Nanoteknologien eta RFID dispositiboen arteko konbergentzia teknologikoa: pribatutasunarentzako mehatxu berri baten atarian?

Ramirez de la Piscina, Aratz
Administrazio Zuzenbidea, Konstituzio Zuzenbidea eta Zuzenbidearen Filosofia Saileko doktorea
aratz.ramirezdelapiscina@ehu.eus

Laburpena

Nanomaterial manufakturatuak (NMM), nanoteknologien ustiapenetik eratortzen diren material berriak, besteak beste irrati frekuentzia bidezko identifikazio sistemadun (RFID) etiketen prestazio teknikoak potentziatzeko erabiltzen dira. Dispositibo elektroniko horiek nagusiki esparru komertzialean produktuen unean uneko trazabilitatea egiteko baliatzen badira ere, norbanakoen informazio pertsonala eskuratzeko ere erabili izan diren kasu batzuk dokumentatu dira dagoeneko. Alde horretatik, ikerketa honen xedea kasu horietan RFID etiketen erabilerak norbanakoen pribatutasuna errespetatu duen edo ez aztertzean datza, horretarako datu pertsonalen babeserako legedia oinarri hartuta.

Hitz gakoak: nanoteknologiak, RFID etiketak, datu pertsonalak, pribatutasuna

Abstract

Manufactured nanomaterials (MNM), those new materials obtained from the employment of nanotechnologies, are used among other things to enhance the technical properties of Radio Frequency Identification tags. Although these electronic devices are mainly used in the commercial area to ensure a constant traceability of products, there have been already documented some cases where they were employed to acquire personal data. In this sense, the objective of this research is to analyze whether in those cases the privacy of individuals has been respected on the basis of the personal data protection regulations.

Keywords: nanotechnologies, RFID labels, personal data, privacy

1. Sarrera eta motibazioa

Nanoteknologiek, materia eskala nanometrikoan (10^{-9} metro) manipulatzetik beren propietate ezberdin eta teknikoki probetxugarriak eskuratzea helburu duten teknologien multzoak, hazkuntza nabarmena izan dute XXI. mende hasiera honetan. Euren ustiapenetik eratortzen diren material berriak, nanomaterial manufakturatu izenekoak (aurrerantzean NMM), gero eta produktu eta aplikazio gehiagotan ikertu, erabili eta komertzializatzen dira, beste batzuen artean, produktu kosmetiko, plagizida, elikagai, ehungintza, elektronika, medikamendu eta tratamendu medikoetan eta industria militarrean[1].

Izan ere, NMMak aniztasun, heterogeneotasun, sofistikazio eta konbergentzia teknologikoaren sinonimo dira. Ekoizten diren NMM moten kopurua gero eta anitzagoa da (gaur egun 4.000 mota inguru dokumentatu dira[2]) eta horietako bakoitzak propietate fisiko-kimiko desberdinak eta heterogeneoak ditu. Denbora igaro ahala, gainera, gero eta sofistikatuagoak dira. Etorkizunera begira garatu dezaketen sofistikazio mailaren arabera, material horien lau

[1] *The Proyect on Emerging Nanotechnologies* izeneko datu base estatu batuarrak (ikus *http://www.nanotechproject.org/cpi/*) merkatuan NMMak erabiltzen dituzten 1827 produktu komertzial identifikatu ditu. Danimarkako ingurugiro eta kontsumitzaileen babeserako gobernuz kanpoko erakundeek landutako *The Nanodatabase* inbentarioan (*http://nanodb.dk/en/*), ordea, kopuru hori 2440 produktutakoa da. Hala ere, Europar Batasuneko Komisioak COM (2012) 572 Komunikazioan onartzen duen bezala, merkatuan eskuragarri diren nanoprodukturen kopurua seguruenez inbentario horietan kalkulatzen diren zifrak baino dezente altuagoa da.

[2] *Nanowerk* erakundeak emandako datua (*http://www.nanowerk.com/*).

belaunaldi desberdin iragarri dira[3] (Roco, 2011). Nanoteknologiek halaber "ahalbidetze teknologia" bezala funtzionatzen dute; hots, NMMak beste teknologia berri batzuen (esate baterako, bioteknologien edo informazio eta komunikazio teknologien) gaitasunak eta funtzioak potentziatzeko erabiltzen dira.

