjes së të dhënave, duke vënë në dukje se *“nuk mund të ketë sasi kapicë të të gjitha llojeve së të dhënave që mbahen, përkundrazi, të dhënat janë subjekt i diferencimit të përshtatshëm, kufizimit dhe përjashtimit”*.

Varësia në rritje nga posedimi i të dhënave të përdoruesve, është tipari i sotëm i shoqërisë së informacionit. Të dhënat janë një aset i çmuar për një sërë sektorësh, për shembull reklamën në lidhje me kërkimin në internet. Ato u mundësojnë aktorëve të industrisë së reklamave të lidhura me kërkimin, të zhvendosen me shpejtësi në tregjet fqinje, të tilla sikurse reklamën që nuk lidhen me kërkimin, ato që lidhen me kontekstin, shfaqjen, postën elektronike dhe të përgjithshme. Tendenca për konvergjencë drejt këtyre formateve të ndryshme të reklamës, e cila i detyrohet zhvillimit të reklamës që lidhet me sjelljen dhe prirjes për të përzier dhe përputhur strategji të ndryshme të reklamimit nga aktorët më të mëdhenj të industrisë, është vërejtur nga Komisioni Evropian gjatë hetimeve që zhvilloi si tek Google/DoubleClick ashtu edhe tek Microsoft/Yahoo-ja.

Në të njëjtën kohë, posedimi i të dhënave prodhon pengesa për hyrjen në treg, duke i veshur mbajtësit të tyre përparësi të cilat nuk mund t'i kenë njëllor aktorët e rinj potencialë që duan të hyjnë. Në veçanti, njësitë e tjera që merren me ofrimin e reklamës që lidhet me kërkimin në internet, do ta kenë shumë të vështirë të ofrojnë të njëjtën cilësi rezultatesh që ofrohen nga firma dominuese, çka do të mund t'i përforconte pozicionin e saj, duke luajtur njëkohësisht në tregje të shumta dhe paralele, në të cilat mund të përftojë, verifikojë, testojë dhe sigurojë specifikime shtesë të informacionit të përftuar në kontekstin e reklamës kërkimore normale.

Si rrjedhojë, tregjet e përqendruara tek të dhënat kanë gjasa të jenë shumë më pak të përcaktuara saktësisht në lidhje me një produkt të caktuar apo shërbim dhe shumë më tepër tek aftësia e një pjesëmarrësi për të përdorur të dhënat në lloje të ndryshme aktivitets. Në këtë mënyrë, një element thelbësor në përcaktimin e këtyre tregjeve, është të përshkruhet qëllimi për të cilin politikat e privatësisë të përdorimit të faqes së internetit (apo motorit të kërkimit) lejojnë përdorimin e informacionit të përftuar nga përdoruesit në kontekste të tjera, ashtu si edhe ofrimin e një shërbimi tjetër nga e njëjta kompani

(ndryshueshmëria brenda së njëjtës kompani – ‘*intra-company versatility*’) dhe për kompani të tjera që ofrojnë të tjera shërbime apo edhe të njëjtin (zhvendosje të shërbimit nga një kompani në tjetrën - ‘*inter-company portability*’).

ANULLIMI I MARRËVESHJES SË KOMISIONIT ME SHBA-TË TË “SAFE HARBOUR”

Zbulimet e Edward Snowden-it në lidhje me survejimin masiv të qytetarëve të BE-së, pati ndikim edhe në të ashtuquajturën skema e “*safe harbour*”-it, e cila përfshinte një sërë parimesh në lidhje me mbrojtjen e të dhënave personale, tek të cilat ndërmarrjet e SHBA-ve mund të pajtoheshin vullnetarisht.¹³ Më hollësisht, më 6 tetor 2015, ECJ-ja e shpalli të pavlefshme¹⁴ marrëveshjen transatlantike të mbrojtjes së të dhënave të Komisionit Evropian që datonte në vitin 2000, duke pretenduar se nuk i mbronte konsumatorët në mënyrë të përshtatshme. Në fakt, ligji i privatësisë së BE-së, ndalon lëvizjen e të dhënave të qytetarëve të saj jashtë BE-së, përveçse nëse transferohen në një vend i cili vlerësohet se ka mbrojtje “të mjaftueshme” të privatësisë, në përputhje me atë të BE-së.