Informazio eta komunikazio teknologien (IKTen) eta nanoteknologien arteko konbergentziatik lortzen diren dispositibo elektroniko sofistikatuek ordea, bestelako ikuspegi batetik aztertuta, gizakien eta orokorrean gizartearen gaineko kontrol eta zaintzarako eskaini ditzaketen aukera berriek kezka nabarmena sortzen dute (Barinas Ubiñas, 2013; Faunce, 2007; Ganascia, 2011). Ikerketa honetan hain zuzen ere konbergentzia harreman horretatik eratorritako aplikazio teknologiko baten jarri da arreta, zehazki, irrati frekuentzia bidezko identifikazio sistemadun (RFID) etiketa elektronikoen erabileran.

Produktuetan txertatzean RFID etiketek euren datuak (ezaugarriak, unean uneko kokapena, etab.) formatu digitalean jaso, gorde, eta irrati frekuentzien bidez dispositibo elektroniko hartzaile batera (ordenagailu batera adibidez) transmititzen dituzte, informazio datu horiek "gauzen internet" izeneko sarera konektatuz[4]. NMMak erabiliz, gainera, RFID etiketen prestazioek nabarmen egin dezakete hobera, informazio bolumen handiagoa eta zehatzagoa jaso, bildu eta transmititzeko gaitasuna eskuratzen baitute, dispositibo hartzailearengandik distantzia gero eta luzeagora[5]. Produktuen unean-uneko trazabilitatea ahalbidetzen duten neurrian, etiketa elektroniko horiek abantaila ugari eskaintzen dituzte esparru komertzialean. Tamaina handiko enpresetan batez ere[6], testuinguru desberdinetan eta gero eta maiztasun handiagoarekin erabiltzen dira, besteak beste, garraio publikoko txarteletan, produktuen antolamendu efiziente baterako edota produktuen lapurretak ekiditeko segurtasun neurri bezala.

Alabaina, RFID etiketek produktuen unean-uneko trazabilitatea egitea posible duten bezalaxe, produktu horiek gainean daramatzaten pertsonen mugimenduak zehaztasun handiz monitorizatzeko edo bestelako datu batzuk lortzeko gaitasun teknikoa ere badute. Ondorioz, dispositibo horiek informazio pertsonala eskuratzeko instrumentu bezala zinez baliagarriak ere badiren neurrian, erabilera horiek norbanakoen pribatutasun esferarekin topo egiten dute. Hartatik, RFID etiketen bidez egindako datu pertsonalen tratamendu horiek legalitatearekin bateragarriak izan daitezen, datu pertsonalen babeserako legedian aurreikusitako bermeak errespetatu behar dituzte.

2. Ikerketaren helburuak

Laburpenean aurreratu den bezala, RFID etiketak norbanakoen informazio pertsonala eskuratzeko erabili izan diren kasu batzuk dokumentatu dira dagoeneko. Ikerketa honetan hurrengo hiru kasuak dira aztergai:

- Las Vegas hiriko kasino batek bere langileen lan uniformeetan irismen luzeko RFID etiketak erantsi zituen (Bibby, 2006) langileen kokalekua eta mugimenduak kontrolatzeko lan-zaintza neurri bezala.

[3] Gaur egun erabiltzen diren nanoestruktura pasiboetatik, hamarkada batzuen buruan, adimen gaitasun propioa duten nanosistema aktiboetara igaro gaitezkeela aurreikusten du doktrina zientifikoak.

[4] Orotara bi RFID etiketa mota existitzen dira: aktiboak eta pasiboak. Etiketa aktiboek energiaz hornitzen dituen bateria txiki bat erabiltzen dute irrati seinaleak bidaltzeko, 10 urte inguruko iraupen epea dutenak. Etiketa pasiboek, ordea, ez dute inolako energia bateriarik erabiltzen eta beren iraupena mugagabea da, irrati seinaleek sortzen duten energiaz aprobetxatzen baitira funtzionatzeko. Aitzitik, etiketa aktiboen seinaleen irismena pasiboena baino askoz ere handiagoa da: lehenengo motatakoen seinaleak 1500 metro inguruko distantzia-arte izan daitezke irakurriak, bigarrenak ordea 10 metro arte soilik.

[5] Horri buruz ikus EBko Komisioaren honako komunikazioa: Comunicación COM 2007 (96) final de la Comisión al Consejo, al Parlamento europeo, al Comité Económico y Social Europeo y al Comité de las regiones La identificación por radiofrecuencia (RFID) en Europa: pasos hacia un marco político.

[6] 2010. urteko datuen arabera, RFID sistemadun dispositiboak enpresa txikien (10-49 langile) %0,8etan, enpresa ertainen (50-249 langile) %8,9etan eta enpresa handien (250 langiletik gorakoak) %20an erabiltzen ziren (INTECO eta AEPD, 2010). 2016-21 bitartean RFID teknologiak mundu mailan izan dezakeen bilakaeraren estimazioak ere egin dira (ikus ResearchMoz, 2016).

- Estatu Batuetako bi ospitalek, 2004-2006 bitartean 100 paziente ingururi eskuineko besoan RFID sistema erabiltzen zuen *Verichip* izeneko inplante bat txertatu zieten, beren osasunari buruzko datuak monitorizatzeko helburuz (Miller eta Kearnes, 2012).

- *Benetton* arropa markak 2003. urtean bere janzkietan RFID etiketak txertatzeko asmoa iragarri zuen, ustez helburu logistiko soiletarako. Alabaina, proiektua argitara irten bezain laster kritika ugari jaso zituen, enpresaren benetako asmoa RFID seinalearen arrastoari jarraituz janzki horietako bat gainean zeraman pertsonaren mugimenduak monitorizatu eta horrela kontsumitzaileen profil osatu bat lortzea zenaren susmoak indarra hartu baitzuen. Presio publikoaren ondorioz, proiektua abian jarri aurretik bertan behera geratu zen.

Lehenengo bi kasuetan RFID dispositiboak langile eta pazienteen datu pertsonalak jaso, bildu eta transmititzeko erabili ziren, eta hartatik, beren datu pertsonalen tratamendua gertatu zen. Hirugarren kasuan *Benetton* arropa marka ez zen proiektua martxan ipintzera iritsi. Hala ere, ikerketa honetan kontsumitzaileen informazioaren balizko erabilera hori datu pertsonalen babeserako legediarekin bateragarria izan daitekeen ere aztertzen da, kontuan hartuta gero eta enpresa gehiago direla beren arropetan RFID etiketak txertatzen dituztenak. Hiru kasu horietan beraz (esan bezala, lehenengo biak errealak dira eta hirugarrena hipotetikoa), tratatutako datu pertsonalen titularren autodeterminazio informatiborako eskubidea (Espainiar Konstituzioko –EK– 18.4 artikuluan aurreikusia) eraginda geratzen da. Oinarrizko eskubide horrez gain, tratamendu horiek halaber pribatutasuna dimentsio desberdinetatik babesten duten beste bi eskubide uki ditzakete. Alde batetik, intimitaterako eskubideari (EK 18.1 art.), norbere bizitzaren zenbait eremu 3. pertsonen ezagutzatik kanpo mantentzeko defentsa eskubide generiko bezala ulertuta. Bestetik, RFID etiketak pertsonen mugimenduak monitorizatzeko erabiltzen diren kasuetan, mugimendu askatasuna (EK 19. art.) ere eraginda geratzen da, norbanakoek beren mugimenduei buruzko informazioa 3. pertsonen ezagutzatik kanpo mantentzeko duten arrazoizko itxaropen bezala ulertuta. Mugimendu askatasunaren dimentsio hori autodeterminazio informatiborako eskubidearen jarduera-eremuan kokatzen da, pertsonen mugimenduei buruzko informazioa, funtsean, datu pertsonalak baitira[7].

Aztergai ditugun kasuetan datu pertsonalak beren titularren esfera pribatua errespetatuz tratatu diren edo ez erabakitzeko, analisi hori autodeterminazio informatiborako eskubidearen prismatik eraman da aurrera. Espainiar ordenamendu juridikoan, gaur-gaurkoz[8], datu pertsonalen tratamenduari buruzko baldintza normatibo orokorrak Datuen Babeserako 15/1999 Lege Organikoan (DBLO) eta 1720/2007 Errege Dekretuan (DBE) arautzen dira[9]. Legedi horrez gain, datu pertsonalen tratamenduari buruz arauketa sektorialek aurreikusten dituzten baldintza normatibo espezifikoak ere kontuan hartu behar dira: osasun eremuan, pazientearen

[7] Jurisprudentziak berriki aintzatetsi egin du mugimendu askatasunaren dimentsio horrek intimitaterako eskubidearekin eta autodeterminazio informatiborako eskubidearekin duen konexio puntu komun hori. Ikus EAEko Justizia Auzitegi Nagusiaren (Lan Arloko 1. Sailaren) 2011ko maiatzaren 10eko ebazpena (AS\2012\2277) eta Auzitegi Gorenaren (Lan Arloko 1. Sailaren) 2012ko ekainaren 21eko ebazpena (RJ\2012\7627).