Faktikisht, edhe vetë Komisioni Evropian kishte shprehur dyshime në lidhje me përshtatshmërinë e skemës së “*safe harbour*”-it. Gjatë një komunikimi të nëntorit 2013, ai e pranoi shqetësimin në rritje të disa autoriteteve të mbrojtjes së të dhënave të BE-së në lidhje me transferimet e të dhënave në kuadër të kësaj skeme dhe vuri në dukje se “*disa autoritete të mbrojtjes së të dhënave të “disa shteteve anëtare”, kanë kritikuar formulimin tepër të përgjithshëm të parimeve dhe varësinë tepër të lartë tek vetë-certifikimi dhe vetë-rregullimi. Shqetësime të ngjashme u ngritën edhe nga industria, duke iu referuar problemeve me konkurrencën, për shkak të mungesës së kuadrit ligjor*”¹⁵

Në vendimin e saj historik, ECJ-ja specifikoi se Komisioni Evropian nuk mund të kufizonte kompetencat e autoriteteve të mbrojtjes së të dhënave sa i takon mbrojtjes së të dhënave personale të qytetarëve të tyre. Ishte mjaft interesant fakti, se vendimi u mor më pak se një javë pas vendimit të ECJ-së për çështjen *Weltimmo*,¹⁶ për të cilën vendosi se kompanitë ndërkombëtare duhet të zbatojnë legjislacionin për mbrojtjen e të dhënave të juridiksionit brenda të cilit operojnë, (çështja kishte të bënte më një kompani me faqe interneti për pronë, të regjistruar në Sllovaki, por që “operonte” në Hungari).

Në vijim të anulimit të marrëveshjes së “*safe harbour*”-it, kompanitë amerikane, përfshirë edhe gjigandët e internetit si Google-i, Facebook-u, Apple-

i dhe Microsoft-i, duhet të përpiqen të hartojnë “modele të klauzolave kontraktuale” që t’u autorizohen transferimet e të dhënave jashtë Evropës, duke garantuar kështu nivel të përshtatshëm mbrojtjeje, në përputhje me rregullat e BE-së. Në këtë mënyrë, ka gjasa që kompanitë e mëdha amerikane të ndërtojnë qendra të dhënash të vendosura në BE, për të trajtuar të dhënat e qytetarëve të BE-së.

Megjithatë, duhet theksuar se BE-ja është duke negociuar me SHBA-të për një “safe harbour” të përmirësuar, e cila të respektojë shqetësimet e ECJ-së, gjithë duke garantuar siguri dhe transparencë.

MODERNIZIMI I KONVENTËS 108 TË KËSHILLIT TË EVROPËS

Paralelisht me iniciativën legjislative të Komisionit, Këshilli i Evropës (CoE) paraqiti në mars të 2012-s propozimet e veta për përditësimin e Konventës për Mbrojtjen e Individëve nga Përpunimi Automatik i të Dhënave Personale (Konventa nr. 108).¹⁷ Në tetor të 2011-s, asambleja parlamentare e KiE-së bëri një rekomandim, i cili mbështeste përforsimin dhe globalizimin e Konventës 108.¹⁸ Në nëntor 2012, komiteti konsultativ i KiE-së, miratoi propozimet e tij përfundimtare për modernizimin dhe ua paraqiti ato Komitetit të Ministrave për miratim.¹⁹

Në fund, komiteti *ad hoc* për mbrojtjen e të dhënave të KiE-së, pas diskutimesh e amendimesh, miratoi më 3 dhjetor 2014, propozimet për modernizimin e konventës. Një draft protokoll amendimesh do të hartohet bazuar në to dhe do t’i transmetohet Komitetit të Ministrave për shqyrtim dhe miratim.²⁰

Edhe pse BE-ja dhe KiE-ja ndajnë të njëjtat shqetësime në lidhje me mbrojtjen e të dhënave, qasjet e tyre janë të ndryshme. Konventa, e cila shërben si një lloj standardi universal, është më pak detyruese dhe më shumë e përqendruar tek të drejtat e njeriut (shih hyrjen e saj).²¹ Por koherenca dhe përputhshmëria e saj me kuadrin rregullator evropian mbetet objektivi i saj kyç.