[8] 2018ko maiatzaren 25etik aurrera ordea EBko Legebiltzarraren eta Kontseiluaren 2016/679 Erregelamendua indarrean sartuko da, Estatu-kideei zuzenean aplikagarri zaien datu pertsonalen araudi komunitario berria. Data horretatik aurrera beraz, 15/1999 Lege Organikoaren eta 1720/2007 Errege Dekretuaren aplikagarritasuna 2016/679 Erregelamenduaren aplikazio eremutik kanpo geratzen diren esparruetara murriztuta geratuko da. Erregelamendu komunitario horren berritasunen artean, besteak beste, honakoak azpimarratu daitezke: ahazte-eskubidearen esanbidezko aintzatespena, datu pertsonalen tratamenduari buruzko gardentasun eta babes-kontrol neurri berriak, datu pertsonalen titularrari hizkera argia erabiltzeko esanbidezko betebeharra eta titularraren baimena lortzeko baldintzen zorroztea, EBkoak ez diren 3. Estatuetara datu pertsonalak transmititzeko baldintzen areagotzea eta orotara, isunen zenbateko ekonomikoaren igoera.

[9] Datu pertsonalak euskal administrazioren batek tratatzen dituenean (EAEko administrazioak, lurralde historikoetako foru-erakundeek edota toki-erakundeek), aipatu oinarrizko legediarekin batera Eusko Legebiltzarraren 2/2004 Legea aplikatzen da, Datu Pertsonaletarako Jabetza Publikoko Fitxategiei eta Datuak Babesteko Euskal Bulegoa Sortzeari buruzkoa. Frantziari dagokionez, hurrengo legea izan behar da kontuan: Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Autonomiari buruzko Legearenak (41/2002 Legea) eta lan eremuan, Langileen Estatutukoak (2/2015 Dekretu Legegilea).

3. Ikerketaren muina

Datu pertsonalak formatu digitalean jaso, gorde eta funtsean tratatu egiten direnean, norbanakoaren "gorputz elektronikoa" (Rodota, 2010) edo kopia digitala bailira funtzionatzen dute, 3. pertsonen ezagutzara irekitzen den norbere pertsonalitatearen alderdi desberdinen adierazpen gisa. Beraz, autodeterminazio informatiborako eskubidearen izate-arrazoia, norbere identitatearen aspektu desberdinak ezagutaraztera ematen dituzten datu pertsonal horien gainean titularrak egikaritzen duen autonomia gaitasunean datza.

Datu pertsonalen tratamenduak oinarrizko eskubide horrekin (eta zeharka intimitate eskubidearekin eta mugimendu askatasunarekin) bateragarriak izateko, tratamendu horiek "kalitatezkoak" izatea exijitzen du legediak. Horretarako, tratamendua orok hiru oinarrizko printzipio legal bete behar ditu: helburuzko printzipioa, egokitasun printzipioa eta egiazkotasun printzipioa[10]. Horietako bat errespetatu ezean, tratamendua legediaren aurkakoa izango da. Helburuzko printzipioaren arabera, datu pertsonalak helburu zehatz, esplizitu eta legitimo batetarako jaso behar dira. Egokitasun printzipioaren arabera, jasotako datu pertsonalek beren tratamendua motibatzen duen helburua betetzeko aproposak, egokiak eta ez-gehiegizkoak izan behar dute; hots, datu pertsonalen tratamendua proportzionaltasun printzipioarekin bateragarria izan behar da. Azkenik, egiazkotasun printzipioak, jasotako datu pertsonalak zehatzak izatea eta momenturo eguneraturik egotea eskatzen du. Bestalde, legeak kontrakoa adierazi ezean[11], datu pertsonalak tratatu ahal izateko beren titularraren baimen informatua lortu behar da: baimen horrek libreki emana (biziorik gabea), espezifikoa (datuak esleitu diren helburu zehatz, esplizitu eta legitimora bideratua) eta argia (zalantzarik gabekoa eta berariazkoa) behar du izan[12].