RRUGA QË KEMI PËRPARA

Negociatat për të reformuar rregullat e BE-së mbi mbrojtjen e të dhënave janë në fazën përfundimtare. Më 17 dhjetor 2015, Komiteti i Parlamentit të BE-së për Liritë Civile, Drejtësinë dhe Çështjet e Brendshme (LIBE) votoi për një marrëveshje jo formale në lidhje me paketën e mbrojtjes së të dhënave.²²

Tekstet përfundimtare të paketës së reformës, do të hidhen në votë dhe do të miratohen formalisht nga Parlamenti Evropian dhe Këshilli gjatë 2016-ës, me gjasa në mars ose prill. Që prej aty, do të ketë një periudhë ndërmjetëse prej dy vitesh, për hyrjen e saj në fuqi.

Përkundër këtij sfondi, strategjia e DSM-së do të luajë rol kyç. Sfida qëndron në trajtimin e çështjeve thellësisht teknike teksa përballesh me qëndrime të forta politike, të cilat nuk ndihmojnë gjithnjë për lehtësimin e rrugës drejt zbatimit. Mendohet që strategjia e DSM-së të zhvillojë aksione të ndryshme nga fundi i 2016-ës, me mbështetjen e Parlamentit dhe Këshillit. Për shkak të këtyre konflikteve potenciale, duhet vendosur një peshore midis riskut që buron prej garës për rregullim absolut – i cili mund të ndrydhte tregun dinamik digjital – dhe një mungese të rrezikshme të një mbrojtjeje të dhënash të plotë brenda Bashkimit Evropian.

Maurizio Mensi është profesor i ligjit ekonomik pranë Shkollës Kombëtare të Administratës (SNA) dhe të ligjit të informacionit dhe komunikimeve pranë LUISS Guido Carli University, Romë. Ai është anëtar i Dhomës së Avokatëve të Romës dhe ka kryer praktikën në gjykatën më të lartë të Italisë. Mensi përqendrohet në komunikime dhe media, Teknologji Infomacioni, privatësi dhe mbrojtje të dhënash, të drejtën e autorit, legjislacioni kibernetik dhe rregullimin e shërbimeve publike.

REFERENCAT **1** Direktiva 95/46/EC për mbrojtjen e individëve nga përpunimi automatik i të dhënave personale dhe mbi lëvizjen e këtyre të dhënave. **2** Mbrojtja e privatësisë në një botë të ndërlidhur: një kuadër ligjor evropian për mbrojtjen e të dhënave personale për shekullin e 21-të. bit.ly/1llhkye **3** Propozimi për një rregullore të Parlamentit Evropian dhe Këshillit mbi mbrojtjen e individëve nga përpunimi i të dhënave personale dhe lëvizja e lirë e këtyre të dhënave (Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave) – Përgatitja e një qasjeje të përgjithshme bit.ly/1ShoM8T **4** Pajtueshmëria me Komisionin për reformën e mbrojtjes së të dhënave të BE-së do të nxisë tregun unik digjital. Njoftim për shtyp i KE-së, 15 dhjetor 2015. bit.ly/1J9ZUdt **5** Google Spanjë – çështje e gjykuar më 13 maj 2014. bit.ly/1MKoqFS **6** Satakunnan Markkinapörssi and Satamedia – çështje e gjykuar më 16 dhjetor 2008. bit.ly/1LEUqHq **7** Direktiva 2002/58/EC e Parlamentit Evropian dhe Këshillit e 12 korrikut 2002 mbi përpunimin e të dhënave personale dhe mbrojtjen e privatësisë në sektorin e komunikimeve elektronike. Shih strategjinë e Komisionit për DSM-në, shtylla II, aksioni 12. **8** Studim i Eurobarometer-it mbi mbrojtjen e të dhënave, qershor 2015. bit.ly/1LPx1Ho **9** Direktiva 2006/24/EC e 15 marsit 2006 mbi mbajtjen e të dhënave të