Aztergai ditugun hiru kasuetan RFID etiketen bidez egiten den datu pertsonalen tratamendua helburuzko printzipioarekin bateragarria izan daiteke:

- Merkataritza jarduerak burutzen dituzten enpresa edo pertsonek, legediaren arabera, posible dute publizitate edo prospekzio komertzial helburuetarako hirugarren pertsonen datu pertsonalak eskuratu eta horien tratamendua egitea. Hori bai, aztergai dugun kasuan datu horien titularrak tratamendu horri aurretiaz baimen informatua ematea ezinbesteko baldintza da[13] (alegia, kontsumitzaileari argitasunez informatu behar zaio RFID etiketa bidez, publizitate edo prospekzio komertzial helburupean, zein datu pertsonal izango zaizkion tratamenduaren objektu). Izan ere, merkataritza jarduerak burutzen dituzten enpresa edo pertsonek kontsumitzaileen datu pertsonalak euren titularren baimen informatua eduki gabe eskuratuz gero, datuok iruzur bidez eta modu ez-leialean jasoak izango lirateke, legedian arau-hauste oso larri bezala tipifikatuta dagoen portaera[14].
- Lan eremuan, enplegatzaileak bere enplegatuen lan-jarduera kontrolatzeko duen ahalmen legala baliatuz[15], bere enplegatuen datu pertsonalak tratatzen dituzten lan-zaintza dispositiboak erabili ditzake, langileen uniformeetan txertatutako RFID etiketak kasu. Arau orokor bezala, enplegatzaileak ez du datu pertsonalen tratamendu horretarako bere enplegatuen baimenik behar[16]. Hori bai, RFID etiketak lan-segurtasun neurri bezala erabiltzen hasi aurretik, enplegatzaileak enpresa komiteari (langileen

[10] Ikus DBLO, 4. art.
[11] Titularraren baimenik gabe bere datu pertsonalak tratatu daitezkeen salbuespen kasuei buruz, ikus DBLO 6.2 art.
[12] Baimen informatuaren inguruan, DBLO 3.h) art. eta 5-6. art.
[13] Ikus DBLO 30. artikulua eta horren edukia garatzen duen DBE 45. artikulua.
[14] DBLO,44.4.a) art.
[15] Langileen Estatutuko 20. artikuluaren 3. eta 4. atalak kontsultatu.
[16] Hori bai, DBLO, 6.2 artikuluari jarraiki ideologia, afiliazio sindikala, erlijioa edo sinesmenei buruzko datu pertsonalak tratatzeko titularraren baimen idatzizkoa eta esanbidezkoa beharrezkoa da (DBLO 7.2 art.). Bestalde, ezin da fitxategirik sortu horien helburu esklusiboa bereziki pertsonalak diren datu horiek biltzean badatza (DBLO 7.4 art.).

ordezkaritza organoari alegia) RFID etiketen berri eman behar dio[17] eta langileek beren datu pertsonalen tratamenduaz eta horrekin bilatzen den helburuaz informatuak izateko eskubidea dute[18], helburua zaintza-sekretua egitea den kasuetan izan ezik[19].

- RFID etiketak pazienteen datuak eskuratzeko erabili diren kasuan, legeak bereziki babesten dituen datu pertsonalen kategoria batekin egiten dugu topo, osasun-datuekin hain zuzen ere. Osasun-datuak tratatu ahal izateko arau orokor bezala euren titularrak baimen informatua berariaz eman behar badu ere[20], hurrengo bi baldintza normatiboak betetzen diren kasuetan baimen hori ez da beharrezkoa[21]: alde batetik, datu tratamenduaren helburua pazientearen osasuna babestea denean, eta bestetik, tratamendu hori profesional sanitarioek egiten dutenean. Hori bai, *Verichip* izeneko inplantea pazientearen gorputzean txertatzeko ebakuntza mediko bat egin behar den aldetik, pazienteak aurretiaz ebakuntza mediko hori modu informatuan baimendu izana ezinbestekoa da (EKn inplizituki barneratzen den pazientearen oinarrizko eskubide baten aurrean baikaude[22]).