krijua ose përpunua në lidhje me ofrimin e shërbimeve të komunikimeve elektronike në dispozicion të publikut ose të rrjeteve publike të komunikimit, që amendon Direktivën 2002/58/EC. **10** Propozimi për një direktivë për mbrojtjen e individëve nga përpunimi i të dhënave personale nga autoritetet kompetente për qëllime të parandalimit, hetimit, zbulimit dhe procedimit të veprave ose ekzekutimin e sanksioneve penale dhe lëvizjen e lirë të këtyre të dhënave, 25 janar 2012. bit.ly/1Tj7acV **11** Grupi i Punës së Nenit 29 përbëhet nga një përfaqësues nga secili autoritet për mbrojtjen e të dhënave të shteteve anëtare të BE-së, Mbikëqyrësi Evropian për Mbrojtjen e të Dhënave dhe Komisioni Evropian, sikurse përcaktohet në Nenin 29 të Direktivës 95/46/EC. **12** Shih Çështjen COMP/M.4731 Google/Double Click; Çështjen COMP/M.5727 Microsoft /Yahoo Search Business. **13** Vendim i Komisionit 2000/520/EC i 26 korrikut 2000 në përputhje me Direktivën 95/46/EC të Parlamentit Evropian dhe të Këshillit mbi përshtatshmërinë e mbrojtjes që ofrojnë parimet e privatësisë së ‘safe harbour’-it dhe pyetje të shpeshta që ngrihen në lidhje me to, të hartuara nga Departamenti i Tregtisë së SHBA-ve. **14** Gjykimi i Çështjes C-362/14. Gjykata e Drejtësisë deklaroi se vendimi i Komisionit për ‘Safe Harbour’-in me SHBA-të është i pavlefshëm. 6 tetor 2015. bit.ly/1FUc1iu **15** Komunikim nga Komisioni tek Parlamenti Evropian dhe tek Këshilli mbi funksionimin e ‘Safe Harbour’-it nga këndvështrimi i qytetarëve të BE-së dhe kompanive me seli në BE. bit.ly/19VRFqN **16** Gjykimi i Çështjes C-230/14. Weltimmo s.r.o. vs Nemzeti Adatvédelmi és Információs Zsabadság Hatóság. 1 tetor 2015. bit.ly/1VrPhIG **17** Konventa për mbrojtjen e individëve nga përpunimi automatik i të dhënave personale, miratuar nga Këshilli i Evropës në 1981-shin. ETS Nr. 10. **18** Rekomandimi 1984 (2011) i Asamblesë parlamentare të Këshillit të Evropës Mbrojtja e privatësisë dhe të dhënave personale në internet dhe mediat *online*. **19** Komiteti konsultativ i konventës për mbrojtjen e individëve nga përpunimi automatik i të dhënave personale (T-PD). Modernizimi i Konventës 108: Dokumenti përfundimtar. Strasburg, 29 nëntor 2012. **20** Komiteti *Ad hoc* për mbrojtjen e të dhënave personale. Takimi i 3-të. 1-3 dhjetor 2014. bit.ly/1sumsTF **21** “Duke marrë në konsideratë dëshirën që të shtohen masat e sigurisë për liritë dhe të drejtat themelore të secilit dhe në veçanti i së drejtës për respektim të privatësisë, duke marrë parasysh qarkullimin ndërkuftar në rritje të së dhënave personale që u nënshtrohen përpunimit automatik [...] duke pranuar se është e nevojshme të bashkërendojmë vlerat fundamentale të respektit për privatësinë dhe qarkullimin e lirë të informacion midis popujve.” Hyrje, Konventa nr. 108. **22** Rregullat e reja të BE-së mbi mbrojtjen e të dhënave, e vendosin sërish qytetarin në sedijen e shoferit. Parlamenti Evropian, njoftim për shtyp, 17 dhjetor 2015. bit.ly/1JECFse