Aitzitik, tratamendu horiek ez dira bateragarriak egokitasun printzipioarekin. RFID etiketen bidez datu pertsonalei ematen zaien tratamendua ez-egokia eta gehiegizkoa da hiru kasu horietako bakoitzean bilatzen den helburu legitimoari konplimendua emateko:

- *Benetton* janzkietan txertatutako RFID etiketen bidez produktua gainean daraman kontsumitzailearen mugimenduak, helbidea, ohitura komertzialak eta bestelako datu pertsonalak lortzea teknikoki posible da. Datu pertsonal horiek prospekzio komertzial edo publizitate helburuetarako zinez baliagarriak izan badaitezke ere, datu horien izaera eta bolumena ez-egokia eta gehiegizkoa da helburu horiek asebetetzeko. Ondorioz, datu pertsonal guzti horiek eskuratu eta tratatzeak *Benetton* janzkia gainean daraman pertsonaren autodeterminazio informatiborako eskubidea modu ez proportzionalean mugatzen du. RFID etiketek pribatutasunaren ikuspegitik planteatzen dituen arazoez ohartuta, gai honetan eskumena duten Komunikazio Teknologien Institutu Nazionalak (INTECO) eta Datuen Babeserako Espainiako Agentziak (AEPD) produktua kontsumitzaileari saltzearekin batera RFID etiketa desaktibatzea eta etiketa horietan kontsumitzailearen datu pertsonalik ez biltzea eskatu dute (INTECO eta AEPD, 2010).
- Lan arloan, kontrol-neurri bezala langileen uniformeetan txertatzen diren RFID etiketek beren kokapena eta mugimenduak uneoro eta etengabe monitorizatzeko gaitasuna dute, lanarekin zerikusia izan dezaketen eta zerikusirik ez duten (esate baterako, komunera noiz eta zenbatetan doazen eta bertan zenbat denbora pasatzen duten) portaeren artean inolako bereizketarik egin gabe. Bestalde, langileen pribatutasuna intentsitate baxuagoan mugatzen duten eta lan-zaintzaren helburua ere eraginkortasunez asebete dezaketen bestelako neurriak eskuragarri ditu enplegatzaileak (bideo zaintzarako kamerak esate baterako).
- Pazienteen osasuna hobeto monitorizatu eta zaintzeko helburuz euren gorputzean txertatzen diren txipen kasuan ere antzeko inguruabarrak ematen dira. Nanomedikuntzari (hots, NMMak erabiltzen dituzten tratamendu mediko berritzaileei) etorkizunera begira garapen nabarmena iragartzen zaio, baita inplanteen alorrean ere. Hartatik, pazienteak monitorizatzeko txipak, nanomedikuntzari esker, gero eta sofistikatuagoak bilakatu eta

[17] Izan ere, enplegatzaileak lan antolakuntza eta kontrolerako neurri berriak hartu edo horiek berrikusten dituen kasuetan, enpresa komitea inguruabar horretaz informatu egin behar du (Langileen Estatutua, 64.6 art.), azken horrek neurri horiei buruz informe bat emititzeko eskumen legala baitu (64.5.f) art.).

[18] Ikus DBLO, 5. art.

[19] Zaintza sekretuek langileen pribatutasun esferan intentsitate handiagoz eragiten dutela kontuan izanda, lan-zaintza neurri horiek baldintza gehigarriak bete behar dituzte legitimoak izateko (ikus Auzitegi Konstituzionalaren 186/2000 ebazpena): zaintza sekretua delituzko jarduera baten edo bestelako arau-hauste larri baten arrazoizko zantzuak daudenean, horiek ikertzeko *ultima ratio* bezala soilik izan daiteke erabilia. Alegia, ustezko arau-hauslea harrapatzeko bestelako zaintza-neurriak eraginkorrak ez diren kasuetan soilik erabili daitezke zaintza-neurri sekretuak.

[20] DBLO, 7.3 art.

[21] DBLO, 7.6 eta Pazientearen Autonomiari buruzko 41/2002 Legea, 2.7 art.

[22] Horri buruz, besteak beste, ikus Auzitegi Konstituzionalaren 37/2011 ebazpenaren 3. oinarri juridikoa.

> pazienteen osasun eta ezaugarri biologikoei buruz gero eta datu bolumen handiagoa eta zehatzagoa lortzeko gaitasuna garatu dezakete, gaur egun lortzea erabat ezinezkoak diren osasun-datuak barne. Nanotxipen bidez eskuratu daitezkeen datu pertsonalak pazientearen osasuna monitorizatu eta zaintzeko helburua asebetetzeko baliagarriak izan badaitezke ere, lortutako osasun-datuen kopurua gehiegizkoa izan liteke helburu horretarako. Horrez gain, RFDI sistemadun txip horiek pazientearen osasuna babesteko helburuarekin inolako zerikusirik ez duten informazio pertsonala eskuratzea ahalbidetzen dute, bere mugimenduak eta kokalekua esate baterako. Azkenik, osasuna babesteko helburu legitimoa asebetetzeko gaitasuna duten eta gorputzarentzat txip inplanteak bezain intrusiboak ez diren bestelako metodo sanitarioak eskuragarri daude.

Atal honekin amaitzeko, errepikatzen den beste arazo komun bati heldu behar zaio: RFID etiketek datu pertsonalak gordetzeko fitxategi bezala duten segurtasun maila oso baxua da. Gogoan izan etiketa elektroniko horiek irrati-frekuentzia seinaleak erabiltzen dituztela barnean gordeta duten informazioa internet bidez interkonektatuta dagoen informazio sare digital batera transmititzeko. Irrati-seinaleak, aitzitik, horiek irakurtzeko gai den edozein dispositiboren bidez izan daitezke atzemanak eta RFID sistemak ez du balizko sarrera ez-legitimo hori erregistratzeko gaitasun nahikorik erakusten (Miller eta Kearnes, 2012). Ondorioz, 3. pertsona batek datu pertsonalak modu ez zilegian eta inolako arrastorik utzi gabe eskuratu eta tratatzea gertatu daiteke. Bestalde, datu pertsonal horiek internet bidez interkonektatuta dagoen informazio sare digital batera transmititzen direnez, sare hori eraso zibernetiko ugariren objektu izan daiteke, datu pertsonalak manipulatu, kaltetu eta suntsitzeko gaitasuna dutenak (INTECO eta AEPD, 2010).

Datu pertsonalak gordetzen dituzten fitxategien osotasuna eta segurtasuna bermatzeko DBLOk eta DBEk aurreikusten dituzten segurtasun-neurri zorrotzak ikusita[23], normatiboki exijitzen den segurtasun maila altu horretatik urrun geratzen dira RFID etiketak. Segurtasun gabezia horiek are garrantzi handiagoa eskuratzen dute RFID etiketak osasun-datuak jaso eta transmititzeko erabiltzen diren kasuetan; legeak bereziki babesten dituen datu pertsonalak izanik, datu horiek gordetzen dituzten fitxategien segurtasun maila gorenekoa izan behar baita[24].

4. Ondorioak

Ikerketa honetan aztergai izan diren hiru kasuetan, RFID dispositiboen bidez helburu legitimo desberdinen betearazpenera zuzendutako datu pertsonalen tratamendua egin da, hurrenez hurren, langileena (laneko betebeharrekin konplitzen dutela kontrolatzeko), pazienteena (beren osasuna babesteko) eta kontsumitzaileena (publizitate edo prospekzio komertzial helburuetarako). Alde horretatik, tratamendu horiek legediarekin bateragarria izateko lehenengo baldintza (helburuzko printzipioa) errespetatu egiten da. Alabaina, tratamendu horietako bat ere ez da proportzionala kasu bakoitzean bilatzen den helburuaren konplimendurako, RFID etiketaren bidez hura gainean daraman pertsonaren datu ugari eta anitzak eskura baitaitezke. Eskuratutako informazio pertsonala bere osotasunean kontuan hartuta, datu horietako batzuek ez dute pertsegitzen den helburua asebetetzeko balio (datu ez-egokiak dira) edo gehiegizkoak dira xede horretarako. Funtsean, ez da betetzen legediarekin bateragarria izateko datu pertsonalen tratamendu orok errespetatu behar duen bigarren baldintza, hots, egokitasun printzipioa. Azkenik, RFID etiketek ez dute datu pertsonalen fitxategi bezala erabiltzeko balio, ez baitituzte barnean gordeta dituzten datu pertsonalen osotasuna eta segurtasuna bermatzeko legediak exijitzen dituen segurtasun-neurriak betetzen.

Funtsean, ikerketa honetan aztergai izan diren kasu guztietan RFID etiketen bidezko datu pertsonalen tratamenduak ez du aplikagarri zaien legedia errespetatzen eta ondorioz, autodeterminazio informatiborako eskubidea, eta zeharka, intimitaterako eskubidea eta mugimendu askatasuna bezalako oinarrizko eskubideak urratu egin dira.

---

[23] Segurtasun neurri horiek DBEren III. kapituluan (89-104 art.) arautzen dira.

[24] DBE 81.3.a) artikuluaren arabera, osasun-datuak biltzen dituzten fitxategiek oinarrizko, maila ertaineko eta goi mailako segurtasun neurriak bete behar dituzte.

5. Etorkizunerako planteatzen den norabidea

Datu pertsonalen babesaren ikuspegitik RFID dispositiboek dakartzaten erronkek, ezbairik gabe, aparteko garrantzia dute. Horretaz jakitun, Europar Batasuneko Komisioak (2009) 32000 Gomendioa[25] onartu zuen. Gomendio horren harira merkatu operatzaileek etiketa elektroniko horiek erabiltzen dituzten produktuak diseinatzean datu pertsonalen eta intimitatearen babesaren ikuspegitik izan dezaketen inpaktua ebaluatu eta neurri zuzentzaileak hartu behar dituzte, eginkizun horretarako agintari publiko komunitario eta nazional eskudunek argitaratu dituzten gidak oinarri hartuta (hurrenez hurren, Grupo de Protección de Datos del Artículo 29, 2011; AEPD, 2014).

Beraz, etorkizunera begira, ikerketa lerro posible bat honakoa izan daiteke: RFID etiketak erabiltzen dituzten merkatu operatzaileek inpaktu ebaluaketa horiek nola aurrera nola eramaten dituzten eta datu pertsonalak babesteko zein neurri zuzentzaile hartzen dituzten aztertzea.

6. Erreferentziak

AEPD (2014): *Guía para una evaluación de impacto en la protección de datos personales*.

Barinas ubiñas, D. (2013), El impacto de las tecnologías de la información y comunicación en el derecho a la vida privada: las nuevas formas de ataque a la vida privada, *Revista electrónica de Ciencia Penal y Criminología*, 15.

Bibby, A. (2006): *Te están siguiendo: Control y vigilancia electrónicos en el lugar de trabajo*, Sindicato Global.

Faunce, T. (2007), Nanotechnology in global medicine and human biosecurity: private interests, policy dilemmas, and the calibration of public health law, *Journal of Law, Medicine and Ethics*, 35 (4), 629-642.

Ganascia, J.(2011), The new ethical trilemma: security, privacy and transparency. *Comptes Rendus Physique, Elsevier,* 12 (7), 684-692.

Grupo de Protección de Datos del Artículo 29 (2011): *Dictamen 9/2011 relativo a la Propuesta Revisada de la Industria para un Marco de Evaluación del Impacto sobre la Protección de Datos y la Intimidad en las Aplicaciones Basadas en la Identificación por Radiofrecuencia (RFID)*, Bruselas.

INTECO y AEPD (2010): *Guía sobre seguridad y privacidad de la tecnología RFID*.

Miller, G. eta Kearnes, M. (2012): *Nanotechnology Ubiquitous Computing and The Internet of Things: Challenges to Rights to Privacy and Data Protection Draft Report to the Council of Europe*, Council of Europe.

ResearchMoz (2016): *Global RFID Tag Market Outlook 2016-2021*.

Roco, M. (2011), The long view of nanotechnology development: the National Nanotechnology Initiative at 10 years, *Journal of Nanoparticle Research*, 13 (2), 427-445.

Rodota, S. (2010), Nouvelles technologies et droits de l'homme: faits, interprétations, perspectives, *Mouvements,* 2 (62), 55-70.

7. Eskerrak

Ikerketa hau ikertzaile doktoreak espezializatzeko Euskal Herriko Unibertsitateak urtebeterako emandako laguntza bati esker eraman da aurrera. Beraz, lerrook baliatu nahi ditut EHUri eskerrak emateko.

[25] Recomendación de la Comisión de 12 de mayo de 2009 sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia [notificada con el número C(2009) 3200].